



**U.S. Department of Housing and Urban Development  
Office of Public and Indian Housing**

**SPECIAL ATTENTION OF:**

Directors of HUD Regional and Field  
Offices of Public Housing;  
Public Housing Agencies that  
Receive Funds under Any Public and  
Indian Housing Program

**NOTICE PIH-2015-06**

Issued: April 23, 2015

Expires: Effective until  
amended, superseded, or  
rescinded

Cross References:

PIH 2014-10, PIH 2010-15

**Subject: U.S. Department of Housing and Urban Development (HUD) Privacy Protection  
Guidance for Third Parties**

- 1) **Purpose:** This notice informs all public housing agencies (PHAs) about their responsibilities for safeguarding personally identifiable information (PII) required by HUD and preventing potential breaches of this sensitive data. HUD is committed to protecting the privacy of individuals' information stored electronically or in paper form, in accordance with federal privacy laws, guidance, and best practices. HUD expects its third party business partners, including Public Housing Authorities, who collect, use, maintain, or disseminate HUD information to protect the privacy of that information in accordance with applicable law.

PIH 2014-14 is being revised to include guidance to assist PHA system administrators and users to fulfill their requirements for information technology security awareness training.

- 2) **Background:** Section 6 of the Housing Act of 1937, the Privacy Act of 1974, 5 U.S.C. § 552a (Privacy Act), The Freedom of Information Act (FOIA), 5 U.S.C. § 552, and Section 208 of The E-Government Act are the primary federal statutes that limit the disclosure of information about public housing residents and recipients of the Housing Choice Voucher program. In addition, the Housing and Community Development Act of 1987, 42 U.S.C. § 1437d (q)(4), 42 U.S.C. § 1437d (t)(2), 42 U.S.C. § 3543, and the Stewart B. McKinney Homeless Assistance Act of 1988, 42 U.S.C. § 3544, further regulate the treatment of this information.
  - a) General HUD program requirements are set forth in 24 C.F.R. Part 5, Subpart B, Disclosure and Verification of Social Security Numbers and Employer Identification Numbers: Procedures for Obtaining Income Information. Subpart B enables HUD and

PHAs to obtain income information about applicants and participants in the covered programs through computer matches with State Wage Information Collection Agencies (SWICAs) and Federal agencies, in order to verify an applicant's or participant's eligibility for or level of assistance.

- i) *Restrictions on Use of Income Information Obtained from SWICA and Federal Agencies.* The restrictions of 42 U.S.C. 3544(c)(2)(A) apply to the use by HUD or a PHA of income information obtained from a SWICA and the restrictions of 42 U.S.C. 3544(c)(2)(A) and of 26 U.S.C. 6103(l)(7)(C) apply to the use by HUD or a PHA of income information obtained from the Internal Revenue Service or the Social Security Administration.
- b) The Privacy Act and other requirements for grants and contracts is spelled out in 24 C.F.R. 5.212 which states:
  - i) *Compliance with the Privacy Act.* The collection, maintenance, use, and dissemination of SSNs, EINs, any information derived from SSNs and Employer Identification Numbers (EINs), and income information under this subpart shall be conducted, to the extent applicable, in compliance with the Privacy Act (5 U.S.C. 552a) and all other provisions of Federal, State, and local law.

*Privacy Act Notice.* All assistance applicants shall be provided with a Privacy Act notice at the time of application. All participants shall be provided with a Privacy Act notice at each annual income recertification.
- c) The Federal Acquisition Regulation (FAR), 48 C.F.R. 24.104, sets forth that compliance with the requirements of the Privacy Act be included in HUD contracts at clause 52.224-2, which provides in part:
  - (a) *The Contractor agrees to—*
    - (1) *Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act ....*

Similar language is included in all HUD Grant Agreements requiring the Grantee to comply with the provisions of the Privacy Act of 1974 and the agency rules and regulations issued under the Act. (See Attachments 1 and 2 for the above provisions)

- d) Additional federal guidance on privacy protection is in OMB privacy-related memoranda, including:
  - i) OMB M-01-05, Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy
  - ii) OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

- iii) OMB M-04-26, Personal Use Policies and —File Sharing Technology
  - iv) OMB M-05-08, Designation of Senior Agency Officials for Privacy
  - v) OMB M-06-15, Safeguarding Personally Identifiable Information
  - vi) OMB M-06-16, Protection of Sensitive Agency Information
  - vii) OMB M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
  - viii) OMB Memo, September 20, 2006, Recommendations for Identity Theft Related Data Breach Notification Guidance
  - ix) OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information
  - x) OMB M-14-04, FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (FISMA). FISMA requires federal agencies to implement a mandatory set of processes designed to ensure the confidentiality, integrity, and availability of system related information. FISMA requires program officials, and the head of each agency, to conduct annual reviews of information security programs, with the intent of keeping risks at or below specified acceptable levels in a cost-effective, timely, and efficient manner.
- e) Definitions

As used in this Notice, the following terms are defined as:

- i) Personally Identifiable Information (PII). Defined in OMB M-07-16 as “. . . information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.”
  - ii) Sensitive Personally Identifiable Information. PII that when lost, compromised or disclosed without authorization could substantially harm an individual. Examples of sensitive PII include social security or driver’s license numbers, medical records, and financial account numbers such as credit or debit card numbers.
- 3) **Guidance on Protecting Sensitive Privacy Information:** The Privacy Act requires that federal agencies maintain only such information about individuals that is relevant and necessary to accomplish its purpose. The Privacy Act also requires that the information be maintained in systems or records – electronic and paper – that have the appropriate

administrative, technical, and physical safeguards to protect the information, however current. This responsibility extends to contractors and third party business partners, such as Public Housing Authorities, who are required to maintain such systems of records by HUD.

- a) Contractors and third party business partners should take the following steps to help ensure compliance with federal requirements:

**i) Security Awareness and Privacy Training**

- (1) The National Institute of Standards and Technology (NIST) publishes [templates and guides](#) for what security awareness trainings should entail in order to be FISMA compliant. These guidelines focus on the following key aspects:
  - **Confidentiality** - Protecting information from unauthorized access and disclosure.
  - **Integrity** - Assuring the reliability and accuracy of information and IT resources by guarding against unauthorized information modification or destruction.
  - **Availability** - Defending information systems and resources to ensure timely and reliable access and use of information. As such, systems are vulnerable to misuse, interruptions and manipulation.
  - **Threat**- A threat in the case of IT security is the potential to cause unauthorized disclosure, unavailability, changes, or destruction of protected information.
  - **Vulnerability**- Any flaw or weakness that can be exploited and could result in a breach or a violation of a system's security policy
  - **Risk** is the likelihood that a threat will exploit vulnerability.
  - **Controls** are policies, procedures, and practices designed to decrease the likelihood, manage the impact, or minimize the effect of a threat exploiting a vulnerability
- (2) Additionally, the NIST provides publications for reference on [Building an Information Technology Security Awareness and Training Program](#) and [Security and Privacy Controls for Federal Information Systems and Organizations](#)
- (3) PHAs should maintain adequate documentation that supports the training for all staff as well as maintain auditable records of training completion. Although there is not required reporting on the training, Office of Field Operations personnel may spot-check compliance on on-site visits.

**ii) Limit Collection of PII**

- (1) Do not collect or maintain sensitive PII without proper authorization. Collect only the PII that is needed for the purposes for which it is collected.
- (2) Consistent with the provisions of this Notice, PHAs may enter into agreements (or in some cases be required) to provide PII to legitimate researchers under contract



or other agreement with HUD to support studies on the effects and operations of HUD programs. Further, HUD encourages PHAs to supply PII to other legitimate researchers who do not have contracts or other agreements with HUD in support of such studies, so long as the PHA in question has taken reasonable precautions to prevent disclosure of PII outside of the research team. Such reasonable precautions generally involve written agreements between the PHA and one or more researchers that specify the legal obligations of the latter to protect PII from disclosure.

### **iii) Manage Access to Sensitive PII**

- (1) Only share or discuss sensitive PII with those personnel who have a need to know for purposes of their work. Challenge anyone who asks for access to sensitive PII for which you are responsible.
- (2) Do not distribute or release sensitive PII to other employees, contractors, or other third parties unless you are first convinced that the release is authorized, proper and necessary.
- (3) When discussing sensitive PII on the telephone, confirm that you are speaking to the right person before discussing the information and inform him/her that the discussion will include sensitive PII.
- (4) Never leave messages containing sensitive PII on voicemail.
- (5) Avoid discussing sensitive PII if there are unauthorized personnel, contractors, or guests in the adjacent cubicles, rooms, or hallways who may overhear your conversations.
- (6) Hold meetings in a secure space (i.e., no unauthorized access or eavesdropping possible) if sensitive PII will be discussed and ensure that the room is secured after the meeting.
- (7) Treat notes and minutes from such meetings as confidential unless you can verify that they do not contain sensitive PII.
- (8) Record the date, time, place, subject, chairperson, and attendees at any meeting involving sensitive PII.

### **iv) Protect Hard Copy and Electronic Files Containing Sensitive PII**

- (1) Clearly label all files containing sensitive PII by placing appropriate physical labels on all documents, removable media such as thumb drives, information systems, and application. Examples of appropriate labels might include —For Official Use Only or —For (Name of Individual/Program Office) Use Only.

- (2) Lock up all hard copy files containing sensitive PII in secured file cabinets and do not leave unattended.
- (3) Protect all media (e.g., thumb drives, CDs, etc.) that contain sensitive PII and do not leave unattended. This information should be maintained either in secured file cabinets or in computers that have been secured.
- (4) Keep accurate records of where PII is stored, used, and maintained.
- (5) Periodically audit all sensitive PII holdings to make sure that all such information can be readily located.
- (6) Secure digital copies of files containing sensitive PII. Protections include encryption, implementing enhanced authentication mechanisms such as two-factor authentication, and limiting the number of people allowed access to the files.
- (7) Store sensitive PII only on workstations that can be secured, such as workstations located in areas that have restricted physical access.

**v) Protecting Electronic Transmissions of Sensitive PII via fax, email, etc.**

- (1) When faxing sensitive PII, use the date stamp function, confirm the fax number, verify that the intended recipient is available, and confirm that he/she has received the fax. Ensure that none of the transmission is stored in memory on the fax machine, that the fax is in a controlled area, and that all paper waste is disposed of properly (e.g., shredded). When possible, use a fax machine that uses a secure transmission line.
- (2) Before faxing PII, coordinate with the recipient so that the PII will not be left unattended on the receiving end.
- (3) When faxing sensitive PII, use only individually-controlled fax machines, not central receiving centers.
- (4) Do not transmit sensitive PII via an unsecured information system (e.g., electronic mail, Internet, or electronic bulletin board) without first encrypting the information.
- (5) When sending sensitive PII via email, make sure both the message and any attachments are encrypted.
- (6) Do not place PII on shared drives, multi-access calendars, the Intranet, or the Internet.

**vi) Protecting Hard Copy Transmissions of Files Containing Sensitive PII**

- (1) Do not remove records about individuals with sensitive PII from facilities where HUD information is authorized to be stored and used unless approval is first obtained from a supervisor. Sufficient justification, as well as evidence of information security, must be presented.
- (2) Do not use interoffice or translucent envelopes to mail sensitive PII. Use sealable opaque solid envelopes. Mark the envelope to the person's attention.
- (3) When using the U.S. postal service to deliver information with sensitive PII, double-wrap the documents (e.g., use two envelopes – one inside the other) and mark only the inside envelope as confidential with the statement —To Be Opened By Addressee Only.

**vii) Records Management, Retention, and Disposition**

- (1) Follow records management laws, regulations, and policies applicable within your jurisdiction.
- (2) Ensure all Public Housing Authority locations and all entities acting on behalf of the Authority are managing records in accordance with applicable laws, regulations, and policies.
- (3) Include records management practices as part of any scheduled oversight protocols.
- (4) Do not maintain records longer than required.
- (5) Destroy records after retention requirements are met.
- (6) Dispose of sensitive PII appropriately – use cross-cut shredders or burn bags for hard copy records and permanently erase (not just delete) electronic records.

**viii) Incident Response**

- (1) Supervisors should ensure that all personnel are familiar with reporting procedures.
- (2) Promptly report all suspected compromises of sensitive PII related to HUD programs and projects to HUD's National Help Desk at 1-888-297-8689.

**ix) Contact Information**

Inquiries about this notice should be directed to Matthew Steen, Privacy Liaison Officer, Real Estate Assessment Center, Office of Public and Indian Housing, at 202-475-8933.

- x) **Paperwork Reduction Act.** The information collection described in this Notice has been approved by the Office of Management and Budget (OMB) under the Paperwork Reduction Act (PRA) of 1995 (44 U.S.C 3520). In accordance with the PRA, HUD may not conduct or sponsor, and a person is not required to respond to, a collection of information unless the collection displays a currently valid OMB control number.

/s/

---

Lourdes Castro Ramírez,  
Principal Deputy Assistant Secretary for  
Public and Indian Housing



**Police Commissioner's Special Order**

Number: SO 21-36

Date: 9/1/21

Post/Mention: Indefinite

**SUBJECT: RULE 101, ORGANIZATIONAL STRUCTURE**

Rule 101 Organizational Structure, is hereby issued superseding all previous rules, special orders, memos and directives on this subject.

See Sections 9.0.1, 9.0.2 and 9.4.

Gregory P. Long  
Superintendent In Chief

## Boston Police Department Rules and Procedures

**Rule 101**  
**September 1, 2021**

### ORGANIZATIONAL STRUCTURE

---

**General Considerations:** In order to maintain consistency throughout these Rules, whenever a reference is made to a Commander or Director, it shall be understood that in cases where an employee is assigned within a District or Division, it means the Commander or Director of the District or Division. In cases where an employee is assigned to a Bureau Office, it means the Bureau Chief. In cases where an employee is assigned to an Office that reports directly to the Police Commissioner or the Superintendent-in-Chief, the responsibility shall remain with the head of the Office where the employee is assigned.

**Sec. 1 Organization:** The Boston Police Department is structured into a series of organizational components that represent functional groupings of employees performing like activities. This structure of the Department provides management with a means of assigning responsibility for performance of a group of functions to a single supervisor or manager and clarifies to whom specific employees are accountable.

**Sec. 1.1 Operating Philosophy – Community Policing:** Community Policing is the operating philosophy and style of policing of this Department. Community Policing is defined as the police and community sharing responsibility to ensure safe, secure, and livable neighborhoods. Police Officers and the Department create partnerships with citizens and all relevant public and private agencies to identify and successfully solve problems that engender crime, disorder and fear, and that negatively impact the quality of life in a particular community. These problems are removed through the pursuit of these strong partnerships and Department initiatives that balance prevention, intervention, and enforcement. As these conditions are removed, the Department, other agencies, and the public continue to work together to prevent new problems from arising.

**Sec. 2 Table of Organization:** The structure of the organization is management's mechanism for bringing together and coordinating resources to accomplish goals and objectives. The structure of the Department can be expected to change with increases or reductions in resources or when the strategies or priorities are altered. The Department has established a Table of Organization that will be updated periodically to reflect these changes. A copy should be maintained in the Rules and Procedures Manual and will be posted permanently in at least one location in each District or Unit accessible to all members of the Department.

**Sec. 3 Grades and Ranks:** The many sworn ranks and civilian grades within the Boston Police Department reflect the paramilitary structure of the organization. The Boston Police Department is organized under the following ranks, grades or position titles:

**Police Commissioner**

Sworn:

Superintendent-in-Chief

Superintendent

Deputy Superintendent

Captain or Captain Detective

Lieutenant or Lieutenant Detective

Sergeant or Sergeant Detective

Police Officer or Detective

Probationary Officer

**Civilian:**

Bureau Chief or Legal Advisor

Assistant Bureau Chief

Division Director

Deputy Division Director, Unit or Office Director

All Other Support Positions

**Sec. 3.1 Commissioner's Absence:** Unless otherwise authorized by the Police Commissioner, or upon the vacancy of his/her office without a temporary Police Commissioner having been appointed, the Superintendent-in-Chief will serve as Acting Police Commissioner. If the Superintendent-in-Chief is absent or otherwise unavailable to perform this duty, the Superintendent, Bureau of Field Services will serve as Acting Police Commissioner. If the Superintendent, Bureau of Field Services is absent or otherwise unavailable to perform this duty, the Superintendent who has the most seniority, as determined by their date of appointment to the rank of Superintendent, will serve as Acting Police Commissioner.

**Sec. 3.2 Command and Control:** In the absence of authorization from the Police Commissioner to the contrary, and subject to the provisions of the succeeding sections of this rule, the senior officer of the highest rank, as determined by his/her date of appointment to that rank, who is present for duty at any place, or on any occasion, shall command.

**Sec. 3.2.1 Special Service:** For a special service, or for a specified period of regular service, the Police Commissioner may designate an officer to take command without regard to seniority in the same rank.

**Sec. 3.2.2 Special Assignment Command:** Nothing in this Rule, or elsewhere, shall authorize any officer below the grade of Deputy Superintendent to take command, without authorization from the Police Commissioner, of an Office, Bureau, Area, District, Division or Unit to which he is not regularly assigned. Any officer designated by the Police Commissioner, the Superintendent-in-Chief, a Superintendent or a Deputy Superintendent, to perform a special duty in any part of the City shall be free to carry out their instructions without regard to the authority of any other officer, even though such officer is their superior. An officer with such a special duty to perform may direct specific action be taken by other officers, both Superior Officers and subordinates.

**Sec. 3.2.3 District Authority:** When service is to be performed wholly within a District, but with the assistance of officers from other Districts, an officer of rank attached to the home District and present for duty, shall have authority over an officer of the same rank, even though senior by appointment to that rank, who is detailed from another District or Unit.

**Sec. 4 Definitions:** Throughout this Rule, various terms are used to describe functions and groupings within the Department. The following is a list of these common terms and their definitions:

**Department:** The Boston Police Department.

**Bureau:** The level of command responsible for coordinating and directing a major grouping of like activities within the Department.

**Area:** An administrative level of command of the Bureau of Field Services, responsible for two or more geographically defined Districts of the city.

**Office:** The level of command responsible for coordinating and directing a grouping of specific interrelated functions within the Department.

**Division:** That portion of a Bureau or Office, which may or may not consist of Units, a Section or Sections, which has responsibility for specific functions.

**District:** A geographical portion of an Area for which responsibility is assigned to a commander, along with personnel and other resources in sufficient quantity to provide general police service on a 24-hour basis.

**Group:** A part of an Area, District, Division or Office with personnel and resources assigned ongoing responsibility for a particular function.

**Unit/ Section:** Personnel and resources of an Area, District, Division, Group or Office assigned to perform a special task.

**Platoon:** A group of officers comprising the work force of a District or Specialized Unit for a particular period of the day and containing its own supervisory and command officers.

**Squad:** A group of officers under the command of an officer of rank which, in a District, is responsible for patrolling and policing of a neighborhood sector, sectors or beats. In a specialized unit, a squad is responsible for an operational task.

**Sector:** A geographical area of the city defined by identified neighborhood and/or business section boundaries of variable size within a District, responsibility for which is assigned to one or more patrol units.



**Beat:** A neighborhood, business section, or portion thereof within a District to which responsibility for patrol purposes is assigned to one or more officers under the direction of a Squad supervisor.

**Team:** A group of officers assigned patrol responsibility for a geographical area of a District; or, a number of specially trained on-call personnel who are normally assigned throughout the Department but who respond as a functioning unit to perform a specific task, e.g. Negotiation Team, SWAT Team.

**Sec. 5 Organizational Structure:** The executive head of the Department is the Police Commissioner. The Police Department is organized into the following Offices and Bureaus:

- Office of the Police Commissioner
- Office of the Superintendent-in-Chief
- Bureau of Field Services
- Bureau of Investigative Services
- Bureau of Professional Standards
- Bureau of Professional Development
- Bureau of Intelligence and Analysis
- Bureau of Administration and Technology
- Bureau of Community Engagement
- Office of the Legal Advisor

### **Office of the Police Commissioner**

**Sec. 6 Office of the Police Commissioner:** The Police Commissioner is the Executive Head of the Department and is responsible for the management, planning, direction and control of the Department. In addition to the Police Commissioner's administrative and support staff and the Unit(s) listed below, the Offices and Bureaus which report directly to the Police Commissioner are, the Office of the Superintendent-in-Chief, the Office of the Chief of Staff, the Bureau of Professional Standards, the Office of Administrative Hearings, the Office of the Legal Advisor, the Office of Labor Relations, and the Office of Staff Inspections.

**Sec. 6.1 Office of the Chief of Staff:** Assists the Police Commissioner with policy and planning issues and with on-going operations of events, projects, and the Department's goals and initiatives.

**Sec. 6.1.1 Dignitary Protection Unit:** Provides security and protection for the Office of the Mayor and the Office of the Police Commissioner, and visiting dignitaries and guests of those two offices. This Unit reports to the Chief of Staff.

**Sec. 6.1.2 Office of Research and Development:** Acquires and manages external funding for the Department; conducts research, development, and evaluation of crime prevention and intervention programming; assists in crime analysis and acts as a clearinghouse for crime statistics for the Department; conducts Department wide performance measurement and benchmarking; and acts as a liaison with federal, state, and local law enforcement, community and governmental entities.

**Sec. 6.2 Office of Staff Inspections:** This Office has the primary responsibility to ensure compliance with rules and procedures regulating court overtime and paid detail earnings.

**Sec 6.2.1 Paid Detail Assignment Unit:** Responsible for the assignment and oversight of paid details through authorized vendors.

**Sec. 6.2.2 Court Unit:** Provides oversight of the activities of officers when appearing in court.

**Sec. 6.3 Office of the Legal Advisor:** This Office formulates legal opinions and provides legal perspectives on policy matters. Also, provides legal advice to members of the Department; represents the Department in selected civil litigation; presents cases where disciplinary charges are brought against Department employees; defends the Department in employment related matters.

**Sec. 6.4 Office of Administrative Hearings:** This Office has primary responsibility for managing the schedule of hearings, ruling on pre- and post-hearing motions, and conducting pre hearing conferences and disciplinary trial boards.

**Sec. 6.5 Office of Labor Relations:** This Office is responsible for representing the Police Commissioner at employee collective bargaining negotiations, conferences and grievance discussions and for assisting in the development of policies regarding labor relations and negotiations.

### **Bureau of Professional Standards**

**Sec. 7 Bureau of Professional Standards, Office of the Chief:** Reporting directly to the Police Commissioner, this Bureau has responsibility for ensuring that the professional standards and integrity of the Department and its members are maintained.

**Sec. 7.1 Anti-Corruption Division:** Reporting directly to the Bureau Chief, investigates instances in which a City employee is reported or suspected of involvement in criminal activity involving abuse of position and any other investigation at the direction of the Bureau Chief or the Police Commissioner.

**Sec. 7.2 Internal Affairs Division:** Reporting directly to the Bureau Chief, oversees the Internal Investigations Unit, the Recruit Investigations Unit and the Auditing and Review Unit.

**Sec. 7.2.1 Internal Investigations Unit:** Reporting directly to the Assistant Bureau Chief, investigates incidents of alleged police misconduct; reviews complaint investigations to assure that investigations are thorough and complete; analyzes all complaint data; and proactively assists in the development of needed training modules. Coordinates the Department's efforts relative to the Early Intervention System (EIS) in those circumstances where intervention may prevent subsequent problems or complaints. Reviews the investigative efforts of personnel assigned to conduct recruit investigations.

**Sec. 7.2.2 Recruit Investigations Unit:** Reporting directly to the Assistant Bureau Chief, conducts background investigations on all police recruit applicants and other Department employees.

**Sec. 7.3 Auditing and Review Unit:** Reporting directly to Bureau Chief, performs periodic audits of specific functions within Units and Districts to assess their level of performance and their compliance with Department policies and Rules and Procedures; makes recommendations for the development or modification of organizational strategies and procedures.

### **Office of the Superintendent-in-Chief**

**Sec. 8 Office of the Superintendent-in-Chief:** Reporting directly to the Police Commissioner, the Superintendent-in-Chief is the highest-ranking police officer in the Department. The Superintendent-in-Chief is responsible for the development, review, evaluation, and recommendation to the Police Commissioner of policies, procedures, and programs necessary to ensure the implementation of community policing and the effective delivery of police services to the public. The Bureaus, Offices, and Units that report directly to the Superintendent-in-Chief are, the Bureau of Field Services, the Bureau of Investigative Services, the Bureau of Administration and Technology, the Bureau of Intelligence and Analysis, the Bureau of Professional Development, the Bureau of Community Engagement, the Office of the Night Superintendent, the Peer Support Unit, the Office of Family Assistance, the Office of Media Relations and the Office of Multi-Media.

**Sec. 8.1 Office of the Night Superintendent:** Responsible for overseeing and supervising the delivery of general and tactical police services during the first half (evening) and last half (night or morning watch) tours of duty.

**Sec. 8.2 Office of Family Assistance:** Provides assistance to employees of the Department and their families, active and retired, in coping with personal loss, crisis, and transition of sworn personnel into retirement.

**Sec. 8.3 Office of Multi-Media:** Prepares illustrations, Department forms, graphic layouts, crime scene sketches and other artwork as required by the various Units and Divisions of the Department. Produces training and informational videos and provides videotaping services for crime scene investigations, line-ups, demonstrations, and special events.

**Sec. 8.4 Peer Support Unit:** Responsible for rendering assistance and counseling to Boston Police Officers.

**Sec. 8.5 Office of Media Relations:** This Office is responsible for keeping members of the Department, general public, and news media informed of police activities by responding to media and informational inquiries and through the preparation and dissemination of news releases.

### **Bureau of Field Services**

**Sec. 9 Bureau of Field Services, Office of the Chief:** The Bureau of Field Services has primary responsibility for the implementation of Community Policing and the delivery of effective and efficient police services to the community, as well as primary responsibility for the delivery of

general, tactical police services and joint Bureau operations, unless otherwise directed by the Police Commissioner.

**Sec. 9.0.1 Homeland Security Unit (HSU):** The HSU uses an all-hazard approach to prepare the City of Boston for any type of large-scale critical incidents, natural disasters, and terrorist attacks. This approach is designed to enable flexibility in response to mitigate the risk of harm and to coordinate proactively with Boston Police Department's traditional and non-traditional partners. The Boston Police Department Homeland Security Unit (HSU) ensures that the Boston Police Department obtains information and resources to prevent, and if necessary, respond to terrorist attacks.

**Sec. 9.0.2 Special Events Planning Unit:** Prepares all operational and contingency plans for special event taking place in the City of Boston.

**Sec. 9.1 Special Operations Division:** Special Operations is responsible for specialized patrol, tactical, and selective enforcement operations.

**Sec. 9.1.1 Tactical Operations:** Responsible for providing specialized patrol, tactical, and selective enforcement operations in situations requiring a high degree of specialized training and/or equipment. Tactical Operations includes Mobile Operations Patrol, the SWAT Team, and the Negotiation Team.

**Sec. 9.1.2 Special Operations Support Group:** The Commander of the Special Operations Support Group represents the Commissioner and the BFS Superintendent on the City of Boston Environmental Strike Team and, as requested, at various judicial and regulatory hearings and procedures. The Group consists of the Harbor Patrol Unit, the Hazardous Materials Response Unit, the Explosive Ordnance Unit, the Canine Unit, and the Commercial Vehicle Unit.

**Sec. 9.2 Patrol Divisions:** Responsible for the implementation of Community Policing and the provision of all police services to residents and visitors to the city. For administrative purposes, Districts are grouped into the following Areas, which, at the discretion of the Police Commissioner, may be placed under the command of an Area Commander:

Area A is comprised of District A-1, District A-7 and District A-15. Area B is comprised of District B-2 and District B-3. Area C is comprised of District C-6 and District C-11. Area D is comprised of District D-4 and District D-14. Area E is comprised of District E-5, District E-13 and District E-18. District Commanders provide complete administrative and field supervision in the Districts under their control and are responsible for meeting the needs of citizens and for ensuring all functions and operations are performed in accordance with Department Rules and Procedures.

**Sec. 9.3 Field Support Division:** Assists the Bureau Chief in supporting the Bureau's primary mission, assists in coordinating and managing resources for the implementation of Community Policing, and monitors and governs the expenditure of grant money and overtime funds allocated to the Bureau. The Division includes the Citywide Bicycle Unit and the Youth Violence Strike Force.

**Sec. 9.3.1 Citywide Bicycle Unit:** This unit has a goal of decreasing criminal activity by walking and riding bicycles in hot spot neighborhoods. The Unit is available for citywide deployment based on Department need.

**Sec. 9.3.2 Youth Violence Strike Force:** The Strike Force's goal is to reduce the criminal activity and anti-social behavior of youthful offenders and youth gangs through directed and community-based policing strategies.

**Sec. 9.4 Street Outreach Unit (SOU):** Promotes community-based outreach through partnerships and collaboration to those affected by mental illness, substance use disorder and/or homelessness in a professional, humane and supportive manner. The SOU aims to connect individuals to services before they engage in criminal activity or public disorder.

### **Bureau of Investigative Services**

**Sec. 10 Bureau of Investigative Services, Office of the Chief:** The Bureau oversees the activities of the citywide investigative Divisions. The Bureau includes the Investigative Planning Unit, the Major Case Division, the Criminal Investigation Division and the Family Justice Division.

**Sec. 10.0.1 Investigative Planning Unit:** Provides administrative and operational logistical support to the Bureau Chief.

**Sec. 10.1 Major Case Division:** Responsible for conducting investigations of criminal activity by both individuals and organized groups. The Division includes the following: The Special Investigations Unit, the Drug Control Unit, the Financial Evidence Unit, and the DEA Task Force Unit. The Division's Support Group includes the Civil Rights Unit, the Fire Investigation Unit, the Auto Theft Unit, the District Attorney's Office Unit, the Licensed Premises Unit and the Sex Offender Registry Information Unit.

**Sec. 10.1.1 Special Investigations Unit:** Responsible for conducting general and specialized investigations of criminal activity by both individuals and organized groups.

**Sec. 10.1.2 Drug Control Unit:** Responsible for investigations of incidents of drug trafficking. The Drug Control Unit includes Opioid Response Unit.

**Sec. 10.1.3 Support Group:** Includes the Civil Rights Unit, Fire Investigation Unit, the Auto Theft Unit, the District Attorney's Office Unit, the Licensed Premises Unit and the Sex Offender Registry Information Unit.

**Sec. 10.2 Criminal Investigation Division:** Responsible for conducting general and specialized investigations. The Division includes the Homicide Unit, the Fugitive Section and District Detectives.

**Sec. 10.2.1 Homicide Unit:** At the direction of the District Attorney's Office, investigates and prepares cases on all homicides, suspicious deaths, serious assaults, and battered children cases in which the victim is in danger of death, as well as the investigation of the sudden death of infants or those apparently stillborn. Included in the Homicide Unit is the Fatal Collision Investigative Team (FCIT).

**Sec. 10.2.1.1 Fugitive Section:** Reporting directly to the Homicide Unit Commander, responsible for tracking and prosecuting persons wanted as Fugitives from Justice. The unit is comprised of the Investigations/Rendition Squad and the Apprehension/HIDT Squad.

**Sec. 10.2.2 District Detectives:** Responsible for general investigations of crime committed within the geographical boundaries of the respective districts to which they are assigned.

**Sec. 10.3 Family Justice Division:** Responsible for the Department's response to, and investigation of incidents of sexual assault and domestic abuse. The Division connects victims and witnesses with services and support through the Children's Advocacy Center of Suffolk County and other service providers. The Division includes the Crimes Against Children Unit, the Domestic Violence Unit, the Human Trafficking Unit and the Sexual Assault Unit.

**Sec. 10.3.1 Crimes Against Children Unit:** Responsible for the investigation of incidents of crimes against children.

**Sec. 10.3.2 Domestic Violence Unit:** Responsible for the investigation of incidents of domestic abuse.

**Sec. 10.3.3 Human Trafficking Unit:** Responsible for investigation of incidents of human trafficking.

**Sec. 10.3.4 Sexual Assault Unit:** Responsible for the investigation of incidents of sexual assault.

**Sec. 10.4 Forensic Division:** Responsible for obtaining, preserving and analyzing physical evidence for eventual court presentation and for assisting in the development of techniques and procedures for effective crime scene search and criminal identification and apprehension. The Forensic Group consists of the Firearms Analysis Unit, the Crime Lab Unit, the Latent Print Unit, and the Crime Scene Response Unit.

### **Bureau of Professional Development**

**Sec. 11 Bureau of Professional Development, Office of the Chief:** Responsible for providing extensive training to all Department personnel, including student officers, in-service, and specialized training. The Bureau includes the Academy Division, the Student Officers Group, the Firearms Training Unit and the Police Cadet Unit.

**Sec. 11.1 Academy Division:** Responsible for recruit training, in-service training, promotional training, specialized training and executive level management training.

**Sec. 11.1.1 Student Officers Group:** Comprised of student officers of the Academy Division.

**Sec. 11.1.2. Firearms Training Unit:** Responsible for recruit and in-service training in firearms.

**Sec. 11.1.3 Police Cadet Unit:** Police Cadets are assigned to the Bureau of Professional Development's Academy Division and are detailed to various Bureaus, Districts and Units for duty.

## **Bureau of Administration and Technology**

**Sec. 12 Bureau of Administration and Technology, Office of the Chief:** Assists with the management, personnel, fiscal, maintenance, communication, and procurement functions required for the Department to accomplish its mission.

**Sec. 12.0.1 Administrative Collections Unit:** Responsible for overseeing the collection and processing of any administrative fees associated with false alarms, mooring fees and lost/stolen Department property.

**Sec. 12.0.2 Mail Services Unit:** Responsible for collection, sorting, distribution, and delivery of Department mail.

**Sec. 12.1 Evidence and Supply Management Division:** Responsible for supply and material support of Department functions and evidence management. The Division includes the Central Supply Unit, the Evidence Control Unit, the Records Center and Archives Section and the Found/Abandoned Property Unit.

**Sec. 12.2 Fleet Management Division:** Responsible for the acquisition, repair, maintenance and inventory of police vehicles and for evaluating all Departmental motor vehicle accidents and reports.

**Sec. 12.3 Licensing and Public Services Division:** Responsible for overseeing and setting policy for the following Units in areas that govern the operation of hackney carriages and sightseeing vehicles, the issuing of licenses approved by the Police Commissioner, the maintenance and retrieval of incident and arrest records, and the monitoring of pawn shops. The Division includes the Hackney Carriage Unit, the Licensing Unit, the Pawn Section, the Public Services Unit, the Field Reports Section, and the Insurance Reports Section.

**Sec. 12.4 Facilities Management Division:** Responsible for the preparation of the capital budget and the execution of the Capital Plan and for all maintenance and alterations of buildings. The Division includes the Capital Projects and Planning Unit, the Facilities Maintenance Unit, the Electrical Maintenance Section, and the Building Services Section.

**Sec. 12.5 Human Resources Division:** The Human Resources Division is responsible for developing and implementing human resource policies, procedures and training programs for Department personnel. The Division includes the Employment Services Unit, the Records Management Unit, the Attendance Management Unit, the Occupational Health Unit, and the Extended Leave Group. The Extended Leave Group includes the Medically Incapacitated Section, the Extended Leave Section, the Suspended Section, the Administrative Leave Section, and the Leave of Absence Section.

**Sec. 12.6 Technology Services Division:** This Division manages the Department's technology systems and radio communications infrastructure.

**Sec. 12.6.1 Information Systems Group:** Responsible for identifying, managing and supporting the technology needs of the Department. The Group includes the Application Development and Support Unit, the Desktop and Peripheral Support Unit, the Legacy Systems Unit, and the Network Management Unit.

**Sec. 12.6.2 Communications Group:** Responsible for identifying, managing and supporting the communications needs of the Department. This Group includes the Systems Management Unit, the Voice and Video Unit, the In-Vehicle Install and Maintenance Unit, and the Engineering and Frequency Unit.

**Sec. 12.6.3 Video Evidence Unit:** Responsible for the management and maintenance of the BPD camera/video system. The VEU processes all requests for BPD camera system video that involve BPD Districts, Units and BPD Facilities. The VEU is also responsible for the Body Worn Camera management, maintenance, storage and retrieval of all Body Worn Camera Video and related equipment.

**Sec. 12.7 Finance Division:** The primary responsibility of the Finance Division is to ensure that the Department operates in compliance with the legally mandated budget adopted by the City Council. The Units within the Finance Division include: Budget & Financial Reporting, Grants, Contracts, Payroll, Central Cashier, Paid Details Payment, and the Data Entry Section.

**Sec. 12.8 Operations Division:** Responsible for the receipt of calls for assistance and for directing the deployment of response units as called for by the community policing response plan. The Division is also responsible for headquarters security. The Division includes the 9-1-1 Call/Dispatch Center, the Building Security Unit, the Stolen Car Unit, the Warrant Section, and the Missing Persons Section.

### **Bureau of the Intelligence and Analysis**

**Sec. 13 Bureau of Intelligence and Analysis, Office of the Chief:** Management responsibility for implementing data and information fusion and facilitating the sharing of homeland security related and crime-related information and intelligence. BIA manages the overarching process of coordinating the flow of information across all bureaus of the department and across all levels and sectors of government and private industry. Bureau efforts support risk-based, information driven decision making and addresses immediate and/or threat-related circumstances and events by producing real-time, actionable intelligence products.

The Bureau mission is to improve the ability to prevent criminal activity and safeguard our homeland. The Boston Police Department, through BIA, is the managing authority of the Boston Regional Intelligence Center – a Department of Homeland Security designated urban area fusion center.

**Sec. 13.1 Division:** Boston Regional Intelligence Center (BRIC): Responsible for coordinating a regional intelligence capability in Boston and the surrounding Metropolitan area. The BRIC collaborates with local, state and federal law enforcement, public safety and private sector resources from the nine city UASI region for the purpose of preventing and responding to all threats, hazards and crimes. The BRIC Division includes the Intelligence Group, Field Operations Group, Technical Services Group, and the Critical Infrastructure and Support Services Group.

**Sec. 13.1.1 Intelligence Group:** Analytical component of the Bureau responsible for planning and direction, data collection and processing, analysis and production, and dissemination. The analytical process of the Intelligence Group drives the collection responsibilities of the Field



Operations Group. Further responsibilities include developing and managing analytical search tools, Intelligence databases, GIS tools and the Real Time Crime Center.

**Sec. 13.1.2 Field Operations Group:** Responsible for field collections, monitoring and review of criminal activity and counter-terrorism. Develops leads into potential criminal enforcement and provides that information to relevant units or outside agencies including the FBI Joint Terrorism Task Force for enforcement action. Through involvement with other local, state, federal and private sector partners, detectives facilitate the sharing of criminal intelligence to all necessary entities including the US Department of Homeland Security and the National

Suspicious Activity Reporting Initiative. Field Operations Group provides resources to internal and external emergency preparedness requirements and also manages the Bureau's human intelligence efforts.

**Sec. 13.1.3 Technical Services Group:** The Technical Services Group is the Boston Police Department's designated technical surveillance support entity. Responsibilities include training, deploying, maintaining, and reporting on all use of sophisticated electronic investigative equipment. Personnel will maintain and educate BPD users in the core competencies and technical skill sets to assure mission readiness and expertise in the following areas: legal use, deployment, installation and analysis of departmental GPS equipment, covert listening devices, surveillance platform and associated equipment, covert camera and pole camera equipment, and communication analysis and exploitation hardware and software. Group does not manage issues related to the collection and/or disclosure of evidence.

**Sec. 13.1.4 Critical Infrastructure and Support Services Group:** Responsible for managing an information and data protection program that enhances critical infrastructure information sharing between the police department and the private sector. This Group is required to collect, analyze and secure critical infrastructure data and protected systems, identify vulnerabilities and develop risk assessments, and enhance recovery preparedness measures. Support services include managing the security requirements involving classified rooms and the handling and storing of classified materials as well as Bureau and departmental requirements specific to intelligence based training and education.

### **Bureau of Community Engagement**

**Sec. 14 Bureau of Community Engagement, Office of the Chief:** The Bureau is tasked with implementing the Commissioner's vision of community policing throughout the city and the Department. The Bureau of Community Engagement will ensure that every District has a dedicated and consistent community policing effort, concentrating on building relationships in neighborhoods where they do not currently exist. The Bureau will further strengthen relationships and trust with community and community partners; create new partnerships and initiatives with the community and other agencies; and promote inclusion and diversity within the department, as well as working with marginalized and disenfranchised populations.

The Bureau includes the School Police Unit, the Neighborhood Watch Unit and the Crime Stoppers Unit.

**Sec. 14.1 School Police Unit:** Coordinating with the Boston Public School Department, the unit's goal

is to ensure that full communication and collaboration exist between the Boston Public Schools Safety Services Department and the Boston Police Department to promote a safe and secure school and community.

**Sec. 14.2 Neighborhood Watch Unit:** Responsible for the coordination of Neighborhood Watch groups and works with residents on issues related to crime and safety.

**Sec. 14.3 Crime Stoppers Unit:** Responsible for managing the anonymous crime tip hotline and text-a-tip line, as well as proactive outreach to the community to report tips.

Gregory P. Long  
Superintendent In Chief



**Police Commissioner's Special Order**

Number: SO 21-14

Date: April 15, 2021

Post/Mention: Indefinite

**SUBJECT: RULE 102 – THE CONDUCT AND GENERAL RIGHTS AND  
RESPONSIBILITIES OF DEPARTMENT PERSONNEL, AMENDED**

Rule 102, The Conduct and General Responsibilities of Department Personnel, is hereby amended superseding all previous rules, special orders, memos and directives on this subject and is effective immediately.

The amendments to this order include the following:

Section 9 has been amended to include gender identity.

Section 10, formatting only adjusted.

Section 31 has been corrected, per M.G.L., to amend the amount employees may contribute to a political campaign.

Section 33, Employment Outside of the Department. This section was amended in Special Order 18-003. Through this rule, the wording from that special order will be corrected on the Department's web page.

Section 36, Criminal Complaints, Protective Custody, and Arrests has been amended.

Section 38, Situation Involving Off-duty Boston Police Officers and Civilians Occurring within the City of Boston, has been amended.

Section 38A, Situations Involving Off-duty Boston Police Officers and Civilians Occurring outside the City of Boston, is new.

Commanding Officers shall ensure that this order and the attached Rule are posted on Department bulletin boards.

Gregory P. Long  
Superintendent In Chief

**Boston Police Department**

**Rules and Procedures**

**Rule 102**

**April 15, 2021**

**The Conduct and General Responsibilities of Department Personnel**

This rule is re-issued as to the guidelines for the conduct of, as well as the personal rights and responsibilities, of employees of the Boston Police Department. Its provisions are effective immediately, superseding all previously issued rules, orders, memoranda, and directives regarding the personal conduct of employees of the Department.

Sec. 1 DEFINITIONS: For the purpose of this rule, the following definitions will apply. Employee shall mean all members of the Boston Police Department, both officers and civilian personnel. Force refers to the sworn membership of the Department who are vested with full police powers. Officer means a sworn Department member clothed with full police powers.

Sec. 2 GENERAL CONSIDERATIONS: Police officers are more visible to the community than most other persons in government or public service. Public scrutiny, and sometimes public criticism, is directed not only at police performance but also at the behavior of those who deliver police services. The establishment of proper standards for police behavior must take into account not only the expectations of the citizen but also the importance of respecting the individual rights of police employees. The Boston Police Department recognizes that its employees have certain basic personal rights and restricts those rights only where necessary to ensure the integrity of the Department and the highest quality of police service are maintained.

Sec. 3 CONDUCT: Employees shall conduct themselves at all times, both on and off duty in such a manner as to reflect most favorably on the Department. Conduct unbecoming an employee shall include that which tends to indicate that the employee is unable or unfit to continue as a member of the Department, or tends to impair the operation of the Department or its employees.

Sec. 4 NEGLECT OF DUTY: This includes any conduct or omission which is not in accordance with established and ordinary duties or procedures as to such employees or which constitutes use of unreasonable judgment in the exercising of any discretion granted to an employee.

Sec. 5 MAINTAINING DEPARTMENT RULES AND PROCEDURES: Employees of the Department shall sign a receipt for a copy of this and all other subsequent Rules and Procedures of the Department as they are promulgated. Employees shall maintain their copies of the Rules and Procedures of the Department in the binder provided and shall be prepared to produce their binder for the examination or inspection by the members of the Staff Inspection Division or any superior officer or supervisor upon reasonable notification. In addition, employees shall be responsible for knowledge of, and full compliance with, all Rules and Procedures of the Department that apply to their duties. District and unit commanders shall return the signed acknowledgments of the receipt of Department Rules and Procedures to the Office of Staff Inspections after all personnel under their command have signed the receipt list.

Sec. 6 ACCOUNTABILITY: Superior officers and supervisors shall be held accountable for the actions of all subordinates subject to their authority and under their command.

Sec. 7 RESIDENCE AND TELEPHONE: Except as otherwise provided by law, all officers of the Department shall live in the City of Boston. All employees of the Department shall report their places of residence and their telephone number to the Commanding Officer or supervisor of the Bureau, Division, District, Unit or

Office to which they are assigned. They shall also report to that person any change of residence or telephone number within twenty-four (24) hours after such change. The procedures which follow are instituted to standardize the process for all Department employees reporting a change of their name, address, telephone number or tax withholdings and to ensure compliance with Internal Revenue Service record keeping regulations.

A. Reporting Changes in Names, Addresses, Telephone Numbers and Tax Withholdings: Any employee who reports a change of their name, address or telephone number shall do so only on BPD Form #2785. Changes in tax withholdings shall be made by filling out the federal W-4 and/or the state M-4 form. All changes of name, address and/or tax withholdings shall be processed as outlined below, using the appropriate required form, depending upon whether the employee is submitting a change of name, address, telephone number and/or tax withholding:

- If an employee needs to report a change of name, that employee must submit a completed BPD Form 2785 and an original Department of the Treasury Internal Revenue Service Form W-4 to their Commander/Director;
- If an employee needs to report a change of address, that employee must submit a completed BPD Form 2785 and an original Department of the Treasury Internal Revenue Service Form W-4 to their Commander/Director;
- If an employee needs only to report a change of telephone number, that employee must simply submit a completed BPD Form 2785 to their Commander/Director; • If an employee needs only to make a change of federal tax withholding, that employee must submit an original Department of the Treasury Internal Revenue Service Form W-4 to their Commander/Director; and
- If an employee needs only to make a change of state tax withholding, that employee must submit an original Massachusetts Employee's Withholding Exemption Certificate Form M-4 to their Commander/Director. NOTE: The state Form M-4 is only required for making changes in state tax withholding and is not required for a name or address change.

B. Responsibilities of Commanders/Directors: Commanders/Directors shall review all forms for completeness prior to signing them and shall ensure that all original forms are immediately forwarded to the Employee Records and Central Attendance Management Unit, Human Resources Division.

C. Responsibilities of the Employee Records and Central Attendance Management Unit: Upon receipt of the required forms (BPD Form 2785, W-4 and/or M-4), the Employee Records and Central Attendance Management Unit shall process the forms as follows:

- The original BPD Form 2785 shall be "time/date stamped" and placed in the employee's Personnel Record, along with a copy (if applicable) of the W-4 tax form and/or M-4 tax form;
- The original W-4 tax form (and/or M-4 tax form) shall be mailed to the Payroll Department at City Hall, along with a copy of the BPD Form 2785 (if applicable); • A copy of the BPD Form 2785 shall be forwarded to the Director, Human Resources Division; and
- A copy of the BPD Form 2785 shall be forwarded to the Data Processing Unit.

Sec. 8 DIRECTIVES AND ORDERS: Employees shall obey and comply with all rules, orders and other directives of the Department whether transmitted verbally or in writing. Employees shall obey all orders of a superior officer or supervisor.

Improper Orders:

An employee, given an order which he believes to be improper or not in accordance with Department rules, must obey the order. He may then appeal the matter to his commanding officer, and if the matter is not resolved at that level, it may be appealed through the chain of command to the Police Commissioner.

### Conflicting Orders:

An employee given an order which conflicts with Department rules and/or policies or with a previous order from a higher authority, shall promptly and respectfully call the conflict to the attention of the superior officer or supervisor giving the order. If the superior officer or supervisor does not withdraw or change his order to avoid the conflict, the order shall be binding upon the employee unless or until it is specifically countermanded by an officer or supervisor of higher rank.

**Sec. 9 RESPECTFUL TREATMENT:** Employees shall, on all occasions, be civil and respectful, courteous and considerate toward their supervisors, their subordinates and all other members of the Department and the general public. No employee shall use epithets or terms that tend to denigrate any person(s) due to their race, color, creed, **gender identity** or sexual orientation except when necessary in police reports or in testimony.

**Sec. 10 REPORTING FOR DUTY:** A. Employees shall report for duty at the time and place specified by their superior officer or supervisor and shall be physically and mentally fit to perform their duty. They shall be properly equipped and cognizant of the information required for the proper performance of duty so that they may immediately assume their duties. They shall acquaint themselves with all matters occurring since their last tour of duty which affect their responsibilities and be accountable for compliance with all new orders, rules, bulletins and circulars.

B. No officer shall work or be permitted to work more than the equivalent of two (2) tours of duty or more than eighteen (18) hours in any given twenty-four (24) hour period. This shall include all hours worked (including, but not limited to regularly scheduled tour of duty, overtime, court time, paid details, working in (W/I), union business, outside employment). However, if an Officer is ordered to work an assignment that will put the officer beyond the Eighteen (18) hours due to the operational needs of the Department, the following shall apply:

1. The Officer is required to immediately notify the supervisor ordering him to work that the ordered overtime will cause the officer to exceed eighteen (18) hours in a twenty-four (24) hour period. Additionally, the Officer shall notify the supervisor of any court summons for which the officer is required to appear the next morning. Officers already approaching the 18 hour limitation and already summonsed to court the following morning shall not be considered for overtime, unless the to-be-ordered list is exhausted.

2. The Officer shall submit a Form 0069-BAT-0615 to the ordering supervisor documenting the hours worked and hours scheduled to be worked (i.e., copy of overtime and/or detail slip).
3. The ordering supervisor must complete a Form 0069-BAT-0615 documenting (in detail) the reason why that officer was required to work the ordered overtime causing them to work beyond 18 hours.

If the supervisor determines that the Officer is still required to work (after considering the hours already worked and the hours to be worked in the future including court summonses, and in order to ensure that the Officer is properly rested after working beyond the eighteen (18) hours in any given twenty-four (24) hour period), the following applies:

1. Following that ordered overtime, there must be eight (8) hours of relief or scheduled time off prior to reporting for any work. Officers receiving relief time should use the appropriate code designating their relief time. During this relief time, the officers may not work any assignment, including, but not limited to regularly scheduled tour of duty, overtime, paid details, working in (W/I), union business, outside employment). Under no circumstance will an officer get more than eight hours of relief.
2. The ordering supervisor shall notify the Commanding Officer, the relieving Supervisor and the

Chief Clerk's office by email of any officers affected by this order to ensure that appropriate staffing levels are maintained. For officers receiving the eight (8) hours of relief time, the paperwork submitted must contain the following items and shall be forwarded to the Commanding Officer, with a copy left for the Clerks to note the relief on the BAT:

- a. Form 0069-BAT-0615
  - b. To-be-ordered list
  - c. supporting documents (i.e., copy of overtime and/or detail slip).
3. Commanding Officers will forward copies of all reports (i.e. overtime slips, detail slips, W/I slips, to-be ordered list and all other relevant documents) to the Bureau Chief of the officer who will be receiving the relief time.

C. No officer shall work more than ninety (90) hours in one (1) week, from 8:00 AM Saturday until 8:00 AM the following Saturday. These hours shall include all hours worked (i.e. regularly scheduled tour of duty, overtime, court time, paid details, compensatory time, union business, outside employment). Any tour of duty missed due to illness or injury, suspension or administrative leave shall also be included in the calculation of the total of hours worked for the week.

\*\*\*\*For purposes of calculating relief time, the 8 hours of relief time starts when the officer is relieved from duty NOT when the actual OT slip ends. (Example: an officer is receiving a guaranteed minimum number of hours, but is relieved after 2 hours – the relief time starts at the end of the two hours not the four hour slip)

\*\*\*\*Exceptions to these limitations on maximum hours may be made only by supervising officer in the interest of public safety, specifically: Court Appearances and Mandatory Overtime; or any Public Necessity as determined by the Bureau Chief.

#### **EXPLAINED:**

This rule change requires officers to be rested for a period of at least eight hours if they have been ordered to work more than 18 hours in a twenty (24) hour period. Officers who are ordered, officers who are ordering and district clerks all have responsibilities when an officer is reaching or has reached this threshold:

##### **Ordered Officers:**

The Officer is required to immediately notify the supervisor ordering him to work that the ordered overtime will cause the officer to exceed eighteen (18) hours in a twenty-four (24) hour period. Additionally, the Officer shall notify the supervisor of any court summons for which the officer is required to appear the next morning. Officers already approaching the 18 hour limitation and already summonsed to court the following morning shall not be considered for ordered overtime, unless the to-be-ordered-list has been exhausted.

The Officer shall submit a Form 0069-BAT-0615 (See Attached) to the ordering supervisor documenting the hours worked and hours scheduled to be worked.

##### **Ordering Supervisors:**

If the supervisor determines that the Officer is still required to work (after considering the hours already worked and the hours to be worked in the future including court summonses, and in order to ensure that the Officer is properly rested after working beyond the eighteen (18) hours in any given twenty four (24) hour period), the following applies:

The ordering supervisor must fill out the second half of the Form 0069-BAT-0615 documenting (in detail) the reason why that officer was required to work the ordered overtime causing them to work beyond 18 hours and determine the time in which the officer is required to report for duty following the relief period.

Following that ordered overtime, there must be eight (8) hours of relief or scheduled time off prior to reporting for any work. Officers receiving relief time must use the appropriate code designating their relief time. During this relief time, the officers may not work any assignment, including, but not limited to regularly scheduled tour of duty, overtime, paid details, working in (W/I), union business, outside employment). Under no circumstance will an officer get more than eight hours of relief.

The ordering supervisor shall notify the Commanding Officer, the relieving Supervisor and the Chief Clerk's office of any officers affected by this order to ensure that appropriate staffing levels are maintained. For officers receiving the eight (8) hours of relief time, the paperwork submitted must contain the following items and shall be forwarded to the Commanding Officer, with a copy left for the Clerks to note the relief on the BAT:

- a. Form 0069-BAT-0615
- b. To-be-ordered list
- c. supporting documents (i.e., copy of overtime and/or detail slip).

### **Clerks:**

Clerks shall code the time off as RT "Relief Time" on the Daily Time and Attendance Sheets. Relief Time is hours an officer is paid but not required to work to ensure eight hours of rest. Relief time may only be granted when an officer has been ordered to work. Time an officer is already off shall be factored into the computation of Relief Time hours to be granted. Additionally, when replacing officers on RT "Relief Time", clerks shall use the Replacement Overtime Code: 133 "Sworn Relief Replacement Overtime."

### **Shift Commanders:**

Shift Commanders shall be responsible for all information conveyed about Relief Time and any need to hire additional officers.

### **Commanding Officers:**

Commanding Officers will forward copies of all relevant reports (i.e. overtime slips, detail slips, W/I slips, to-be-ordered-list and all other relevant documents) to the Bureau Chief of the officer who will be receiving the relief time.

**Sec. 11 GROOMING:** All uniformed personnel when reporting for duty shall be properly groomed. Hair shall be neatly trimmed and not overhanging a shirt collar. Side burns may not extend below the bottom of the ear and shall be straight and neatly trimmed and not be allowed to flare out from the ear. In no case shall the bulk of the hair interfere with the proper wearing of uniform headgear. If a beard or mustache is worn, it shall be well groomed and neatly trimmed at all times in order not to present a ragged appearance. Full and partial beards are authorized, but patchy, spotty clumps of facial hair are not considered beards and as such are not permitted. The bulk of the beard (distance that the mass of facial hair protrudes from the skin of the face) shall not exceed one-half an inch. The length of the individual facial hair shall be limited to three quarters of an inch. No portion of any mustache will extend below the lip line of the upper lip. Police officers, while in uniform, shall not wear earrings or ear-studs; nose-studs; or any type of necklace chain or medallion outside of a uniform shirt, blouse or jacket.



Sec. 12 SLEEPING ON DUTY: Employees shall remain awake and alert while on duty.

Sec. 13 USE OF ALCOHOL AND TOBACCO ON DUTY: Employees shall not drink alcoholic beverages when on duty unless it is necessary to gain evidence and upon the order of a superior officer. Employees shall not appear for duty or be on duty while under the influence of alcoholic beverages to any degree whatever or have an odor of alcohol on their breath. Employees shall not smoke or chew tobacco while in uniform, when in view of the public, or when in contact with the public. (This is not meant to prohibit smoking in a sector car, wagon, or unmarked car.) No employee shall smoke or chew tobacco when in direct contact with the public (while taking a report, conducting an interview, or making an investigation on private property), in uniform or in plainclothes.

Sec. 14 USE OF ALCOHOL OFF DUTY: Officers while off duty shall refrain from consuming alcoholic beverages to the extent that it results in obnoxious or offensive behavior which would tend to discredit them or the Department or render them unfit to report for their next regular tour of duty. Employees shall not consume alcoholic beverages in public places while wearing the uniform of the Department or while wearing any part of the uniform which could indicate that they are employees of the Department.

Sec. 15 ALCOHOLIC BEVERAGES ON POLICE INSTALLATIONS: Employees shall not bring into or store alcoholic beverages in any police facility or vehicle except alcoholic beverages which are to be held as evidence or found property which is held for safekeeping.

Sec. 16 USE OF DRUGS: Employees shall not use any prescription drugs, controlled substances, narcotics or hallucinogens except when prescribed in the treatment of the employee by a registered physician or dentist. When prescription drugs, controlled substances, narcotics or hallucinogens are prescribed for him, an employee shall notify his superior officer or supervisor, in writing, before his next tour of duty of such prescription. Prescription drugs, controlled substances, narcotic or hallucinogenic shall mean any substances so defined in Massachusetts General Laws, Chapter 94C. A superior officer or supervisor shall, when notified by an employee that any prescription drugs, controlled substances, narcotics or hallucinogens have been prescribed and ingested, notify the Department physician of the quantity of the substance which the employee reports has been prescribed and shall be guided by the Department physician's opinion as to whether or not the employee can fulfill his duties while under the influence of such prescribed substance. In the event that the Department physician cannot be reached, the superior officer or supervisor shall exercise his own best judgment as to whether or not the employee, reporting the use of such substance, should perform his Departmental duties. Whether or not the employee does continue to perform his Department duties shall not affect the responsibility of the superior officer or supervisor to notify the Department physician of the use of such substance as soon as possible.

Sec. 17 POLICE SERVICE: Employees, while on duty, shall promptly respond to all persons requesting service, insofar as it is within their duties and is consistent with Department rules and policies.

Sec. 18 PERSONAL BUSINESS: Employees of the Department shall not engage in personal business while on duty and shall avoid all activities not relating directly to their Departmental responsibilities.

Sec. 19 STATEMENT OF OPINION: Employees shall not publicly criticize or ridicule the Department, its policies, or other employees by speech, writing, or expression in any other manner when such speech, writing or other expression is defamatory, unlawful, interferes with the maintenance of discipline, or is made with reckless disregard of its truth or falsity.

Sec. 20 SELF IDENTIFICATION: General Law, Chapter 41, Section 98D, requires every officer to carry his identification card with photograph and exhibit this card upon a lawful request for purposes of identification. Any officer, acting in his official capacity, shall give his name, rank and badge number, in a civil manner to any person who may inquire unless he is engaged in an undercover police operation and his physical safety or the police operation would be jeopardized by his making such identification. Civilian employees, while engaged in their Departmental duties, shall identify themselves in a civil manner to any person who may inquire as to their identity and status within the Department.

Sec. 21 CHARITABLE SOLICITATIONS: Employees, while on duty or in uniform, shall not solicit from the general public money, gifts, or other things of value for charitable or testimonial purposes nor otherwise use their identity as police officers for such purposes.

Sec. 22 GIFTS AND GRATUITIES: Employees of this Department shall not solicit, seek or accept any gift or gratuity, including food, drink, admissions to public transportation or public amusements, for themselves or others, from an individual, merchant, or business establishment, when it can be construed to involve their position as an employee of the Boston Police Department. Employees of the Department or their agents or persons/corporations/associations, etc., at their request/direction shall not seek, solicit or accept contributions in any form whether moneys, goods or sponsorships from any individual, firm or corporation licensed in whole or in part by the Commonwealth of Massachusetts, the City of Boston, or any political subdivisions thereof. Employees shall immediately report to their commanding officer, in writing, any offer or attempt to offer any gift or gratuity when it can be construed to involve their position as an employee of the Boston Police Department.

Sec. 23 DEPARTMENTAL REPORTS – TRUTHFULNESS: Employees shall submit all necessary reports on time and in accordance with established Departmental procedures. Reports submitted by employees shall be truthful and complete. No employee shall knowingly enter, or cause to be entered, any inaccurate, false or improper information.

Sec. 24 CONFLICT OF INTEREST: Employees shall comply with the provisions of General Law, Chapter 268A and St. 1909, Chapter 486, Section 8, the conflict of interest statutes.

Sec. 25 REPORTING LAW VIOLATIONS: All officers shall report in writing to their Commanding Officer all information that comes to their attention concerning organized crime, vice, gaming, liquor or narcotic violations, all felony violations of the criminal statutes of the Commonwealth, and violations of the conditions of any license which have been issued to persons or premises.

Sec. 26 REWARDS: Employees may be permitted by the Commissioner, at his discretion, to receive rewards with a monetary value tendered for services rendered in the discharge of their duties which are especially meritorious or otherwise in the public interest. In each and every case, application must be made in writing to the Commissioner for permission to give or receive any reward.

Sec. 27 ABUSE OF PROCESS – WITHHOLDING EVIDENCE: Officers shall not intentionally manufacture, tamper with, falsify, destroy, or withhold evidence or information nor make any false accusations of a criminal charge or seek to influence the outcome of any investigations.

Sec. 28 RECOMMENDATIONS OF SERVICE: Employees shall not recommend or suggest in any manner except in the transaction of personal business, the employment or procurement of a particular product, professional service, or a commercial service, including, but not limited to, the services of an attorney, bondsman, bail commissioner or funeral director, an ambulance service or a towing service. In the case of an

ambulance or towing service, when such service is necessary and the person needing the service is unable or unwilling to procure it, the officer shall proceed in accordance with established Department procedure.

**Sec. 29 ENDORSEMENT OF COMMERCIAL PRODUCTS:** The Department does not endorse commercial products or allow its facilities to be used for such endorsements. Departmental personnel shall not make any endorsements of commercial products in their capacity as members of the Department.

**Sec. 30 POLITICAL ACTIVITY:** Employees shall be permitted to: Register and vote in any election. Express opinions as private individuals on political issues and candidates, subject to the provisions of Section 19 of this Rule. Attend political conventions, rallies and similar political gatherings as private individuals. Sign political petitions as private individuals. Become candidates for election to an office of any town or city, other than the City of Boston, in any county other than Suffolk County, or other local or regional office which are not prohibited by Section 31 of this Rule. Hold membership in a political party and participate in its functions to the extent consistent with law and with these rules. Participate fully in public affairs to the extent that such endeavors do not impair the natural and efficient performance of official duties, or create real or apparent conflicts of interest.

**Sec. 31 EMPLOYEES NOT ON LEAVE OF ABSENCE PURSUANT TO SECTION 32 OF THIS RULE ARE PROHIBITED FROM:**

- Becoming a candidate for election to or holding any office of the City of Boston, Suffolk County, the Commonwealth of Massachusetts or the Federal Government.
- Using their official capacity to interfere with or affect any election.
- Engaging in the direct or indirect solicitation of funds for political candidates, political campaigns, political parties or political organizations.
- Soliciting votes in support of or in opposition to any candidates in any way which would identify an employee as a member of the Boston Police Department.
- Engaging in any political activities prohibited by federal law, state statute or municipal ordinance.
- Except for the Police Commissioner and/or his or her designee[s] when acting in their official capacities, publicly endorsing or opposing political candidates and/or issues in any way which would cause a reasonable person, having knowledge of the relevant circumstances, to conclude that the employee was acting in his or her official capacity as a member of the Boston Police Department. No bargaining unit member shall be compelled to act as the “designee” under this provision. Under no circumstances shall a member of the Department, other than the Commissioner and/or his or her designee acting in their official capacity, appear in uniform on behalf of a political candidate or on a political issue, whether on or off duty.
- Utilizing public resources (e.g., office equipment, vehicles or staff) for political campaign activity.  
Political Contributions: Pursuant to state and federal law employees may make political financial contributions with the following exceptions and limitations:
  - An employee may make campaign contributions to state or local candidates or to candidate’s committees so long as the total of all contributions for the benefit of any one state or local candidate and the candidate’s committee does not exceed \$1,000.00 in any calendar year.
  - An employee may, in addition, make contributions for the benefit of state or local political party committees, whether elected or non-elected, (e.g., the democratic state committee) so long as the total of contributions for the benefit of any one state or local political party committee does not exceed \$5,000.00 in any one calendar year.
  - The aggregate of all contributions from any one employee to all such state and local candidates and candidate’s committees shall not exceed \$12,500.00 in any one calendar year.
  - An employee may make contributions without limitation to state and local ballot question committees.
  - An employee may make campaign contributions to federal candidates or candidate’s committees

(e.g., candidate for U.S. Senate) so long as the total of all contributions for the benefit of any one federal candidate and the candidate's committee does not exceed \$1,000.00 per election.

- An employee may make contributions for the benefit of federal political party committees (e.g., the democratic national party) without limitation with the exception that if the employee designates such contribution for federal election purposes the employee is subject to an annual contribution limitation of \$20,000.00. (Section Amended by Special Order 99-35, issued June 4, 1999)

Sec. 32 EMPLOYEES SEEKING POLITICAL OFFICE: Every employee of the Police Department upon becoming a candidate for election to any office specified in Section 31 shall take a leave of absence, without pay, effective with the day he requests nomination papers or subscribes his statement of candidacy and continuing until whichever of the following first occurs; his failure of nomination or election at the primary or final election or his failure to become, or withdrawal as a candidate, or if elected, the termination of his term of office.

Sec. 33, EMPLOYMENT OUTSIDE OF THE DEPARTMENT: Employees may engage in off duty employment subject to the following limitations (this section does not apply to Department assigned paid details):

- A. The Police Commissioner's written approval must be granted prior to engaging in off-duty employment. To receive such approval, employees shall fill out BPD Form 2196 (revised 1996), "Request for Permission to Hold Off-Duty Employment" and give it to their Commanding Officer/Director. Commanding Officers/Directors shall forward such forms with their recommendation for approval or disapproval to the appropriate Bureau Chief.
- B. Upon reviewing the recommendation of the employee's Commanding Officer/Director, the Bureau Chief shall forward the request with their recommendation for approval or disapproval to the Police Commissioner for consideration.
- C. Upon reviewing the employee's request and the recommendations of the Commanding Officer/Director and the Bureau Chief, the Police Commissioner shall approve or disapprove the request. All requests will be forwarded to the Director/ Human Resources Division, Bureau of Administration and Technology, where they will be kept on file. The Director, Human Resources Division is responsible for ensuring that employees are sent a copy of their request, approved or disapproved, once the Police Commissioner has acted upon it. No employee may engage in off-duty employment prior to receiving a copy of his or her request, which has been approved by the Police Commissioner.
- D. A new BPD form 2196 must be filled out every time an employee who has received permission for off-duty employment changes jobs, off-duty employers or number of hours worked.
- E. All employees who have permission to hold off-duty employment shall fill out a new BPD form 2196 every year during the month of October. Upon receiving a copy of such form, approved by the Police Commissioner, from the Director, Human Resources Division, the employee's permission to hold off-duty employment is renewed until December 31st of the following year, unless revoked earlier by the Police Commissioner. Permission to hold off-duty employment is automatically revoked on December 31st of any year in which an employee fails to file the above form and maintain proof of having done so.
- F. Responsibility to the Boston Police Department is paramount for its employees. Each employee shall consider the Boston Police Department its primary employer. In no case shall an employee permit responsibilities to a secondary employer to interfere with the employee's responsibilities to the

Department, including, but not limited to, the requirement to be available to work mandatory overtime.

1. Off-duty employment shall constitute no more than thirty-two (32) hours' work per week. This limitation does not apply during any week that the employee does not report for duty because the employee is serving an unpaid suspension. Additionally, employees on administrative duty shall not work more than 90 hours per week, between their employment with the Boston Police Department and a secondary employer, during the period of their administrative leave / duty.

G. Sworn employees shall not engage in any employment or business, or acquire or retain a financial interest in, any employment or business that is licensed by the Licensing Board of the City of Boston. Such business include, but are not limited to, those that engage in the sale or distribution of alcoholic beverages within the City of Boston, nightclubs, private clubs, hotels, and inns.

1. Civilian employees shall be permitted to engage in such employment as described in paragraph G, except where the Department determines that a conflict exists.

H. Sworn employees shall not be employed as a guard or security officer.

I. Employees shall not engage in any employment or business which would constitute a violation of M.G.L. c. 268A, "Conduct of Public Officials and Employees", or St. 1909, Chapter 486, Section 8.

J. Employees shall not hold any elective office specified in Section 31 of this Rule.

K. Employees shall not engage in, acquire or retain a financial interest in any business or employment involving investigatory work outside the Department. Investigatory work includes, but is not limited to, private detectives, insurance company investigations, collection or credit agencies or as the investigator for any attorney or bail bond agency.

L. It is of utmost importance that each employee avoid private financial or business relationships with convicted felons or with persons who openly associate with felons. Each employee must remain vigilant to ensure that they do not work for an employer or acquire a financial interest in any business with a person who has been convicted of a felony or who openly associates with convicted felons. It is the Department's policy to provide notice to the officer when violations of this subsection come to its attention. Once notified, the officer shall forthwith discontinue any relationship in violation of this subsection. No notice will be provided to an officer that may compromise an investigation. The Department shall bear the burden of proving violations of this section.

M. Employees who are lawyers and who receive permission to practice law may not represent clients in criminal cases, consult or offer advice to other attorneys on criminal cases.

N. Employees who have received permission to hold off-duty employment may have such permission revoked at the discretion of the Police Commissioner. The employee may request in writing an explanation for the revocation. (Section Amended by Special Order 03-02, issued January 28, 2003)

Sec. 34 MUTUAL PROTECTION: In an emergency, an officer shall promptly come to the aid of any officer who, when carrying out his official duties, is in need of assistance.

Sec. 35 CONFORMANCE TO LAWS: Employees shall obey all laws of the United States, of the Commonwealth of Massachusetts, all City of Boston ordinances and by-laws and any rule or regulation having the force of law of any board, officer, or commission having the power to make rules and regulations. An employee of the Department who commits any criminal act shall be subject to disciplinary action up to and including discharge from the Department. Each case shall be considered on its own merits, and the circumstances of each shall be fully reviewed before the final action is taken.

Sec. 36 CRIMINAL COMPLAINTS, PROTECTIVE CUSTODY, AND ARRESTS: An employee of the Department, upon learning that an application for a criminal complaint has been made against them, or that a complaint has been issued against them, or has been arrested, or has been taken into protective custody, shall notify their commanding officer verbally and in writing within 24 hours, or as soon as possible. Failure to provide proper notification may result in a separate disciplinary action for failure to notify, in addition to any discipline that may be considered for the underlying incident. Such notification shall be a summary of the complaint sought or issued and the projected date of the hearing or trial; or in the case of an incident of protective custody or arrest the circumstances and details related to the protective custody or arrest. The commanding officer receiving such notification shall transmit a copy of the employee's report to the Office of the Police Commissioner and the Superintendent of the Bureau of Professional Standards.

The Supervisor of Cases at each court, upon receipt of information that a complaint or indictment has been sought or issued against a Department employee, shall submit a separate report to the Office of the Police Commissioner and the Superintendent of the Bureau of Professional Standards, furnishing the subject matter of the complaint or indictment and the date of the hearing or trial.

Sec. 37 SITUATIONS INVOLVING FAMILY OR FRIENDS: An officer confronted with a situation requiring police intervention, in which a member of his family or a friend is involved, shall not intervene unless an emergency exists, and then only to meet the emergency. The officer concerned shall notify the Operations Section, or if outside the City of Boston, the appropriate police agency, so that a more objective police unit may handle the matter.

Sec. 38 SITUATIONS INVOLVING OFF-DUTY BOSTON POLICE OFFICERS AND CIVILIANS OCCURRING WITHIN THE CITY OF BOSTON: When an officer is confronted with a situation in which the conduct of an off-duty Boston Police Officer or civilian employee is in question, that officer shall follow appropriate and normal police procedures and, as soon as possible, shall notify the Operations Section and request that a Superior Officer respond to the incident. The responding Superior Officer shall notify the Operations Division to notify the Superintendent of the Bureau of Professional Standards if the off-duty officer or civilian employee is arrested, detained, if they have information to indicate that a criminal complaint will be filed, or if the Superior Officer determines that the conduct in question should be referred to the Bureau of Professional Standards. In addition, the Superior Officer shall notify the Commander of the area, division or unit to which the off-duty officer or civilian employee is assigned.

Sec. 38A SITUATIONS INVOLVING OFF-DUTY BOSTON POLICE OFFICERS AND CIVILIANS OCCURRING OUTSIDE THE CITY OF BOSTON: When an on-duty officer or civilian employee is made aware of a situation in which the conduct of an off-duty Boston Police Officer or civilian employee is in question, that officer or civilian employee shall notify their immediate supervisor. The supervisor shall notify the Operations Division to notify the Superintendent of the Bureau of Professional Standards if the off-duty officer or civilian employee is arrested, detained, if they have information to indicate that a

complaint will be filed, or if the Superior Officer believes that the conduct in question should be referred to the Bureau of Professional Standards. In addition, the Superior Officer shall notify the Commander of the area, division or unit to which the off-duty officer or civilian employee is assigned.

Sec. 39 ASSOCIATION WITH CRIMINALS: Department employees shall not associate with persons whom they know, or should know, are persons under criminal investigation, or who have a reputation in the community or in the Department for recent or present involvement in felonious or criminal activities. This rule shall not apply where said associations are necessary in the performance of official duties, or where said associations are unavoidable due to familial relationships of employees.

Sec. 40 RESIDENCY:

A. All members of the AFSCME, SEIU and SENA bargaining units hired by the city after July 1, 1980 shall be subject to the City of Boston Residency Ordinance. All other civilian employees shall be subject to the Residency Ordinance regardless of their date of hire, except as referenced in the Ordinance itself.

B. All members of the Department who become sworn permanent officers after July 1, 1994 shall be subject to the City of Boston Residency Ordinance.

Gregory P. Long  
Superintendent In Chief

## **Rules and Procedures**

### **Rule 109**

**April 12, 1983**

#### **Rule 109 - DISCIPLINE PROCEDURE, AMENDED**

Sec. 1 This rule is written and promulgated to be used in conjunction with Rule 102, which defines the conduct, general rights and responsibilities of Police Department Personnel. It is designed to provide maximum flexibility in the discipline process and to increase the responsiveness of the Department to the needs of the individual member and of the community.

Sec. 2 "Discipline" has too long had the connotation of simple punishment; this rule envisions a disciplinary process which incorporates the idea of training both for effective self-discipline and for a group discipline, or esprit de corps. To accomplish this design, the rule recognizes the wide spectrum of discipline and through such provisions as the five-day suspension program and the district personnel records places discipline at a level where it can respond better to the individual member.

Sec. 3 Scope: This rule is designed strictly to be procedural in nature, and is not meant to create new rights or duties not previously granted by law or contract.

For example, CETA employees, probationary employees, and provisional employees shall continue to be governed by the respective rules and laws pertaining to them, and this rule shall not apply to them where inappropriate or inconsistent with those rules or laws. This rule is also not meant to change the working conditions of members of the Department, but instead is a managerial guideline controlling administration. It does not necessarily promulgate a new set of procedures, but in most cases simply compiles existing departmental policy and practice. In addition, the special procedures relating to written reprimands, ss. 21-27 apply only to police officers covered by the Agreement between the City of Boston and the Boston Police Patrolmen's Association. Finally, if any substantive changes in the rights and duties of employees or the Department made by future changes in the law or the contract affect sections of this rule, such changes shall notwithstanding override the affected sections.

Sec. 4 Part I of this rule, "Spectrum of Discipline," defines the outlines of the Department's disciplinary program. It contains a general discussion of the sanctions which may be used by the Department followed by a discussion of the concept of "Progressive Discipline." Section C of Part I establishes district personnel records which are to be utilized in connection with progressive discipline; finally, the procedures used in three types of sanctions-written reprimands, five-day suspensions, and punishment duty are specifically detailed, to provide for uniformity of treatment under the discipline rule.



Sec. 5 Parts III through V of the rule state the procedures to be used by the Department in handling complaints, administrative investigations of allegations of misconduct by Department members, and hearings.

The complaints section creates a unified procedure for the handling of all complaints made the Department either from inside or outside. The section on investigations seeks to promote quick, thorough investigations without abridging the rights of Department members or injuring the reputations of members unjustly accused. It should be noted that the provisions governing investigations are strictly limited to investigations of allegations against Department personnel and are not to apply to criminal investigations or administrative studies or surveys concerning policy or practices. The hearings section deals with the three different types of administrative hearings: disciplinary hearings, appeals from punishment duty or five-day suspensions, and detective hearings--and sets up uniform practices designed to arrive at just decisions efficiently.

## PART I: SPECTRUM OF DISCIPLINE

### A. TYPES OF SANCTIONS used by the Boston Police Department include the following:

Sec. 6 Oral Reprimands: Oral reprimands, given by supervisors for minor violations of the Rules and Procedures, such as improper uniform or reporting late for duty, are simply spoken censures or reproofs. While a notation that an oral reprimand was given is entered into the district permanent personnel record, no record of the reprimand goes into the permanent personnel file. The rule contemplates that such reprimands will be given on an informal basis without any form of prior notice.

Sec. 7 Written Reprimands: Written reprimands are issued either for minor offenses committed by employees for whom oral reprimands have proven ineffective, or for other offenses under Rule 102 which are accompanied by ameliorating circumstances. The reprimand is entered into the permanent personnel file. In situations in which an employee has the right to a hearing with respect to a written reprimand, the procedures for such a hearing are described below in part D, ss. 21-27. Section 21 of this rule establishes the guideline for determining which employees have such a right.

Sec. 8 Disciplinary Probation: At the option of the Commissioner, disciplinary probation may be imposed upon an employee for violations of the Rules and Procedures. If just cause is found in any disciplinary action taken against an employee while on such probation, the probation shall be taken into account in determining the severity of the sanction imposed.

Where the employee is a police officer, covered by the Collective Bargaining Agreement, the

procedures which are used for written reprimands (ss. 21-27) shall be followed prior to imposition of disciplinary probation unless the employee on probation shall fulfill such conditions as the Commissioner may order, and failure to fulfill such conditions shall render the employee liable for further disciplinary action.

Sec. 9 Punishment Duty: Massachusetts General Laws, C. 31, s. 62 authorize the imposition of punishment duty upon sworn personnel. Such duty is extra, unpaid duty assigned above and beyond an officer's normal hours by the officer's commander for violations of the Rules and Procedures. Such duty shall not be demeaning, unduly fatiguing, nor outside of the scope of the officer's job classification. The procedures used for punishment duty are described below in part F, ss. 36-39.

Sec. 10 Suspensions: Suspensions are periods of time during which an employee is relieved of duty and for which the employee is not paid. Suspensions for a period which does not exceed five days may be imposed without a prior hearing either by the Commissioner or by persons designated this authority by the Commissioner. In addition, if the employee to be suspended is tenured under the Civil Service Law, such a suspension may only be imposed for specific offenses, as outlined below in part E, ss. 28-35. Only the Commissioner may impose a suspension of more than five days, and then only after the procedures designated in part V, ss. 56-63 below, have been followed.

Employees of the Boston Police Department may also be relieved from duty with pay. Such action is not a disciplinary action, but is designed to maintain the efficiency of the force if for some reason an employee is rendered unfit for duty. In such a case, the Commissioner may relieve the employee from duty with pay.

Sec. 11 Discharge or Reduction in Rank: An employee may be discharged or reduced in rank only by the Police Commissioner, and then only after a hearing as described in ss. 56-63 or waiver of such a hearing by the employee.

## B. PROGRESSIVE DISCIPLINE

Sec. 12 Persons who utilize this disciplinary rule shall apply the concept of progressive discipline. Progressive discipline means that progressively stricter disciplinary action shall be taken against persons who persist in violations of the Rules and Procedures. Such a program serves a training function, in that, for a first time violation, an employee may be warned or given a relatively light sanction as an indication that the Department does not condone such action. Upon repetition, then, it is assumed that the employee knows that the violation is wrong, and will receive more harsh sanction.

Sec. 13 It is not necessary for the proper implementation of progressive discipline that all stages of discipline be exhausted, nor that progressive discipline start at any one level or proceed with

any particular incrementation. Much is left open to the discretion of the person imposing the discipline, it is simply to be recalled that progressive discipline be used as a guiding precept.

#### C. DISTRICT PERSONNEL RECORD

Sec. 14 General Considerations: Commanding officers are often called upon to make evaluations of employees assigned to them. Such evaluations are necessary for applying progressive discipline, and are also used in connection with promotion and reassignment. Accurate evaluation must be based on recorded personnel histories, such as those established by this rule.

Sec. 15 The Record Card: The commanding officer of each unit shall establish a personnel file consisting of a file card for each employee in the command. When an officer is assigned to a command, the commanding officer shall have a new card prepared for that officer. Each card shall have the officer's name and I.D. number at the top, and shall be kept in an alphabetical file.

Sec. 16 Maintenance of the Record: Maintaining the unit personnel file is the joint responsibility of the commanding officer and the supervising officer. Whenever an incident which merits entry in the record takes place, the supervisor of the individuals involved shall report the incident to the commanding officer or person designated by him in his absence. The commanding officer or person designated by him shall make an entry in the card, including the date, subject matter, and reporting officer's name.

Sec. 17 The record file shall be kept in the commanding officer's office or other secure place, and shall be available only to the Office of the Police Commissioner, the commanding officer, the respective bureau chief, and the Bureau of Professional Standards and Development.

Sec. 18 Subject Matter of the Record: The record shall maintain a notation of all minor offenses, all praiseworthy conduct and all oral reprimands. In addition, the cards shall also contain notations of any disciplinary actions taken or any commendations received from the Department. The notation need not go into specific detail; it shall suffice for the record simply to state that the employee was the subject of a type of incident (e.g., that the employee was reprimanded for a particular incident).

Sec. 19 Periodic Review: The Bureau of Professional Standards and Development shall make periodic random reviews of the District Personnel Records to make certain that accurate up-to-date records are maintained.

Sec. 20 Disposal of the Record: The records shall be maintained by the Unit until the reassignment to another unit of an officer, or upon an officer's retirement or termination, whichever occurs first. At that time, the record card for that officer shall be sent to the Bureau of Professional Standards and Development.

#### D. WRITTEN REPRIMANDS

Sec. 21 The collective bargaining contract between the Boston Police Patrolmen's Association and the City of Boston, effective July 1, 1974, provides:

No material which contains an allegation of misconduct against an employee shall be included in his/her personnel file until the charges have been verified by affidavit and a hearing held. If a determination is made that the allegation is without substance, then the allegation shall not be included in the employee's personnel file.

Therefore, a letter of reprimand may not be placed in the personnel file of a police officer covered by the collective bargaining contract, unless the allegations in the letter are supported by affidavit and the police officer is given a hearing or unless the police officer waives the right to verification and a hearing. The following procedures are established for letters of reprimand.

Sec. 22 The commander of the bureau or unit to which a police officer is assigned, or the Commander of the Internal Affairs Division, or the Commander of the Staff Inspection Division may recommend that the procedures for a letter of reprimand be initiated, and must submit a report to the Police Commissioner detailing the circumstances surrounding the subject of the letter. The report shall include the names of all witnesses and Superior Officers involved, and the dates and times of the incidents. The report must detail the facts of the incident and not rely on conclusory phrases.

Sec. 23 The Commissioner shall have the proposed letter of reprimand prepared, and then the original shall be sent back to the bureau or unit initiating the letter for verification. Such verification shall consist of either an affidavit of the complaint or the signature of the commander so verifying.

Sec. 24 The proposed letter shall then be forwarded to the chief clerk and to the Bureau of Professional Standards and Development. When the police officer has a right to a hearing the Bureau of Professional Standards and Development shall schedule a hearing and the Commissioner shall designate a hearing officer. The police officer who is the subject of the proposed letter shall be notified by the Bureau of Professional Standards and Development of the time and date of the hearing.

Sec. 25 The hearing shall be conducted pursuant to part V, ss. 59-62 below. No later than five days after the conclusion of the hearing, the hearing officer shall submit a report which briefly summarizes the evidence and recommends whether the letter should be signed by the Commissioner. Also, the hearing officer may recommend changes in the proposed letter.

Sec. 26 A police officer may waive a hearing and consent in writing to having the letter placed in the personnel file.

Sec. 27 If the Commissioner signs the proposed letter, that letter shall be served on the police officer and a copy placed in the personnel file. A copy of the letter shall also be placed in the Internal Affairs Division file.

#### E. SUSPENSION FOR FIVE DAYS OR LESS

Sec. 28 General Procedures. The Civil Service Laws, M.G.L. c. 31, s. 41 permits the Police Commissioner to delegate the authority to immediately impose suspensions of five days or less without first providing a hearing to a tenured civil service employee. The law requires that within twenty-four hours after such a suspension the subordinate be given a copy of sections 41 to 45 of Chapter 31 of the General Laws and a written notice which states the specific reasons for the suspension. That notice must inform the subordinates that they may within forty-eight hours of the receipt of such notice request in writing a hearing by the appointing authority. Such a hearing must be given within five days of the receipt of such a request. Procedures for such a hearing are detailed below in Part V, Section 65.

Sec. 29 Delegation. The Police Commissioner may delegate any member of the department the authority to impose immediate suspensions of five days or less. That delegation shall be in writing and shall specify the name or position of the member to whom the authority has been delegated and shall specify whether the authority is limited to a particular division or bureau of the Department. The delegation shall be in full force and effect unless and until it is revoked by a subsequent written notice by the Police Commissioner.

#### PART II: PROCEDURES

##### Sec. 30 Specific Procedure:

1. When an offense of the type covered by Section 32 of this rule comes to the attention of a person who has been delegated the authority, he or she may immediately impose a suspension without pay of five working days or less. The suspension is effected by orally informing the subordinate of the period of suspension. Where feasible the oral suspension shall be effected in the presence of another superior officer. If the subordinate is a sworn member, the officer shall immediately turn in the police badge and gun.
2. The Civil Service Laws require that the employee who is suspended without a prior hearing shall be given within twenty-four hours of the suspension a copy of the Notice of Suspension (BPD Form #1919). However, the notice should, if possible, be handed to the offender at the time of the imposition. The written notice must be a formal statement of the reasons for the suspension, the number of working days the suspension lasts, and the date the suspension commences. Copies of M.G.L. c. 31, s.s. 41 to 45 shall also be included. The written notice will have five copies, to be routed as

follows:

- a. original to the disciplined subordinate;
- b. one copy retained by the commanding officer;
- c. one copy to the Bureau of Professional Standards and Development;
- d. one copy to the appropriate departmental bureau (Bureau of Field Services, etc.);
- e. one copy to the Personnel Division.

It is important that all copies be routed as quickly as possible so the payroll division can be notified and the employee taken from the payroll for the suspension period. Whenever problems or questions arise in completing the notice, the person suspending should feel free to contact the Office of the Legal Advisor.

Sec. 31 Acceptance of Discipline: It should at all times be kept in mind that the most effective discipline is that which is accepted by the individual. Therefore, where practicable the person delegated the authority to suspend should discuss the infraction and the contemplated discipline with the individual.

A subordinate may waive the right to request a hearing before the appointing authority. In such a case, the subordinate waives that right by signing a statement to that effect on the copies of the Notice of Suspension.

Sec. 32 Offenses Covered by the Five-Day Rule: The following offenses are subject to the Five Day rule, and may be disciplined by imposition of immediate suspension of not more than five days. If an employee commits an offense not on this list, that offense may not form the basis of an immediate suspension.

1. Rule 102 s. 3:

- a. Fighting or quarreling with members of the force;
- b. Negligent use of a firearm, providing no injury or death resulted from the misuse;
- c. Negligent discharge of a firearm, providing no injury or death resulted from the discharge;
- d. Participation in unlawful games of chance or gambling.

2. Rule 102, s. 4:

- a. Failure to properly patrol beat or section;
- b. Failure to properly cover school crossings;
- c. Failure to properly care for assigned equipment, damaging or losing same due to carelessness;
- d. Willfully damaging police department property;
- e. Interference with police radio broadcasting;
- f. Improperly turning off police radio;
- g. Failure to remove keys from patrol car when left unattended;
- h. Failure to report as witness when duly notified or subpoenaed;

- i. Failure to notify Operations Division of availability for assignment
- 3. Rule 102 s. 5: Failure to properly maintain a copy of the rules book.
- 4. Rule 102 s. 6:
  - a. Failure to properly supervise subordinates;
  - b. Failure to prefer disciplinary charges or take appropriate disciplinary action.
- 5. Rule 102 s. 7: Failure to report their place of residence and telephone number or change in either of them.
- 6. Rule 102 s. 8: Failure to obey and comply with all rules, orders and other directives of the Department and of superior officers, whether written or oral.
- 7. Rule 102 s. 9:
  - a. Failure to be civil and respectful, courteous and considerate toward all members of the Department and the general public;
  - b. Use of epithets or terms that tend to denigrate a particular race or ethnic group except when necessary in police reports or testimony.
- 8. Rule 102 s. 10:
  - a. Failure to report for duty;
  - b. Unauthorized absence from duty;
  - c. Failure to be mentally and physically fit to perform duty;
  - d. Failure to be in proper uniform and properly equipped.
- 9. Rule 102 s. 11: Failure to be properly groomed.
- 10. Rule 102 s. 12: Failure to remain awake and alert while on duty.
- 11. Rule 102 s. 13:
  - a. Drinking of alcoholic beverages while on duty unless it is necessary to gain evidence and is under the order of a superior officer;
  - b. Reporting for duty while under the influence of alcoholic beverages to any degree whatever or with an odor of alcohol on one's breath.
- 12. Rule 102 s. 14:
  - a. Consumption of alcoholic beverages while off duty to the extent that it results in obnoxious behavior that would tend to discredit the officer of the Department or would render the officer unfit to report for the next regular tour of duty.
  - b. Consumption of alcoholic beverages while in uniform or while wearing any part of the uniform.
- 13. Rule 102 s. 17: Failure to respond to a radio call or to the request of a civilian.
- 14. Rule 102 s. 18: Engaging in personal business while on duty.
- 15. Rule 102 s. 20: Failure to give prescribed identification.
- 16. Rule 102 s. 21: Soliciting from the general public money, gifts, or other things of value for charitable or testimonial purposes, or otherwise using identity as a police officer for such purposes.
- 17. Rule 102 s. 22: Seeking or accepting food and/or drink from any individual, merchant or business establishment, when it can be construed to involve the position as an employee of the Boston Police Department.
- 18. Rule 102 s. 23: Submitting false information in an oral or written report or in response to

a B.I.S. inquiry.

19. Rule 102 s. 25: Failure to report any serious felonies or less serious crime that comes to the employee's attention.
20. Rule 102 s. 28: Recommending any employment or procurement of a particular service or product except in the transaction of personal business or when proceeding in accordance with established Departmental procedure.
21. Rule 102 s. 34: Failure to come to the aid of a fellow officer in an emergency if, in the course of carrying out his official duties, that officer is in need of assistance.
22. Rule 102 s. 35: Receipt of excessive moving vehicle violations or excessive unpaid parking violation tickets.
23. Rule 102 s. 37: Intervening in a situation requiring police attention when the officer's family and/or friend(s) are involved except in the case of an emergency.
24. Rule 102 s. 38: Failure to report the questionable behavior of a fellow officer.
25. Miscellaneous offenses:
  - a. Reckless driving;
  - b. Unreported paid details;
  - c. Failure to maintain proper records, such as the district control log;
  - d. Misuse of sick time;
  - e. Overtime abuses.

Sec. 33 Subsequent Offenses: If the employee persists continually in the violation of the rules, then the person delegated the authority to suspend shall recommend the matter for a disciplinary hearing. Furthermore, certain offenses are considered major if repeated within certain periods and are to be immediately recommended for disciplinary hearing. The offenses are:

1. Two offenses within one year:
  - a. Negligent handling of a firearm;
  - b. Willfully damaging police equipment;
  - c. Interfering with police broadcasting;
  - d. Failure to remain awake while on duty;
  - e. Seeking and/or accepting food or drink when it can be construed to involve position as Department employee;
  - f. Untruthfulness in written or oral reports or in response to B.I.S. investigations;
  - g. Failure report felonies.
2. Two offenses within two years:
  - a. Negligent discharge of a firearm;
  - b. Failure to come to the aid of a fellow officer in an emergency.
3. Third offense in one year:

Failure to report as a witness when duly notified or subpoenaed.

Sec. 34 Periodic Review: The Chief of the Bureau of Professional Standards and Development



shall periodically review the actions taken by persons delegated authority under this Section and the list of offenses provided for in Sections 32 and 33 in order to determine whether additional offenses should be included or offenses deleted from this rule. In addition, the Chief of the Bureau of Professional Standards and Development shall submit to the Police Commissioner periodic reports detailing the action taken pursuant to this rule.

Sec. 35 A suspension under this Section does not preclude the possibility of further punishment; however, before the Department can take further action, a hearing must be held following the procedures outlined in Part V, ss. 56-63.

#### F. PUNISHMENT DUTY:

Sec. 36 Punishment duty may be assigned to any officer of the Department by his commanding officer or by the Police Commissioner. Such duty shall be performed under the direction of the officer's commanding officer.

Sec. 37 Punishment duty must be useful work, whether as an addition to the strength of the force, or as a relief for other employees who have worked hard and faithfully. No suggestion of favoritism shall attach to either the assignment of the duty or to the reliefs created by the duty. Punishment duty must be assigned so that the employee under punishment shall not suffer undue fatigue or be otherwise unfit for regular or extra work; and except with the employee's written consent no more than seven consecutive hours of punishment duty shall be performed at any one time, or more than fourteen hours in four consecutive days, or more than twenty one hours in seven consecutive days. Neither shall the employee be compelled, without written consent, to perform such duty within two hours before or after a tour of regular or special duty.

Sec. 38 Whenever any portion of the punishment duty as ordered has been performed, the officer in charge of the punishment assignment shall report to the Bureau of Professional Standards and Development the name of the employee, the number of hours and the character of the work done. When the punishment duty assignment has been completed, the officer in charge shall so certify in such form as the Bureau of Professional Standards and Development shall prescribe.

Sec. 39 Whenever punishment duty is assigned, the employee under punishment shall have the right of appeal from such duty as described below in Part V, Section 65.

#### PART III: COMPLAINTS

Sec. 40 Complaint Control Form: A Complaint Control Form (B.P.D. Form #1920) shall be used to record all complaints against Department personnel, whether from citizens or members of the Department. Each Complaint Control Form shall have an identifying number so that the processing of complaints can be monitored.

Sec. 41 Manner of Recording Complaints:

- a. All complaints shall be received and recorded courteously. No citizen shall be denied an opportunity to register a complaint, nor shall any complainant be directed to another building to register a complaint.
- b. Known Complainants: When the information received from the complainant includes the complainant's name and address, the officer taking the complaint shall inform the complainant that he or she will be contacted by a member of the Department assigned to investigate the complaint. The complainant shall be instructed to telephone the Bureau of Professional Standards and Development if not contacted by the Department within seventy-two hours of making the complaint.
- c. Walk-in Complaints: Whenever a person indicates a desire to make a complaint concerning a Department employee, that person shall be directed to the nearest available superior officer. If necessary the complainant shall be assisted in making contact with a superior officer. The officer recording the complaint shall complete a Complaint Control Form, after obtaining as much information as possible from the complainant.
- d. Letter Complaints: Letters alleging misconduct by a Department employee shall be forwarded to the Bureau of Professional Standards and Development. An officer assigned to the Bureau of Professional Standards and Development shall complete a Complaint Control Form. Copies shall be distributed as indicated in section 44 of this rule, save that the complainant's copy shall be mailed to the complainant if the name and address are known.
- e. Telephone Complaints: Complainants contacting the Department by telephone shall be transferred to a superior officer if immediately available who will obtain as much information as possible from the complainant and complete a Complaint Control Form. In no case shall a telephone complaint be refused because a superior officer is unavailable, or because the complainant is not identified. All copies of the Complaint Control Form shall be forwarded to the Bureau of Professional Standards and Development, which shall distribute copies as indicated in Section 44 of this rule, save that the complainant's copy shall be mailed to the complainant if the name and address are known.
- f. Departmental Complaints: Whenever a member of the Department desires to initiate a complaint against another member--including complaints by superior officers against subordinates and subordinates against superior officers--that member shall complete a Complaint Control Form. The Complaint Control Form shall be used whenever a supervisor or superior officer seeks to initiate formal charges against department personnel.
- g. Governmental Agencies: When information is received from governmental agencies alleging specific acts of misconduct by a Department employee, the information shall be forwarded to the Bureau of Professional Standards and Development. An officer assigned to the Bureau of Professional Standards and Development shall complete a

Complaint Control Form and distribute copies as indicated in Section 44 of this rule, save that the complainant's copy shall be retained by the Bureau of Professional Standards and Development.

- h. Policy Complaints: Complaints concerning Departmental Policy, performance, or practice and not alleging misconduct by specific employees, known or unknown, shall be recorded on a complaint form. One copy will be retained at the unit and the other three routed to the Bureau of Professional Standards and Development for appropriate distribution.
- i. The completed form should contain a detailed description of the alleged act(s) of misconduct, including date, time and place; names or descriptions of Department employees involved in the incident; the names and addresses of witnesses, if known; and any other relevant information.

Sec. 42 Signing of the Complaint Control Form: If the complaint is made in person, when the officer has completed the complaint form the complainant shall read it and make any necessary corrections. The officer shall request the complainant to sign the complaint. If the complainant refuses to sign, a notation to that effect shall be made on the form. In all other respects unsigned complaints shall be processed in the same manner as signed complaints.

Sec. 43 Immediate Resolution of Complaints: Complaints resolved at the time of the complaint to the complainant's satisfaction shall be recorded on a Complaint Control Form with a notation that the complaint was resolved. Where possible, the complainant should acknowledge the resolution in writing, and such acknowledgment should be attached on the Complaint Control Form.

Sec. 44 Routing the Complaint Form: If the employee complained of is attached to the unit which receives the complaint, copies of the Complaint Control Form shall be distributed immediately as follows:

- a. One copy to the complainant;
- b. One copy to the commanding officer of the unit;
- c. One copy to the superior officer investigating the complaint;
- d. One copy to the Bureau of Professional Standards and Development.

If the employee complained of is not assigned to the unit which receives the complaint, copies of the Complaint Control form shall be distributed immediately as follows:

- a. One copy to the complainant;
- b. Three copies to the Bureau of Professional Standards and Development. The Bureau of Professional Standards and Development shall retain one copy and may distribute, upon the discretion of the Chief of the O.I.I., the remaining copies as follows:
- c. One copy to the commanding officer of the unit to which the employee complained of is attached;

- d. One copy to the superior officer investigating the complaint.

Sec. 45 Notification of Internal Affairs Division: The Internal Affairs Division shall be notified immediately upon receipt of a complaint alleging:

- a. Brutality, death or serious injury caused by a Department employee; b. Firearm discharge resulting in personal injury or property damage caused by a Department employee;
- c. The commission of a felony by a Department employee;
- d. Possible corruption or bribery of a Department employee;
- e. When in the judgment of the superior officer receiving the complaint an immediate investigation by the Internal Affairs Division is justified;
- f. If the employee against whom the complaint is rendered so requests.

This immediate notification will be in addition to and separate from the regular distribution outlined in Section 44.

Sec. 46 Monitoring of Complaint Control Forms:

- a. The Bureau of Professional Standards and Development shall maintain a log of all Complaint Control forms issued to all districts and units. The log shall record the date each form was issued and the district or unit to which the form was issued. The log shall also record the date the form was used and the name and rank of the officer who completed the form.
- b. The Bureau of Professional Standards and Development shall maintain a file of all cases investigated.
- c. Access to the complaint file shall be authorized in writing by the Police Commissioner, the Superintendent of the Bureau of Professional Standards and Development or the Commanding Officer of the Special Investigations Unit.

Sec. 47 An employee against whom a complaint has been made shall not attempt, directly or indirectly, by threat, appeal, persuasion or the payment of promise of money or other things of value, to secure the withdrawal or abandonment of the complaint. Such actions shall be dealt with very strictly by the Department.

#### PART IV: INVESTIGATIONS

Sec. 48 Confidentiality of Disciplinary Process: Prior to the completion of the investigation of a complaint, information concerning such an investigation shall not be released unless authorized by the Commissioner.

However, the fact that a complaint was received and a departmental investigation is under way may be disclosed unless the Chief of the Bureau of Professional Standards and Development determines that for security reasons it should remain confidential.

Sec. 49 Initiating Investigation: Where practicable in investigations initiated by complaints, the complaints shall be verified before the investigation commences; however, the absence of verification shall not impede the registration and investigation of a complaint.

If the complaint is received at the unit to which the complainee is assigned, the commanding officer of the unit shall determine whether the matter can be appropriately dealt with at the unit level. In such cases commanding officers shall appoint an investigating officer, although the Bureau of Professional Standards and Development may intervene at any time and assume control of any investigation.

If the commanding officer determines that the complaint is not appropriate for investigation at the unit level, it shall be referred to the Bureau of Professional Standards and Development for investigation. In such cases, the chief of the Bureau of Professional Standards and Development shall appoint an investigating officer, or return the complaint to the commanding officer of the person who is the subject of the complaint for investigation at the unit level.

If the complaint is received at a unit to which the complainee is not assigned then the Bureau of Professional Standards and Development shall initiate the complaint at either the unit level or through the Bureau. The Bureau of Professional Standards and Development may also initiate investigations into such matters as it sees fit, whether or not a complaint has been received.

Sec. 50 Investigative Techniques: The investigating officer may use any lawful investigative techniques, including, but not limited to, inspecting public records, questioning of witnesses, interrogation of the member complained of, questioning of fellow employees and surveillance.

Sec. 51 Interrogation of Members of the Department: The following provisions shall apply whenever, as part of an investigation of alleged violations of the Rules and Procedures, a member of the department is ordered to submit a report or to an interrogation.

- a. An interrogation of a member of the department shall be at a reasonable hour, preferably when the member of the department is on duty, unless the exigencies of the investigation dictate otherwise. No member shall suffer loss of pay for the time spent under interrogation.
- b. The interrogation shall take place at a location designated by the investigating officer. Usually it will be at the command to which the investigating officer is assigned or at the district station within which the incident allegedly occurred.
- c. The member of the department shall be informed of the rank, name and command of the interrogating officer and all persons present during the interrogation. If a member of the department is directed to leave his/her post and report for interrogation to another command, the commanding officer shall be promptly notified of the member's whereabouts.
- d. Whenever a member of the department is ordered to submit a report or to an interrogation pursuant to this Rule, the member may be informed of the nature of the

investigation, including the name of the complainant. The address of the complainants and/or witnesses need not be disclosed; however, sufficient information to reasonably apprise the member of the allegations should be provided. If the complaint is filed in writing, a copy may be furnished to said member(s). If it is known that the member of the department being interrogated is a witness only, he should be informed at the initial contact.

- e. Questioning during an interrogation shall not be overly long. Reasonable respites shall be allowed. Time shall also be provided for personal necessities, meals, telephone calls and rest periods as are reasonably necessary.
- f. The member of the department shall not be subjected to any offensive language, nor be threatened with transfer, dismissal or other disciplinary punishment.
- g. Whenever a member is ordered, pursuant to these rules, to submit a report or to interrogation, that member shall be advised that any such report or interrogation cannot be used by the Department as evidence in criminal proceedings against that member. When a member of the department is complained against and is directed by a superior officer to submit a report or to an interrogation relative to such complaint, that member is required to reply.
- h. In any case, the refusal by a member of the force to answer pertinent questions may result in disciplinary action.
- i. The law imposes no obligation, legal or otherwise on the department to provide an opportunity for a member of the department to consult with counsel or anyone else when questioned by a superior officer about his or her employment or matters relevant to his or her continuing fitness for police service. Nevertheless, the department shall afford an opportunity for a member of the department, if so requested, to consult with counsel before being questioned concerning a serious violation of the rules and regulations, provided the interrogation is not unduly delayed. However, in such cases the interrogation may not be postponed for purpose of counsel past 10 a.m. of the day following the notification of interrogation. Counsel, if available and a representative of a certified employee organization may be present during the interrogation of a member of the department. Requests for an opportunity to consult with counsel in connection with minor violations will be denied unless sufficient reasons are advanced.
- j. In the event that an employee claims that there have been violations of any provisions of this Section, such employee, either alone or together with the employee organization representative, may file a signed, written complaint with the Police Commissioner against the person committing the alleged violation. The Police Commissioner shall cause such complaint to be investigated and render a decision with respect to any such complaint. The decision shall be in writing and shall state with particularity the consideration and reasons in support thereof including a statement of the facts found. A copy of the decision shall be given forthwith to both the person who is the subject of the complaint and the employee organization representative.

The Police Commissioner in his discretion may endeavor to eliminate any unlawful act or practice which constitutes a violation of this Section by informal methods or conference,

conciliation and persuasion.

Sec. 52 Investigation Report: As soon as practical, though not the expense of a thorough investigation, the investigating officer shall bring the investigation to a close and prepare an investigation report. The report shall summarize all evidence gathered during the investigation and shall contain the investigating officer's recommendation that the complaint be found:

- a. sustained (investigation disclosed sufficient evidence to support allegations in the complaint);
- b. not sustained (investigation failed to prove or disprove the allegations); c. exonerated (the action complained of did occur, but investigation revealed that action was proper, legal and reasonable); or
- d. unfounded (investigation revealed that conduct did not occur).

In addition, if the investigating officer has discovered misconduct not based on complaint, he shall so state in his report.

The report shall then be forwarded to the commanding officer if a unit-level investigation, or to the chief of the Bureau of Professional Standards and Development. The commanding officer or the chief of the Bureau of Professional Standards and Development shall then make recommendations for disciplinary action or shall impose an immediate suspension for five days or less if the complaint has been sustained. If a unit-level investigation, a copy of the report along with the commanding officer's disciplinary action will be sent to the Bureau of Professional Standards and Development for confirmation.

If the investigation was inaugurated by a complaint from outside the department, upon completion of the investigation a letter shall be sent to the complainant informing him or her of the results of the investigation.

## PART V: HEARINGS

### A. FORUMS

Sec. 53 The Police Commissioner is the appointing authority pursuant to the provision of M.G.L. c. 31, s. 41 and as such may hear cases relating to discharge, removal, transfer to another agency, suspension, lowering in rank or compensation, abolition of office or punishment duty. In addition, he may appoint either a hearing officer or a trial board to hear such cases.

Sec. 54 Trial Boards: Pursuant to the Acts of 1962, Chapter 322, the Police Commissioner may from time to time convene a Trial Board to be composed of three captains, to inquire into such matters as the Commissioner directs. No member of a Trial Board may sit on any matters involving the member's district, or with which the member has direct personal contact. In such

cases the member must be disqualified, and the Commissioner shall appoint another captain to the Board.

Pursuant to the Acts of 1950, Chapter 735, a Trial Board must be convened at the request of any person who has been reassigned from duties as a detective after his probationary period. For rules governing such hearings, see Section 65, "Detective Hearings" below.

Sec. 55 Hearing Officer: The Police Commissioner may, pursuant to M.G.L. c. 31, s. 41, appoint a hearing officer to hear any cases concerning proposed discharge, removal from office, transfer to another agency, suspension, lowering in rank or compensation, abolition of office, or imposition of punishment duty. In such a case, the Commissioner shall send to the Bureau of Professional Standards and Development and the Chief Clerk a designation in writing containing the name of the hearing officer and the employee who is the subject of such action. The Hearing Officer shall follow the general rules of procedure outlined below.

## B. PROCEDURE

Sec. 56 Notice: Before any action affecting employment or compensation of a tenured employee as delineated in M.G.L. c. 31 s. 41, is taken, the officer or employee involved shall be given a written statement of the specific reason or reasons for the contemplated action, together with a copy of M.G.L. c. 31, ss. 41-45. The employee then may consent in writing to the imposition of discipline and waive the right to a hearing on the specific reason or reasons given. If no such waiver or consent is executed, the Police Commissioner shall determine whether the hearing is to be before the Commissioner, Hearing Officer, or Trial Board, and shall notify the Bureau of Professional Standards and Development in writing of the hearing, the forum, the employee and the proposed action.

The Bureau of Professional Standards and Development shall then set a time and date for the hearing, and shall cause notice to be served upon the employee as to time, date and forum. The notice of the hearing must be served at least three days before the hearing except in cases involving abolition of position, in which case the notice must be served at least seven days before the hearing.

Sec. 57 Postponement: Postponement of a hearing to another date may be allowed by the Commissioner, Trial Board or Hearing Officer for an adequate reason presented either by the complainant or the defendant. However, the request for such postponement must be received before the day set for the hearing. In case of such postponement, both parties shall be notified of the new hearing date at least three days in advance of the hearing. A request for a postponement for medical reasons requires a doctor's statement from a department appointed physician.

Sec. 58 Attorneys: Both the complainant and the defendant may have attorneys present to represent them at a hearing. In addition, the defendant may be accompanied by an employee organization representative.

Sec. 59 Evidence: The hearing shall be informal and administrative. The purpose of a hearing is



to determine the facts and situations surrounding a case, and members of a hearing forum, especially when counsel is not present, shall protect the rights of all parties involved whenever through the lack of ability, inexperience, or oversight, either side's case may seem to be improperly prejudiced. The rules of evidence observed by law need not be applied. Evidence which reasonable persons are accustomed to rely on in the conduct of their affairs may be considered. Unduly repetitious evidence may be excluded, and documentary evidence may be admitted in the form of copies or excerpts or by incorporation by reference. All evidence, written, oral and real, offered by the parties which is relevant to the statement of reasons shall be considered.

Sec. 60 Witnesses: Both parties may bring witnesses before the hearing. The complainant and the defendant shall be responsible for the attendance of their respective witnesses, but the Bureau of Professional Standards and Development may be requested to give reasonable assistance in securing such attendance. Witnesses, before testifying, shall be sworn or shall make an affirmation. Examination of each witness shall be made separately and apart from other witnesses, and each side shall have the opportunity to cross-examine all witnesses.

Sec. 61 The Record: The Bureau of Professional Standards and Development shall designate an employee prior to the date of the hearing to serve as clerk during the hearing. The clerk shall make a record of all testimony before the hearing and shall be responsible for marking and preserving all other evidence for the sole use of the hearing body and the Commissioner.

Sec. 62 Other Procedural Rules: The hearing forum may establish further reasonable rules to expedite the hearing. In addition, several hearings may, if appropriate and at the discretion of the Commissioner, be consolidated into one general hearing.

Sec. 63 Finding: Upon completion of the hearing, the hearing forum shall forthwith submit a written report to the Police Commissioner, with a copy to the Bureau of Professional Standards and Development. That report shall summarize the evidence introduced by the parties, make specific findings of fact, and make recommendations as to the disposition of the charges including recommendations as to the appropriate discipline if any.

The Police Commissioner shall immediately review the report of the hearing forum. He may return it for elaboration, further explanation or further hearings and findings of fact if necessary and practicable within the time limits required by law. Recommendations made by the hearing forum will not be binding on the Police Commissioner. Within seven days after the filing of the report of the hearing officer, the Police Commissioner shall give to the employee a written notice of his decision stating fully and specifically the reasons therefor.

Sec. 64 Detective Hearings:

- a. Whenever a detective is reassigned to the regular police staff, that detective shall have the right to appeal the reassignment, pursuant to the Acts of 1950, Chapter 735. A

detective who wishes to appeal must submit a notice in writing to the Police Commissioner requesting such an appeal within thirty days of the effective date of the order or reassignment.

- b. When such a notice is received, the Police Commissioner shall designate three captains to sit as members of the Trial Board after the expiration of the thirty day period following the effective date of the order or reassignment. One of the captains shall be designated as chairman and another as clerk, and an order designating the members of the Board and their duties served shall be transmitted to the Chief Clerk and to the Bureau of Professional Standards and Development.
- c. Upon receipt of the designation, the Bureau of Professional Standards and Development shall schedule the hearing and notify all interested parties of the place, date and time for the commencement of the hearing. Such notice must be received by the parties at least three days prior to the date set for the hearing.
- d. In cases where more than one member has appealed a reassignment, the appeals may be consolidated and heard by one Trial Board.
- e. The Trial Board sitting on a detective hearing shall apply the same rules governing evidence and witnesses as provided above (Sections 59 and 60), and in addition, shall also have the power to make such rules as it deems necessary to expedite the hearing.
- f. Where the assignment was the result of a complaint of misconduct or due to reasons which might impose a stigma, such as allegations of illegal conduct, the member shall be given, at the time the notice of hearing is served, a statement of charges which fairly summarizes those allegations. In addition, if the name of the complainant is known, the member shall be informed of that name. In such case, the reassignment shall be affirmed if the board finds that there is substantial evidence that the allegations are true and are sufficiently serious to reflect upon the ability of the member to perform the duties of a detective.
- g. Where the reassignment was not due to such aforesaid reason, but was an attempt to increase efficiency or economy of the Department by means of a reorganization or reallocation of manpower, or because of a member's lack of investigative ability, the reassignment shall be affirmed if the board finds there is substantial evidence that the reassignment is a good faith attempt to promote the efficiency or economy of the Department.
- h. No later than ten days after the conclusion of the hearing the board shall file its notice of decision with the Chief Clerk and the Bureau of Professional Standards and Development. If the hearing results in a change in status of the employee, the Personnel Division shall be notified by the Bureau of Professional Standards and Development. The decision shall be supported by a memorandum which shall specify reasons in support of its decision. The decision of the board as to the reassignment is final, and no provisions of Chapter 31 of the Massachusetts General Laws shall be applicable to any such hearing or determination made thereunder.
- i. The Bureau of Professional Standards and Development shall notify the parties of the result. The decision and the reasons thereof shall remain on file with the Chief Clerk and

the parties may, upon reasonable notice, inspect and copy that decision.

Sec. 65 Review From Imposition of Immediate Suspension or Punishment Duty: When an employee is suspended for five days or less or is assigned punishment duty by a commanding officer, that employee receives a written notice concerning the action within twenty-four hours. The employee may then, if so wished and within forty-eight hours of the receipt of the notice, request a hearing to determine whether there is just cause for such an action. If such a request is made, then a hearing must be held within five days of the receipt of the request by the Police Commissioner. The hearing shall be conducted using the rules procedures outlined above (Sections 56 through 62).

Within two days after the conclusion of the hearing, the Police Commissioner shall give the employee concerned a written notice of the decision. Where just cause has not been found, the discipline shall be deemed not to have been imposed and the employee shall be compensated for lost time or extra hours worked. If it is decided that just cause did exist and the employee refuses to accept such a finding, the employee shall have the right of appeal pursuant to the Massachusetts General Laws.

NOTES: Rule No. 109 was amended September 14, 1979, at which time the Bureau of Inspectional Services assumed control of procedures which the Bureau of Professional Standards and Development had previously administered.

In February, 1983, The Bureau of Professional Standards and Development was given those duties which they had originally administered.

In addition, Section No. 22 was rewritten so that the Commander of the Staff Inspection Division was given the authority to initiate procedures for a letter of reprimand to be issued.

In April, 1983, violations of Rule No. 102, sections 7 and 11, were added to Section 32 of this rule as offenses covered by the five-day suspension rule. This resulted in a renumbering of section 32.

Notes: Amended by SO 07-016, issued April 2, 2007, update the organization names to reflect the new BPD organizational structures. Sections 17, 19, 20, 24, 30, 34, 38, 41 (b,d,e,g,h), 44 (b,c,d), 46 (a,b,c), 48, 49, 52, 55, 56, 60, 61, 63, 64 (b,c,h,i).

## **Rules and Procedures**

### **Rule 113**

**May 31, 1995**

#### **Rule 113 - PUBLIC INTEGRITY POLICY**

Sec. 1 PURPOSE: The purpose of this policy is to set forth the standards of ethics which will guide both the Boston Police Department, as an organization, and its officers and employees in the conduct of their private and professional affairs.

Sec. 2 BACKGROUND: Policing in America today, especially in a major urban area, is a complex and, for many, a stressful occupation. Naturally, the police role has evolved greatly over the years. Officers now face enormous dangers to their physical and mental health. The increased level of violence and the increased level of sophistication of today's criminal present unprecedented challenges for the criminal justice system, especially for those in law enforcement. Additionally, the temptations that they face have created an added stress for the men and women who are on the front lines in the battle against crime and disorder. These temptations not only include possibilities of personal gain, monetary and otherwise, they also encompass over-zealousness in the investigation and prosecution of criminal suspects.

In order to maintain the highest standards of honesty and integrity--as a Department and as individuals--we need to attract and retain persons of outstanding character who are qualified and willing to meet the challenges of policing a diverse urban center such as Boston. Additionally, we need to correct and retrain those who have acted in a manner inconsistent with the values of the Boston Police Department and punish and/or terminate those who are unable or unwilling to act in accordance with established standards of ethical behavior.

The necessity of such a course of action--and the need to establish and articulate a public integrity policy--is undeniable given the history of problems encountered in most American police departments, especially those in large urban areas. Boston certainly has not been immune to those problems. Corruption, brutality, falsifying evidence, and bias cannot be tolerated among individuals sworn to uphold the law. Nor can hypocrisy, unfairness, deceit and discrimination be tolerated in an organization dedicated to the highest ideals of justice and the rule of law.

The Boston Police Department, mindful of its crucial role in a democratic society, has embraced those principles and values that reflect its commitment to preserving life and property while respecting the rights and dignity of all those with whom it may become involved. Accordingly, we rededicate ourselves to those principles and values by formally adopting ethical standards that will enable us to uphold the public trust. Through the adoption of this policy statement, we reaffirm our responsibility to be accountable for our actions and the conduct of our employees. By doing so, we hope to continue to merit the trust and support of the people that we have sworn to serve.

Sec. 3 POLICY: It is the policy of the Boston Police Department that every action of the Department as an organization, and those of the individuals who act on its behalf, will reflect the highest standards of honesty and integrity. In all of our dealings, whether with the public, other elements of the criminal justice system, or with each other, we will act in accordance with the ethical standards that are set forth below. Additionally, it is the responsibility of each and every member of the Boston Police Department to adhere to those standards and to take all necessary and prudent actions to expose those who knowingly violate the public trust. It is the responsibility of the Department to prevent, detect and correct instances of misconduct, administrative or criminal, within the organization.

Sec. 4 DEFINITIONS:

Integrity: Soundness of moral principles; the character of uncorrupted virtue; uprightness, honesty, self-control, courage, compassion.

Public Trust: Exercising public authority within the legal limits and according to the ends for which it was created, i.e., to serve the public interest.

Authority: The legally-granted right to issue commands or give directions to others.

Discretion: The authorized capacity to make judgments and choose from among a variety of actions, within the limits of law and Departmental policy, to resolve a problem.

Ethics: Standards or principles of conduct governing a profession; the rules of conduct or duty.

Corruption: Acts involving the misuse of authority by an employee in a manner designed to produce personal gain for himself, herself, or others.

Falsifying Evidence: Fabricating evidence that does not exist; destroying or distorting material evidence; knowingly failing to seek, discover or bring forth evidence that a reasonable person/officer would conclude might have an impact on the outcome of a matter before a court or tribunal of competent jurisdiction, and which prudence and justice dictates should be brought to the attention of a magistrate, officer of the court or hearing officer; or lying or deliberately misrepresenting the truth while under oath.

Bias: The use of authority, legal or otherwise, which results in the unequal application of the law toward some identifiable group or group member because of his/her affiliation with that group.

Employees: All sworn and civilian employees.

Supervisor: Supervisors, managers, directors and commanders.

Sec. 5 CANONS OF ETHICS: General Statement - In furtherance of this policy, the following

Canons of Ethics are adopted. They are not meant to be exclusive, but are presented because history and sound judgment indicate that violations of these canons severely undermine the ability of the Department to gain the confidence of both its employees and the public, and also negatively affect its ability to fulfill its essential mission. They are not meant to replace or supersede existing laws, special orders, rules or regulations, but to supplement them; they also serve as a reminder of the public trust that has been conferred upon the Boston Police Department by the citizens of Boston, and the need for constant vigilance in support of that trust.

Canon One: The Boston Police Department and every employee acting under its authority shall uphold the Constitution of the United States, the Constitution of the Commonwealth of Massachusetts and all laws enacted or established pursuant to legally constituted authority.

Canon Two: As a law enforcement organization, the Boston Police Department and its agents shall treat all those with whom it comes into contact, or who may seek its assistance, or who may come under its care or custody, with the respect and dignity inherent in every person.

Canon Three: As an employer, the Boston Police Department shall treat its personnel with fairness, respect, and consideration in all aspects of the job including hiring, assignment, promotion, training, collective bargaining, discipline and, when necessary, termination. It shall establish and promulgate rules, procedures and orders in such a manner as to promote professionalism, merit, and equal opportunity for advancement as well as equal access to resources. The Department shall value communication and solicit and respect the opinions of its employees on matters in which they have expertise, or which may affect their professional interests.

Canon Four: Police officers shall at all times be prepared for the proper discharge of their duties; knowledgeable in the law and legal procedures; competent in the use of authorized weapons and tactics; respectful of other elements in the criminal justice system; and possessing the necessary temperament and attitude to effect the cause of public safety and justice.

Canon Five: Employees shall be impartial in the use of their authority, providing fair access to their services and favoring no group or individual for any improper reason. They shall not allow their prejudices or biases to affect their official actions. They shall exercise their discretion so as to achieve the ends of justice and in a manner consistent with the rule of law and Departmental policy.

Canon Six: Employees shall avoid all conflicts of interests and appearances of impropriety. They shall never seek or accept gratuities when it can be construed to involve their official position within the department.

Canon Seven: Employees shall not engage in any corrupt or unlawful activity. They shall immediately report all corruption and illegal activity involving members of the Department that

may come to their attention to the Anti-Corruption Division.

Canon Eight: Employees shall conduct their private affairs so as not to reflect unfavorably on the Boston Police Department; or in such a manner as to affect their ability to perform their duties honestly, effectively, fairly, and without impairment.

Canon Nine: Police officers shall use only that amount of force reasonably necessary to achieve their lawful purpose. Excessive or unauthorized force is never justified and every officer not only has an affirmative duty to intervene to prevent such violence, but also to report any such instances that may come to their attention.

Canon Ten: Police officers shall exhibit the utmost respect for the legal rights of all. They shall not falsify evidence nor deny to anyone the equal protection of the law. They shall attend to all proceedings where their presence is necessary to the administration of justice and shall conduct themselves professionally and respectfully before any court or tribunal. Police reports and records shall adequately reflect the truth as it is known to the officer at the time they are created.

Canon Eleven: While the responsibility to uncover and report knowledge of illegal and unethical conduct belongs to all employees, regardless of rank or assignment, members of the command staff and supervisors may be personally accountable for the actions of the personnel under their command if they knew or should have known that their actions were illegal or unethical. This places upon them a specific duty to proactively prevent, detect, expose and punish improper conduct. Additionally, they shall conduct themselves in such a manner as to serve, by uncompromising adherence to these canons, as an example to those who serve under them.

Sec. 6 GENERAL RESPONSIBILITY: The Boston Police Department Rules and Procedures direct which unit or division shall have responsibility for certain areas of misconduct. Generally, the Anti-Corruption Division has responsibility for the investigation of ongoing criminal activity that involves abuse of position by an employee. Examples of that conduct are bribery, unlawful drug usage or distribution, extortion, conflict of interest, fraud and gaming.

The Internal Affairs Division is responsible for the administrative investigation of all police misconduct, including violations of the law. It is also responsible for monitoring complaint histories of all officers to identify and address those officers that may have developed a pattern of troublesome behavior, or who may be unfit or unsuitable for particular assignments. The Internal Affairs Division may also investigate licensed Special Police Officers who violate their license under Rule 400 or 400A.

Additionally, the Internal Affairs Division will ensure that the integrity and character of police applicants is considered when evaluating their fitness to become members of the Department.

Other agencies may have exclusive or concurrent jurisdiction for handling other types of

misconduct, criminal or administrative, depending on the offense and the circumstances. Current rules and directives should be consulted to determine the appropriate investigative entity or entities.

## SPECIFIC RESPONSIBILITIES

Historically, investigations of police misconduct have been reactive in nature and initiated only when the wrongdoing has been alleged or exposed for some reason. However, the Public Integrity Policy of the Boston Police Department incorporates the concept of proactive prevention to ensure that integrity is maintained in the organization at all times. Accordingly, specific responsibility is assigned to certain units, and the commanders and supervisors of those units. Additionally, those units or individuals will be held accountable for maintaining integrity in those areas of responsibility.

The following procedures and processes are instituted to assure that the goals of this policy are implemented by clearly defining areas of responsibilities.

### 1. The Anti-Corruption Division

Officers of the Anti-Corruption Division will be responsible for handling corruption prevention programs as well as proactive and reactive investigations. Specifically, they will:

- A. Review monthly summations of citizen and internal complaints for indicators of misuse of authority by a Department employee or misuse of City of Boston employee status for personal gain.
- B. Review the findings of Internal Affairs investigations for patterns of conduct which are indicative of corrupt police behavior.
- C. As appropriate, cooperate in the investigation of any City of Boston employee with or by any other agency including state, local, or federal authorities, offices of the various district attorneys, the office of the U.S. Attorney or the office of the Attorney General of the Commonwealth.

The commanding officer of the Anti-Corruption Division shall be responsible for determining whether an investigation will be conducted solely by the Anti-Corruption Division or cooperatively with another unit, division, district, or area within the Department. In any event, the Anti-Corruption Division will maintain an oversight role in any criminal or corruption related investigation of any Department employee.

- D. Review the results of department inspection and audit reports to specifically identify indicators of corruption.
- E. Operate a reporting method for citizens and Department/City of Boston employees to report behavior indicative of corruption.
- F. Immediately notify the Police Commissioner through the Chief, Bureau of Professional Standards and Development when a suspicion of significant corruption enters an investigation. Inform an employee's commanding officer of such a suspicion as soon as



possible when such notification would not negatively impact an on-going investigation and/or prosecution. Upon the arrest, indictment, or commencement of any other criminal proceeding the Anti-Corruption Division shall notify the following:

- 1.The Police Commissioner
- 2.Chief, Bureau of Internal Investigations
- 3.Employee's Bureau Chief
4. Employee's Commanding Officer

G. Coordinate, in cooperation with the Commander of the Training and Education Division, in the development and conducting of informational and educational sessions for members of the Department as may be deemed appropriate by the Chief, Bureau of Professional Standards and Development or the Police Commissioner.

H. Be notified and review its records before a personnel order is issued promoting, transferring, commending, or rating Department personnel. After such review, the Anti Corruption Division will notify the Chief, Bureau of Professional Standards and Development concerning the status of active investigations or complaints sustained.

I. Ensure that criminal or corruption related investigations of Department employees will be conducted in full conformance with the rules and procedures of the Boston Police Department, state and federal laws and court decisions, especially as they relate to employee's rights and protections against self-incrimination. Investigations will be conducted without regard to influences, pressures, or mandates from those who would improperly seek to affect the outcome of any investigation.

J. Have the option to coordinate any prosecution in a criminal court involving a Department employee with the appropriate district attorney's office, the Office of the Attorney General of the Commonwealth, or the Office of the United States Attorney.

K. Maintain records, files, and other data as appropriate to the proper functioning of the Division. Such information shall be only accessible to officers of the Anti-Corruption Division, the Chief of the Bureau of Professional Standards and Development and the Police Commissioner. Anonymity and confidentiality, where appropriate, shall be respected and strictly adhered to.

The mission of the Anti-Corruption Division shall not be limited to investigations of allegations of corruption or criminality on the part of employees of the Boston Police Department, but may include investigations of any agency, department, division and its employees of the City of Boston as may be deemed appropriate by the Police Commissioner. Further, the Anti-Corruption Division shall be authorized to conduct any other investigation as may be directed by the Police Commissioner.

## 2. The Internal Affairs Division

The Internal Affairs Division shall be required to immediately notify the Anti-Corruption Division concerning any allegation of corruption or serious criminal activity reported to them or uncovered during the course of any internal affairs investigation.

On a monthly basis it shall submit a report to the Chief of the Bureau of Professional Standards

and Development containing information that may assist in determining whether patterns of corruption may be developing. Specifically, the report shall contain the following information for the preceding month:

- Names of Department employees complained against;
- the nature of the complaint, and;
- prior complaints (and dispositions) for each employee complained against.

This report will be forwarded to the Anti-Corruption Division for review and analysis for potential linkage to ongoing Anti-Corruption Division investigations.

### 3. Supervisors

Supervisors will be accountable for the foreseeable or preventable illegal conduct of those employees under their assigned area of supervision or command.

Supervisors are responsible for reporting any suspicious behavior which they knew or should have known was indicative of corruption. This behavior may include duty-related activities, personal or off-duty related activities, or personal patterns of conduct that may come to their attention through any means.

Commanders are responsible for monitoring the activities of their subordinate supervisors, especially in regard to the supervisor's concern for accountability and integrity within his/her respective unit or area of supervision.

### 4. All Officers and Employees

The established and published values of the Boston Police Department are applicable to all Department employees. All Department employees are responsible for reporting other Department employees whose behavior is clearly illegal or who exhibit behavior that a reasonable and prudent employee would clearly judge to be indicative of illegal activity.

All Department employees are required to fully cooperate in any investigation being conducted by the Anti-Corruption Division without regard to the conventional requirements of the chain of command. Said cooperation shall include, but is not limited to, providing the Anti-Corruption Division with any oral or written reports required by investigators, taking into consideration any and all protections against self-incrimination; any and all records, documents, or any other items of evidentiary or investigative value known to the employee or requested by Anti Corruption Division investigators.

**Sec. 7 RESPONSE AND REPORTING PROCEDURES:** Whenever any Department employee receives a complaint, or is made aware of a complaint through any means--whether written, oral, identified complainant or anonymous; or whenever any Department employee is made aware of any criminal activities or allegations of corruption by any Department member(s) or other City of Boston employee(s); the employee shall adhere to the following procedures:

- a. Notify a sworn member of the Anti-Corruption Division, within 24 hours of being made aware of the activity or allegation by calling the Anti-Corruption Division (617)343-4366. If it is after normal business hours or sworn personnel are unavailable, then a message and return telephone number should be left and the call will be forwarded to an on-call investigator who will return the call forthwith.
- b. Following oral notification, the employee shall submit within 24 hours a written report detailing his/her knowledge of the relevant activities or allegations directly to the Commander of the Anti-Corruption Division. Normal chain-of-command requirements and formal procedures pursuant to Rule 109 are specifically exempt from those situations covered by this rule.
- c. Subsequent communications regarding such activities or allegations shall only be between the employee and the Anti-Corruption Division directly unless the Police Commissioner, the Chief of the Bureau of Professional Standards and Development or the Commander of the Anti-Corruption Division determines otherwise.
- d. Refrain from discussing a matter referred to the Anti-Corruption Division with any other individual(s) without the consent and knowledge of the Police Commissioner, the Chief of the Bureau of Professional Standards and Development or the Commander of the Anti-Corruption Division.

The reporting requirements, as set forth in this section, shall not be construed as abrogating the responsibility of a sworn member of the Department from taking appropriate action as required by law or dictated by prudence and the exercise of sound judgment, when confronted with a situation involving criminal acts.

The criminal investigation of allegations of corruption and/or criminal behavior shall take precedence over any administrative disciplinary proceeding or investigation. However, such criminal investigation shall not preclude the Department from proceeding administratively against an employee provided that the administrative investigation or proceeding does not compromise a criminal investigation.

Sec. 8 Information regarding investigations of corruption or alleged criminal activity by members of the Department will be released to the public and media if deemed appropriate by the Police Commissioner or the Chief of the Bureau of Internal Investigations.

Sec. 9 Failure to follow the reporting requirements of this rule and any other applicable rules, or violation of any other section, may result in disciplinary action, up to and including termination.

Notes:

- Amended by SO 07-016, issued April 2, 2007, update the organization names to reflect the new BPD organizational structures. Section 6 (1) (B,F,G,H,K) and (2), Section 7 (C,D), Section 8.



**Police Commissioner's Special Order**

Number: SO 21-24

Date: May 25, 2021

Post/Mention: Indefinite

**SUBJECT: RULE 113A, BIAS-FREE POLICING POLICY**

Rule 113A, Bias-Free Policing Policy is hereby issued superseding all previous rules, special orders, memos and directives on this subject.

This rule is effective immediately.

As part of the Boston Police Department's ongoing commitment to police reform Rule 113A Bias Free Policing has been updated based on Massachusetts Police Reform Legislation and the recommendations of Mayor Walsh's Task Force on Police Reform. The Department also used the International Association of Chiefs of Police (IACP) model bias-free policing policy as a guide, adapting their format and language to fit the BPD. This policy has been reviewed by an internal BPD DEI committee as well as the Mayor's Office of Equity.

Commanding Officers shall ensure that this order and the attached Rule are posted on Department bulletin boards.

Gregory P. Long  
Superintendent In Chief

**Boston Police Department**

**Rules & Procedures**

**Rule 113A**

**May 25, 2021**

**BIAS-FREE POLICING POLICY**

**Section 1. General Considerations**

The Boston Police Department is committed to building and strengthening trust with all members of the community. Actual or perceived bias by police undermines this trust and damages relationships with the community – relationships that are at the heart of an effective community policing approach. Bias practices are unfair, ineffective, promote mistrust, and perpetuate negative and harmful stereotypes. The Department recognizes that bias can occur at both an individual and an institutional level. All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. The Boston Police Department is committed to bias-free policing.

**Section 2. Policy**

All people having contact with Boston Police Department personnel shall be treated in a fair, impartial, bias-free, and objective manner, in accordance with law, and without consideration of specified characteristics as defined in this policy.

**Section 3. Purpose**

The purpose of this policy is to emphasize the Boston Police Department's commitment to fair and bias-free treatment of all people and to clarify the circumstances in which Department personnel may consider specified characteristics when carrying out duties. Fair and bias-free policing enhances legitimate law enforcement efforts and promotes trust within the community.

**Section 4. Definitions**

**Sec. 4.1 Bias-free Policing**, as defined by MGL Chapter 6E Section 1:

“**Bias-free policing**”, policing decisions made by and conduct of law enforcement officers that shall not consider a person's race, ethnicity, sex, gender identity, sexual orientation, religion, mental or physical disability, immigration status or socioeconomic or professional level. This definition shall include policing decisions made by or conduct of law enforcement officers that: (1) are based on a law enforcement purpose or reason which is non-discriminatory, or which justifies different treatment; or (2) consider a person's race, ethnicity, sex, gender identity, sexual orientation, religion, mental or physical disability, immigration status or socioeconomic or professional level because such factors are an element of a crime.

**Sec. 4.2 Biased Policing:** Discrimination in the performance of law enforcement duties or delivery of police services, based on personal prejudices or partiality of department personnel toward classes of people based on specified characteristics.

**Sec. 4.3 Police Services:** Includes the full spectrum of police interactions with the community in the service of public safety. This includes law enforcement, community policing, community engagement, and partnerships with governmental and non-governmental organizations.

**Sec. 4.4 Specified Characteristics:** For the purposes of this policy, real or perceived personal characteristics, to include but not limited race, ethnicity, sex, gender identity, sexual orientation, religion, mental or physical disability, immigration status or socioeconomic or professional level. (Per MGL Chapter 6E Section 1 definition of bias-free policing listed above.)

## **Section 5. Fair and Impartial Treatment: Use of Personal Characteristics in Law Enforcement Activities**

Per MGL Chapter 6E Section 1, bias-free policing includes “policing decisions made by or conduct of law enforcement officers that: (1) are based on a law enforcement purpose or reason which is non-discriminatory, or which justifies different treatment; or (2) consider a person’s race, ethnicity, sex, gender identity, sexual orientation, religion, mental or physical disability, immigration status or socioeconomic or professional level because such factors are an element of a crime.” (See definition of bias-free policing in Section 4.)

1. Biased policing is prohibited both in enforcement of the law and the delivery of police services.
2. Department personnel shall take equivalent enforcement actions and provide bias-free services to all people in the same or similar circumstances. This does not mean that all people in the same or similar circumstances must be treated identically. Reasonable concessions and accommodations may be, and sometimes should be made, for example when dealing with people with disabilities, injury, or illness.
3. Department personnel may only consider specified characteristics when credible, timely intelligence relevant to the locality links a person or people with a specified characteristic(s) to a particular unlawful incident, or to particular unlawful incidents or criminal patterns.
4. Restrictions on the use of specified characteristics do not apply to law enforcement activities designed to strengthen the agency’s relationship with its diverse communities.

## **Section 6. Training**

All sworn Department personnel will receive periodic in-service training and, where deemed necessary, remedial training on subjects related to fair and bias-free policing, to include legal aspects and the psychology of bias.

## **Section 7. Compliance: Supervision and Discipline**

1. Where appropriate, Department personnel are encouraged to intervene at the time the biased policing incident occurs. Department personnel who witness or who are aware of instances of biased policing shall report the incident to their immediate supervisor. 2. Supervisors shall:

- a. Ensure that all Department personnel in their command are familiar with the content of this policy and shall be alert and respond to indications that biased policing is occurring.
- b. Respond to violations of this policy with training, counseling, discipline, or other remedial intervention as appropriate to the violation.
- c. Ensure that those who report instances of biased policing are not subject to retaliation. 3.

Information on biased-policing complaints and any additional relevant information shall be provided to the Police Commissioner in a manner most suitable for administrative review, problem assessment, and development of appropriate officer-level and/or agency-level corrective actions. At least annually, a summary of biased-policing complaints will be provided to the Police Commissioner.

## **Section 8. Transparency and Accountability**

The Department is committed to an ongoing and open dialogue with community leaders to ensure that it is engaging in bias-free policing. The Department is committed to community policing in all of the City's neighborhoods, proactively engaging with youth, families and community members to build lasting relationships, solve problems, and prevent crime.

The Department is committed to continuing analysis and public release of data related to documented police interactions with community members. The Boston Police Department Accountability and Transparency webpage on [boston.gov](http://boston.gov) with associated interactive data dashboards will be an important tool for review and analysis and provides transparency to the community.

Gregory P. Long  
Superintendent In Chief

## **Rules and Procedures**

### **Rule 200**

**August 16, 2002**

#### **C Rule 200 - CRITICAL INCIDENT MANAGEMENT**

This Rule is issued to establish the policy of the Boston Police Department for its response to and management of all Critical Incidents with special attention to the management of special circumstances. The purpose of the policy is to provide guidelines to the entire Department for the operation and management of Critical Incidents while maintaining compatibility with the Incident Command System (ICS) to efficiently manage resources and plan for the tactical resolution of an incident. In addition to having the flexibility to expand or contract as the needs of an incident require, ICS allows for the practical inclusion of outside agencies in the planning and operational process with clearly definable roles and common terminology assuring a properly coordinated effort.

##### **Sec. 1.0 Incident Command System - An Overview**

The Incident Command System (ICS) is a management system which has the flexibility and adaptability to be applied to a wide variety of incidents and events both small and large. The individual designated as the Incident Commander (IC) has responsibility for all ICS management functions. Those functions and their responsibilities are as follows:

1. Command - The IC is responsible for all incident or event activity. Although some functions may be left unfilled with those duties being wielded by the IC, there will always be an Incident Commander;
2. Operations - The Operations Section is responsible for directing the tactical actions to meet incident objectives;
3. Planning - The Planning Section is responsible for the collection, evaluation, and display of incident information, maintaining status of resources, and preparing the Incident Action Plan and incident-related documentation;
4. Logistics - The Logistics Section is responsible for providing adequate services and support to meet all incident or event needs; and
5. Finance/Administration - The Finance/Administration Section is responsible for keeping track of incident-related costs, personnel and equipment records and administering procurement contracts associated with the incident or event.

The Incident Commander can elect to perform all the above functions or each of these functional areas can be delegated and expanded as needed into additional organizational units with further delegation of authority.



### Sec. 1.1 Management by Objectives:

With ICS, every incident, regardless of size or complexity, must include the following:

1. A solid understanding of Department policy and direction;
2. The establishment of incident objectives;
3. The selection of an appropriate strategy; and
4. The application of tactics appropriate to the strategy, assigning the right resources and monitoring of performance.

### Sec. 1.2 Unity and Chain of Command:

In ICS, Unity of Command means that every individual has only one designated supervisor. Chain of Command means that there is a line of authority within the ranks of the organization with lower levels subordinate to and connected to, higher levels. In the vast majority of incidents, the command structure will consist only of:

1. Command; and
2. Single resource(s)

However, as incidents expand in size and complexity, the Chain of Command is expanded through an organizational structure which can consist of as many layers as needed, such as:

1. Command;
2. Sections;
3. Branches;
4. Divisions/Groups;
5. Units; and
6. Resources.

### Sec. 1.3 Establishment and Transfer of Command:

Command at an incident is initially the responsibility of the highest ranking person on scene from the agency which has jurisdiction over the incident. Transfer of Command at an incident occurs for any of the following reasons:

1. A higher ranking or more qualified person assumes command;
2. The incident situation changes over time to where a jurisdictional or agency change in command either is legally required or it would make good management sense to make such a transfer; or
3. There is a normal turnover of personnel on long or extended incidents.

#### Sec. 1.4 Organizational Flexibility:

Flexibility is key to the proper functioning of ICS. At any given time, the structure and organization of an incident should reflect only what is required to meet planned tactical objectives with the size of the current organization and that of the next operational period being determined through the incident action planning process.

Depending on the complexity and scope of an incident, a number of organizational elements may be activated in the various sections without designating individual section chiefs. The IC may decide to perform all or some management functions, while appointing section chiefs to others. Although each activated element must have a person in charge of it, a single person may initially command more than one unit.

Elements which have been activated and which are clearly no longer needed are deactivated to decrease organizational size.

#### Sec. 1.5 Unified Command:

Unified Command is an ICS management process which allows all agencies who have jurisdictional or functional responsibility for the incident to jointly develop a common set of incident objectives and strategies. This is accomplished without losing or giving up agency authority, responsibility or accountability.

Allowing all agencies who have a legitimate responsibility at an incident to be part of the Incident Command function is an important part of ICS. Under a Unified Command the following always applies:

1. The incident will function under a single coordinated (jointly decided upon) Incident Action Plan;
2. One Operations Section Chief will have responsibility for implementing the Incident Action Plan; and
3. One Incident Command Post will be established.

#### Sec. 1.6 Span of Control:

Span of Control means the number of individuals that one supervisor can effectively manage. Maintaining an effective Span of Control is particularly important on incidents where safety and accountability are a top priority.

In ICS, the Span of Control for any supervisor should fall within a range of three to seven with five being the optimum number. Any time a supervisor has fewer than three people reporting, or more than seven, some adjustment to the organization should be considered.

#### Sec 1.7 Common Terminology:

Because ICS may evolve into a Unified Command involving different agencies with various multi-agency terms, it is important to use common terminology to avoid confusion. In ICS, common terminology is applied to:

1. Organizational Elements - There is a consistent pattern for designating each level of the organization, e.g., sections, branches, et cetera.
2. Position Titles - Those charged with management or leadership responsibility in ICS are referred to by an ICS position title such as Officer, Chief, Director, Supervisor, et cetera. This is done to provide a way to place the most qualified personnel in organizational positions on multi-agency incidents without confusion caused by various multi-agency rank designations. It also provides a standardized method for ordering personnel to fill positions.
3. Resources - Common designations are assigned to various kinds of resources. Resources may also be further classified by type and type classification, e.g., a vehicle used in fire suppression would be classified as an engine, but would also be classified by type, tank capacity, staffing level, et cetera.

#### Sec. 1.8 Personnel Accountability:

ICS ensures personnel accountability through the following:

1. Check-In - Requires all personnel to check-in upon arrival at an incident;
2. Unity of Command - Ensures everyone has only one supervisor;
3. Resource Status Unit - Maintains the status of all assigned resources;
4. Division/Group Assignment Lists - Identifies resources with active assignments in the Operations Section; and
5. Unit Logs - includes a record of personnel assigned and of major events occurring in all ICS organizational elements.

#### Sec. 1.9 Integrated Communications:

The ability to effectively communicate within ICS is absolutely critical. There are at least three ways to view the communications issues that must be solved:

1. The "hardware" systems that transfer information;
2. The planning that must occur for the use of all available communications frequencies and resources; and
3. The actual procedures and processes for transferring information.

Effective communication during every Critical Incident requires a Communications Plan. Depending on the complexity of the incident and the number of agencies involved, the communications plan can be simple or complex and involve several different communication networks. These may include:

1. Command Net - Established to link supervisory personnel from Incident Commander down to and including Division and Group supervisors;
2. Tactical Nets - Established in various ways, e.g., by agency, department, geographical area or function. Tactical nets may be established for each branch or for Divisions and groups, depending upon hardware and frequency availability and specific incident needs;
3. Support Nets - Established on larger incidents to handle logistics traffic and resource status changes;
4. Ground-to-Air - Established to coordinate ground-to-air traffic; and
5. Air-to-Air - Assigned for coordination between aircraft assigned to an incident.

An awareness of available communications systems and frequencies, combined with an understanding of incident requirements, will enable the Communications Unit Leader to develop an effective Communications Plan for each operational period.

To ensure that all personnel understand clearly the information that is being transmitted, especially in a multi-agency incident management system, all transmissions will be in clear text without the use of radio codes (or miscels).

#### Sec. 1.10 Resources Management:

Resources assigned to an incident are categorized in one of the following ways:

1. Single Resources - Single Resources include both personnel and their assigned equipment.
2. Task Forces - Task Forces refer to any combination of single resources within span of control guidelines. They are assembled for a particular tactical need, with common communications and a leader. Task Forces can be pre-determined or assembled at an incident from available single resources.
3. Strike Teams - Strike Teams are combinations of a designated number of the same kind and type of resources with common communications and a leader. The number of resources to be used in the team will be based on what is needed to perform the function. Span of control guidelines should apply. Strike Teams can be pre-determined or assembled at an incident from available single resources.

Advantages of the use of both Task Forces and Strike Teams are:

1. Maximization of the effective use of resources;
2. Reduction in the span of control; and
3. Reduction in communications traffic.

Tactical Resources assigned to an incident will always be in one of three status conditions:

1. Assigned - Resources are performing an active assignment;

2. Available - Resources are ready for deployment, but not assigned; or
3. Out of Service - Resources are not available.

#### Sec. 1.11 Incident Action Plan:

Every incident must have an Incident Action Plan, oral or written, which shall provide all incident supervisory personnel with appropriate direction for future actions.

Written plans should be used when it is essential that all levels of a growing organization have a clear understanding of the tactical actions associated with the next operational period. It is important to use written action plans whenever:

1. Two or more jurisdictions are involved;
2. The incident will overlap major changes in personnel changes or go into a new operational period;
3. There is a partial or full activation of the ICS organization.

For smaller incidents, an ICS Incident Briefing Form may be used to record initial actions and list assigned and available resources. A more formal written Incident Action Plan, based on an ICS format, is necessary as incidents grow in size and/or complexity.

#### Sec. 2.0 ICS Position Responsibilities

The ICS organization develops around five major functions that are required on any incident whether it is large or small. For some incidents, and in some applications, only a few of the organization's functional elements may be required. However, if there is a need to expand the organization, additional positions exist within the ICS framework to meet virtually any need.

ICS establishes lines of supervisory authority and formal reporting relationships. There is complete unity of command as each position and person within the system has a designated supervisor. Direction and supervision follows established organizational lines at all times. The following are the major responsibilities and duties of all ICS positions. Individual agencies may have additional responsibilities and more detailed lists of duties.

#### Sec. 2.1 Incident Commander (IC) and ICS Command Staff:

The Incident Commander and the ICS Command Staff consist of the following:

1. Incident Commander
2. Information Officer
3. Liaison Officer
4. Agency Representatives
5. Safety Officer

## Sec 2.11 Responsibilities of the Incident Commander

1. Assess the situation and/or obtain a briefing from the prior IC;
2. Determine incident objectives and strategy;
3. Establish the immediate priorities;
4. Establish an Incident Command Post;
5. Establish an appropriate organization;
6. Ensure planning meetings are scheduled as required;
7. Approve and authorize the implementation of an Incident Action Plan;
8. Ensure that adequate safety measures are in place;
9. Coordinate activity for all Command and General Staff;
10. Coordinate with key people and officials;
11. Approve requests for additional resources or for the release of resources;
12. Keep agency administrator informed of incident status;
13. Approve the use of trainees, volunteers and auxiliary personnel;
14. Authorize release of information to the news media; and
15. Order the demobilization of the incident when appropriate.

## Sec. 2.12 Responsibilities of Incident Command Staff

### 1. Information Officer

The Information Officer is responsible for developing and releasing information about the incident to the news media, to incident personnel and to other appropriate agencies and organizations.

Only one Information Officer will be assigned for each incident, including incidents operating under a Unified Command and multi-jurisdiction incidents. As necessary, the Information officer may have assistants, who may or may not represent assisting agencies or jurisdictions.

The following are the major responsibilities of the Information Officer which would generally apply on any incident:

1. Determine from the IC if there are any limits on information release;
2. Develop material for use in media briefings;
3. Obtain the approval of the IC on all media releases;
4. Inform the media and conduct media briefings;
5. Arrange for tours and other interviews or briefings that may be required;
6. Obtain media information that may be useful to incident planning;
7. Maintain current information summaries and/or displays on the incident and provide information on status of incident to assigned personnel; and
8. Maintain Unit Log.

## 2. Liaison Officer

Incidents that are multi-jurisdictional, or have several agencies involved, may require the establishment of the Liaison Officer position on the Command Staff. The Liaison Officer is the contact for the personnel assigned to the incident by assisting or cooperating agencies. These are personnel other than those on direct tactical assignments or those involved in a Unified Command.

Liaison Officer major responsibilities and duties are:

1. Be a contact point for Agency Representatives;
2. Maintain a list of assisting and cooperating agencies and Agency Representatives;
3. Assist in establishing and coordinating interagency contacts;
4. Keep agencies supporting the incident aware of incident status;
5. Monitor incident operations to identify current or potential inter-organizational problems;
6. Participate in planning meetings, providing current resource status, including limitations and capability of assisting agency resources; and
7. Maintain a Unit Log.

## 3. Agency Representatives

In many multi-jurisdictional incidents, an agency or jurisdiction will send a representative to assist in coordination efforts. Known in ICS as an Agency Representative, this person is an individual assigned to an incident from an assisting or cooperating agency who has been delegated authority to make decisions on matters affecting that agency's participation at the incident. Agency Representatives report to the Liaison Officer, or in the absence of the Liaison Officer, to the Incident Commander.

Responsibilities of an Agency Representative are:

1. Ensure that all agency resources are properly checked-in at the incident;
2. Obtain briefing from the Liaison Officer or the IC;
3. Inform assisting or cooperating agency personnel on the incident that they are appointed as the Agency Representative for that agency;
4. Attend briefings and planning meetings as required;
5. Provide input on the use of agency resources unless resource technical specialists are assigned from the agency;
6. Cooperate fully with the Incident Commander and the General Staff on agency involvement at the incident;
7. Ensure the well-being of agency personnel assigned to the incident;
8. Advise the Liaison Officer of any special agency needs or requirements;
9. Report to home agency dispatch or headquarters on a pre-arranged schedule;

10. Ensure that all agency personnel and equipment are properly accounted for and released prior to departure;
11. Ensure that all required agency forms, reports and documents are complete prior to departure; and
12. Have a debriefing session with the Liaison Officer or Incident Commander prior to departure.

#### 4. Safety Officer

The Safety Officer's function is to develop and recommend measures for assuring personnel safety and to assess and/or anticipate hazardous and unsafe situations.

Only one Safety Officer will be assigned for each incident. The Safety Officer may have assistants who may or may not represent assisting agencies or jurisdictions. Safety Assistants may have specific responsibilities such as hazardous materials, air operations, et cetera.

Responsibilities of the Safety Officer are:

1. Participate in planning meetings;
2. Identify hazardous situations associated with the incident;
3. Review the Incident Action Plan for safety implications;
4. Exercise emergency authority to stop and prevent unsafe acts;
5. Investigate accidents that have occurred within the incident area;
6. Assign assistants as needed;
7. Review and approve the medical plan; and
8. Maintain a Unit Log.

#### Sec. 2.2 ICS General Staff Positions:

The General Staff consists of the following positions:

1. Operations Section Chief
2. Planning Section Chief
3. Logistics Section Chief
4. Finance Administration Section Chief

#### Sec. 2.21 Operations Section

The Operations Section is responsible for the direction and coordination of all incident tactical operations. This is done under the direction of the Operations Section Chief. The Operations Section may consist of Single Resources or be further subdivided into Branches, Division/Groups and Task Force/Strike Teams, as the needs of the incident require.



Tasks and responsibilities within the Operations Section may be divided along functional lines, geographic areas or a combination of both.

1. Responsibilities of the Operations Section Chief are:

1. Manage tactical operations;
  1. Interact with next lower level of Section (Branch, Division/Group) to develop the operations portion of the Incident Action Plan; and
  2. Request resources needed to implement the Operation's tactics as a part of the Incident Action Plan development.
2. Assist in development of the operations portion of the Incident Action Plan;
3. Supervise the execution of the Incident Action Plan for Operations;
  1. Maintain close contact with subordinate positions; and
  2. Ensure safe tactical operations.
4. Request additional resources to support tactical operations;
5. Approve release of resources from assigned status (may not release from the incident);
6. Make or approve expedient changes to the Incident Action Plan during the Operational Period as necessary;
7. Maintain close communication with the Incident Commander; and
8. Maintain a Unit Log.

2. Responsibilities of Branch Director (Branches may be functional or geographic)

1. Obtain briefing from the Operations Section Chief;
2. Supervise Branch operations;
3. Develop alternatives for Branch control operations;
4. Interact with the Operations Section Chief and other Branch Directors to develop tactics to implement incident strategies;
5. Be prepared to attend incident planning meetings at the request of the Operations Chief;
6. Review Division/Group assignments within the Branch and report status to the Operations Section Chief;
7. Monitor and inspect progress and make changes as necessary;
8. Resolve logistics problems reported by subordinates; and
9. Maintain a Unit Log.

3. Responsibilities of Division/Group Supervisor

1. Obtain briefing from the Operations Section Chief or appropriate Operations Branch Director;
2. Review assignments with subordinates;
3. Inform Resource Unit (if established) of status changes of resources assigned to the Division/Group;
4. Coordinate activities with adjacent Divisions/Groups;

5. Monitor and inspect progress and make changes as necessary;
6. Keep supervisor informed of situation and resources status;
7. Resolve tactical assignment and logistics problems within the Division/Group;
8. Keep supervisor informed of hazardous situations and significant events;
9. Ensure that assigned personnel and equipment get to and from their assignments in a timely and orderly manner; and
10. Maintain a Unit Log.

#### 4. Responsibilities of Task Force/Strike Team Leader

1. Obtain briefing from supervisor (Division/Group Supervisor, Operations Section Chief or Incident Commander - depending upon how the incident is organized);
2. Review assignment with subordinates and assign tasks;
3. Travel to and from active assignment area with assigned resources;
4. Monitor and inspect progress and make changes as necessary;
5. Coordinate activities with any adjacent Task Force/Strike Team, single resources or functional group working in the same location;
6. Keep supervisor advised of situation and resource status;
7. Retain control of assigned resources while in available or out-of-service status; and
8. Maintain a Unit Log.

#### 5. Responsibilities of person in charge of a Single Resource

The person in charge of a single tactical resource will carry the unit designation of the resource.

1. Obtain briefing from the Division/Group Supervisor or Task Force/Strike Team Leader;
2. Review assignments;
3. Obtain necessary equipment/supplies;
4. Review weather/environmental conditions for assignment area;
5. Brief subordinates on safety measures;
6. Monitor work progress;
7. Ensure adequate communications with supervisor and subordinates;
8. Keep supervisor informed of progress and any changes;
9. Inform supervisor of problems with assigned resources;
10. Brief relief personnel and advise them of any change in conditions;
11. Return equipment and supplies to appropriate unit; and
12. Complete and turn in all time and use records on personnel and equipment.

#### 6. Responsibilities of a Staging Area Manager

Whenever an incident is not large enough for a Logistics Section to be activated, the

Staging Area Manager reports to the Operations Section Chief (or to the Incident Commander if the Operations Section Chief position has not been filled).

1. Establish layout of the Staging Area(s);
2. Post areas for identification and traffic control;
3. Provide check-in for incoming resources;
4. Determine required resource reserve levels from the Operations section Chief or Incident Commander;
5. Advise the Operations Section Chief or Incident Commander when reserve levels reach minimums;
6. Maintain and provide status to Resource Unit of all resources in Staging Area(s);
7. Respond to Operations Section Chief or Incident Commander requests for resources;
8. Request logistical support for personnel and/or equipment as needed;
9. Maintain Staging Area in an orderly condition;
10. Demobilize or move Staging Area(s) as required; and
11. Maintain a Unit Log.

#### Sec. 2.22 Planning Section

The Planning Section collects, evaluates, processes and disseminates information for use at the incident. When activated, the Planning Section is managed by the Planning Section Chief who is a member of the General Staff.

The four units within the Planning Section that can be activated as necessary are:

1. Resources Unit
2. Situation Unit
3. Documentation Unit
4. Demobilization Unit

#### 1. Responsibilities of Planning Section Chief

1. Collect and process situation information about the incident;
2. Supervise preparation of the Incident Action Plan;
3. Provide input to the Incident Commander and Operations Section Chief in preparing the Incident Action Plan;
4. Reassign out-of-service personnel already on-site to ICS organizational positions as appropriate;
5. Establish information requirements and reporting schedules for Planning Section units (e.g., Resources, Situation Units);
6. Determine need for any specialized resources in support of the incident;
7. If requested, assemble and disassemble strike teams and task forces not assigned to operations;

8. Establish special information collection activities as necessary, e.g., weather, environmental, toxic, et cetera;
9. Assemble information on alternative strategies;
10. Provide periodic predictions on incident potential;
11. Report any significant changes in incident status;
12. Compile and display incident status information;
13. Oversee preparation of Incident demobilization plan;
14. Incorporate the incident traffic plan (from Ground Support) and other supporting plans into the Incident Action Plan; and
15. Maintain a Unit Log.

## 2. Unit Leaders - Common Responsibilities

In ICS, a number of Unit Leader responsibilities are common to all units in all parts of the organization. Instead of repeating them within the responsibilities of each Unit Leader, the Common responsibilities of all Unit Leaders listed below are:

1. Obtain briefing from Section Chief;
2. Participate in incident planning meetings, as required;
3. Determine current status of unit activities;
4. Confirm dispatch and estimated time of arrival of staff and supplies;
5. Assign specific duties to staff; supervise staff;
6. Develop and implement accountability, safety and security measures for personnel and resources;
7. Supervise demobilization of unit, including storage of supplies;
8. Provide Supply Unit Leader with a list of supplies to be replenished; and
9. Maintain unit records, including a Unit Log.

## 3. Responsibilities of Resources Unit

In addition to the common Unit responsibilities listed above, this Unit is responsible for maintaining the status of all assigned resources (primary and support) at an incident by:

1. Overseeing the check-in of all resources;
2. Maintaining a status-keeping system indicating current location and status of all resources; and
3. Maintenance of a master list of all resources, e.g., key supervisory personnel, primary and support resources, et cetera.

## 4. Responsibilities of Situation Unit

In addition to the common Unit responsibilities listed above, this Unit is responsible for the collection, processing and organizing of all incident information. The Situation Unit may prepare future projections of incident growth, maps and intelligence information.

1. Beginning collection and analysis of incident data as soon as possible;

2. Collecting, processing and organizing all incident information;
3. Preparing, posting or disseminating resource and situation status information as required, including special requests;
4. Preparing future projections of incident growth, maps and intelligence information;
5. Preparing predictions, periodically or as requested;
6. Preparing the incident status summary; and
7. Providing photographic services and maps, as required.

#### 5. Responsibilities of Documentation Unit

In addition to the common Unit responsibilities listed above, this Unit is responsible for:

1. Sets up work area and begin organization of incident files.
2. Establish and provide duplication services.
3. File all official forms and reports.
4. Review records for accuracy and completeness and inform appropriate units of errors or omissions.
5. Provide incident documentation as required.
6. Store files for post-incident use.
7. Maintain accurate, up-to-date incident files, which shall be stored for legal, analytical, and historical purposes.

#### 6. Demobilization Unit

On large incidents, demobilization can be quite complex, requiring a separate planning activity. Note that not all agencies require specific demobilization instructions.

In addition to the common responsibilities listed above, this Unit is responsible for:

1. Review incident resource records to determine the likely size and extent of demobilization effort.
2. Develop the Incident Demobilization Plan.
3. Add additional personnel, workspace and supplies as needed.
4. Coordinate demobilization with Agency Representatives.
5. Monitor ongoing Operations Section resource needs.
6. Identify surplus resources and probable release time.
7. Develop incident checkout functions for all units.
8. Evaluate logistics and transportation capabilities to support demobilization.
9. Establish communication with off-incident facilities.
10. Develop an incident demobilization plan detailing specific responsibilities and release priorities and procedures.
11. Prepare appropriate directions (e.g., maps, instructions, etc.) for inclusion in the Demobilization Plan.
12. Distribute Demobilization Plan (on and off site).

13. Ensure that all Sections/Units understand their specific demobilization responsibilities.
14. Supervise execution of the Incident Demobilization Plan.
15. Brief Planning Section Chief on the Demobilization Plan.

## 7. Technical Specialists

Certain incidents or events may require the use of Technical Specialists who have specialized knowledge and expertise. Technical Specialists may function within the Planning Section, or be assigned wherever their services are required. In the Planning Section, Technical Specialists may report to either the Planning Section Chief or the Designated Unit Leader.

## Sec. 2.23 Logistics Section

With the exception of aviation support, all incident support needs are provided by the Logistics Section. The Logistics Section is managed by the Logistics Section Chief, who may assign a Deputy Section Chief. A Deputy Section Chief is most often assigned when all designated units (listed below) within the Logistics Unit are activated.

Units which may be established within the Logistics Section are:

1. Supply Unit
2. Facilities Unit
3. Ground Support Unit
4. Communication Technology Unit
5. Provisions Unit
6. Medical Unit

### 1. Responsibilities of Logistics Section Chief

The Logistics Section Chief will determine the need to activate or deactivate a unit. If a unit is not activated, responsibility for that unit's duties will remain with the Logistics Section Chief. The Logistics Section Chief's duties and responsibilities include:

1. Manage all incident logistics;
2. Provide logistical input to the Incident Commander in preparing the Incident Action Plan;
3. Brief Branch Directors and Unit Leaders as needed;
4. Identify anticipated and known incident service and support requirements;
5. Request additional resources as needed;
6. Review and provide input to the Communications Plan, Medical Plan, and Traffic Plan;
7. Supervise requests for additional resources; and

8. Oversee demobilization of Logistics Unit.

## 2. Responsibilities of Supply Unit

The Supply Unit's duties and responsibilities include:

1. Provide input to Logistics Section planning activity;
2. Provide supplies to Planning, Logistics, and Finance/Administration Sections;
3. Determine the type and amount of supplies en route;
4. Order, receive, distribute, and store supplies and equipment;
5. Respond to requests for personnel, equipment, and supplies;
6. Maintain an inventory of supplies and equipment;
7. Service reusable equipment, as needed; and
8. Ordering all off-site incident resources, including tactical and support resources, personnel and all expendable and non-equipment support supplies.

## 3. Responsibilities of Facilities Unit

The Facility Unit's duties and responsibilities include:

1. Set up, maintenance and demobilization of all incident support facilities except Staging Areas;
2. Participate in Logistics Section/Support Branch planning activities;
3. Determine requirements for each incident facility;
4. Prepare layouts of facilities and inform appropriate unit leaders;
5. Activate incident facilities;
6. Obtain and supervise personnel to operate facilities, including Base, Camp and Security Managers;
7. Provide security services;
8. Provide facility maintenance services, e.g., sanitation, lighting, etc.; and
9. Demobilize base, camp facilities.

The following Managers report directly to the Facilities Unit Leader:

1. Security Manager
2. Base Manager
3. Camp Manager

1. Security Manager

The Security Manager's duties and responsibilities include:

1. Establish contacts with local law enforcement agencies as required;

2. Contact the Resource Use Specialist (if assigned) or Agency Representatives to discuss any special custodial requirements which may effect operations;
3. Request necessary personnel to accomplish work assignments;
4. Ensure that support personnel are qualified to manage security problems;
5. Develop a security plan for incident facilities;
6. Adjust the security plan for personnel and equipment changes and release.
7. Coordinate security activities with appropriate incident personnel;
8. Keep the peace, prevent assaults, and settle disputes through coordination with Agency Representatives;
9. Prevent theft of all property;
10. Investigate and document all complaints and suspicious occurrences;
11. Demobilize in accordance with the Incident Demobilization Plan; and
12. Provide safeguards necessary for protection of personnel and property from loss or damage.

## 2. Base Manager

The Base Manager's duties and responsibilities include:

1. Determine requirements for establishing an Incident Base;
2. Understand and comply with establishing restrictions;
3. Determine personnel support requirements;
4. Ensure that appropriate sanitation, security and facility management services are in place at the Base;
5. Obtain necessary equipment and supplies;
6. Ensure that all facilities and equipment necessary for base support operations are set up and functioning;
7. Make sleeping area assignments;
8. Ensure strict compliance with applicable safety regulations;
9. Ensure that all facility maintenance services are provided;
10. Ensure that adequate security and access control measures are being applied; and
11. Demobilize Base when directed.

## 3. Camp Manager

On large incidents, one or more camps may be established. Camps may be in place several days or they may be moved to various locations.

The Camp Manager's duties and responsibilities include:

1. Determine or establish number of personnel assigned to camp;



2. Determine any special requirements or restrictions on facilities or operations.
3. Obtain necessary equipment and supplies;
4. Ensure that all sanitation, shower, and sleeping facilities are set up and properly functioning;
5. Make sleeping arrangements and assignments;
6. Provide direct supervision for all facility maintenance and security services;
7. Ensure strict compliance with safety regulations;
8. Ensure that all camp-to-base communications are centrally coordinated;
9. Ensure that all camp-to-base transportation scheduling is centrally coordinated;
10. Provide overall coordination of camp activities to ensure that all assigned units operate effectively and cooperatively in meeting incident objectives; and
11. Demobilize the camp in accordance with the Incident Action Plan.

#### 4. Ground Support Unit

The Ground Support Unit's duties and responsibilities include:

1. Participate in Support Branch/Logistics Section planning activities;
2. Provide support services (fueling, maintenance, and repair) for all mobile equipment and vehicles, with the exception of aviation resources;
3. Order maintenance and repair supplies (e.g., fuel, and spare parts);
4. Provide support for out-of-service equipment;
5. Develop the Incident Traffic Plan;
6. Maintain an inventory of support and transportation vehicles;
7. Record time use for all incident-assigned ground equipment (including contract equipment);
8. Update the Resources Unit with the status (location and capability) of transportation vehicles;
9. Provide ground transportation of personnel, supplies and equipment; and
10. Maintain incident roadways as necessary.

##### 1. Equipment Manager

The Equipment Manager reports to the Ground Support Unit Leader and is responsible for the following:

1. Service, repair, and fuel for all equipment;
2. Transportation and support vehicle services; and
3. Maintenance of equipment use and service records.

## 5. Communication Technology Unit

The Communication Technology Unit's duties and responsibilities include:

10. Advise on communications capabilities/limitations.
11. Prepare and implement the Incident Radio Communications Plan (ICS Form 205)
12. Establish and supervise the Technology, Incident Communications Center and Message Center.
13. Establish telephone, computer links, and public address systems.
14. Establish communications equipment distribution and maintenance locations.
15. Install and test all communications equipment.
16. Oversee distribution, maintenance and recovery of communications equipment, e.g., portable radios and FAX machines.
17. Develop and activate an equipment accountability system.
18. Provide technical advice on:
  1. Adequacy of communications systems
  2. Geographical limitations
  3. Equipment capabilities
  4. Amount and types of equipment available
10. Develop plans for the use of incident communications equipment and facilities.

## 6. Provisions Unit

The Provisions Unit's duties and responsibilities include:

9. Determine food and water requirements;
10. Determine method of feeding to best fit each facility or situation;
11. Obtain necessary equipment and supplies and establish cooking facilities;
12. Ensure that well-balanced menus are provided;
13. Order sufficient food and potable water from the Supply Unit;
14. Maintain an inventory of food and water;
15. Maintain food service areas, ensuring that all appropriate health and safety measures are being followed;
16. Supervise caterers, cooks, and other Provisions Unit personnel as appropriate; and
17. Provide food for the entire incident, including all remote locations (e.g., Camps, Staging Areas), and for personnel unable to leave tactical field assignments.

## 7. Medical Unit

The Medical Unit's responsibilities and duties include:

0. Develop an Incident Medical Plan (to be included in the Incident Action Plan).
1. Determine level of emergency medical activities prior to activation of Medical Unit.
2. Provide medical aid.
3. Acquire and manage medical support personnel.
4. Prepare the Medical Emergency Plan (ICS Form 206).

5. Develop procedures for managing major medical emergencies.
6. Respond to requests for:
  1. Medical Aid
  2. Medical Transportation
  3. Medical Supplies
7. Assist the Finance/Administration Section with processing paper work related to injuries or deaths of incident personnel.

Note that the provision of medical assistance to the public or victims of the emergency is an operational function, and would be done by the Operations Section and not by Logistics Section Medical Unit.

#### Sec. 2.24 Finance/Administration Section

The Finance/Administration Section is responsible for managing all financial aspects of an incident. Not all incidents will require a Finance/Administration Section. Only when the involved agencies have a specific need for Finance/Administration services will the Section be activated. There are four units, which may be established within the Finance/Administration Section.

1. Time Unit
2. Procurement Unit
3. Compensation/Claims Unit
4. Cost Unit

#### 1. Responsibilities of Finance/Administration Section Chief

The Finance/Administration Section Chief's duties and responsibilities include:

1. Manage all financial aspects of an incident.
2. Provide financial and cost analysis information as requested.
3. Gather pertinent information from briefings with responsible agencies.
4. Develop an operating plan for the Finance/Administration Section.
5. Fill supply and support needs.
6. Determine need to set up and operate an incident commissary.
7. Meet with Assisting and Cooperating Agency Representatives as needed.
8. Maintain daily contact with agency(s) administrative headquarters on Finance/Administration matters.
9. Ensure that all personnel time records are accurately completed and transmitted to home agencies according to policy.
10. Provide financial input to demobilization planning.
11. Ensure that all obligation documents initiated at the incident are properly prepared and completed.
12. Brief agency administrative personnel on all incident-related financial issues needing attention or follow-up.

## 2. Time Unit

The Time Unit's duties and responsibilities include:

1. Determine incident requirements for time recording function.
2. Contact appropriate agency personnel/representatives.
3. Ensure that daily personnel time recording documents are prepared and in compliance with agency(s) policy.
4. Maintain separate logs for overtime hours.
5. Establish and manage commissary operation on larger or long-term incidents.
6. Submit cost estimate data forms to Cost Unit as required.
7. Maintain record security.
8. Ensure that all records are current and complete prior to demobilization.
9. Release time reports from assisting agency personnel to the respective Agency Representatives prior to demobilization.
10. Collect and process time records for each operational period.

Two positions may report to the Time Unit Leader:

1. Personnel Time Recorder - Oversees the recording of time for all personnel assigned to an incident. Also records all personnel-related items, e.g., transfers, promotion, etc.
2. Commissary Manager - Establishes, maintains, and demobilizes commissary. Also responsible for commissary security.

## 3. Procurement Unit

All financial matters pertaining to vendor contracts, leases, and fiscal agreements are managed by the Procurement Unit. This Unit works closely with local fiscal authorities to ensure efficiency.

The Procurement Unit's duties and responsibilities include:

1. Review incident needs and any special procedures with Unit Leaders.
2. Coordinate with local jurisdiction on plans and supply sources.
3. Obtain Incident Procurement Plan.
4. Prepare and authorize contracts and land-use agreements.
5. Draft memoranda of understanding.
6. Establish contracts and agreements with supply vendors.
7. Provide for coordination between the Ordering Manager, agency dispatch, and all other procurement organizations supporting the incident.
8. Ensure that a system is in place, which meets agency property management requirements. Ensure proper accounting for all new property.

9. Interpret contracts and agreements, and resolve disputes.
10. Coordinate with Compensation/Claims Unit for processing claims.
11. Coordinate use of imprest funds (funds loaned or advanced for the operation of the incident) as required .
12. Complete final processing of contracts and send documents for payment.
13. Coordinate cost data in contracts with Cost Unit Leader.
14. Maintain equipment time records.
15. Manage all equipment rental agreements.
16. Process all rental and supply fiscal document billing invoices.

Equipment Time Recorder - Oversees the recording of time for all equipment assigned to an incident. Also posts all charges or credits for fuel, parts, service, etc., used by equipment.

#### 4. Compensation/Claims Unit

In the ICS, Compensation-for-Injury and Claims are contained within one Unit. Separate personnel may perform each function, however, given their differing activities. These functions are becoming increasingly important on many kinds of incidents.

Compensation-for-Injury oversees the completion of all forms required by workers' compensation and local agencies. A file on injuries and illnesses associated with the incident will be maintained, and all witness statements will be obtained in writing. Close coordination with the Medical Unit is essential.

The Compensation/Claims Unit's duties and responsibilities include:

1. Establish contact with incident Safety Officer and Liaison Officer (or Agency Representative if no Liaison Officer is assigned).
2. Determine the need for Compensation-for-Injury and Claims Specialist and order personnel as needed.
3. Establish a Compensation-for-Injury work area within or as close as possible to the Medical Unit.
4. Review Incident Medical Plan.
5. Review procedures for handling claims with Procurement Unit.
6. Periodically review logs and forms produced by Compensation/Claims Specialists to ensure compliance with agency requirements and policies.
7. Ensure that all Compensation-for-Injury and Claims logs and forms are complete and routed to the appropriate agency for post-incident processing prior to demobilization.
8. Investigate all claims involving property associated with or involved in the incident.

Two specialists report to the Compensation/Claims Unit Leader:

1. Compensation-for-Injury Specialist - Administers financial matters arising from serious injuries and deaths on an incident. Work is done in close cooperation with the Medical Unit.
2. Claims Specialist - Manages all claims-related activities (other than injury) for an incident.

#### 5. Cost Unit

The Cost Unit's duties and responsibilities include:

1. Coordinate with agency headquarters on cost reporting procedures.
2. Collect and record all cost data.
3. Develop incident cost summaries.
4. Prepare resources-use cost estimates for the Planning Section.
5. Make cost-saving recommendations to the Finance/Administration Section Chief.
6. Provide all incident cost analysis.
7. Ensure the proper identification of all equipment and personnel requiring payment.
8. Records all cost data, analyzes and prepares estimates of incident costs, and maintains accurate records of incident costs.

### Sec. 3.0 Mission Statement

The primary mission of the Department in any Critical Incident situation is the protection and preservation of life. Tactical operations that are conducted in these instances shall be managed by the Operations Chief who shall be guided by the premise that preservation of life extends to all persons, and includes sworn personnel, suspects, perpetrators, hostages and uninvolved bystanders. The Department recognizes that Critical Incidents may also create multi-jurisdictional or multi-functional responsibilities and, should the situation require, it is fully prepared to establish a Unified Command to ensure the efficient use of resources and expertise to bring about a successful resolution of the incident or the efficient transfer of command should jurisdictional or functional needs change.

The Department recognizes that in such situations personnel are subjected to extraordinary demands and stresses and shall provide, under the direction of the Stress Support Unit, evaluation, education and stress mediation through a Critical Incident Debriefing process.

### Sec. 4.0 Critical Incident Definitions

Sec. 4.1 Barricaded Suspect: Any person who has the demonstrated capability and/or the stated intention to cause death or great bodily harm to himself and/or another person and has

achieved tactical superiority by the use of physical obstruction including but not limited to buildings, open fields, vehicles or any other natural or man-made barrier.

Sec. 4.2 Critical Incident: Any man-made or natural disaster, major violent incident, or incident involving an act of violence or potential act of violence in which public safety personnel and/or civilians are subject to extreme danger.

Sec. 4.3 Code 99: The Department's code which identifies a situation as being a Special Threat Situation and sets the appropriate notification/response system in action.

Sec. 4.4 Code 100: The Department's code which identifies a situation as being a Crowd Control Problem and sets the appropriate notification/response system in action.

Sec. 4.5 Code 101: The Department's code which identifies a situation as one involving Fire, Explosion or Structural Collapse incidents and sets the appropriate notification/response system in action.

Sec. 4.6 Code 102: The Department's code which identifies a situation as being one involving a Mass Casualty incident and sets the appropriate notification/response system in action.

Sec. 4.7 Code 103: The Department's code which identifies a situation as being a Natural Disaster (e.g. hurricane, major storm, etc.) incident and sets the appropriate notification/response system in action.

Sec. 4.8 Code 104: The Department's code which identifies a situation as being one involving Hazardous Materials (HazMat) or Weapons of Mass Destruction (WMD) incidents and sets the appropriate notification/response system in action.

Sec. 4.9 Code 105: The Department's code which identifies a situation as being one involving Active Shooter Rapid Deployment Protocol incidents and sets the appropriate notification/response system in action.

Sec. 4.10 Critical Incident Negotiation Team: A group of sworn officers who have been specially trained in negotiation techniques.

Sec. 4.11 Critical Incident Negotiation Team Coordinator: A Superior Officer who is an active member of the Critical Incident Negotiation Team, as well as being responsible for their selection, training, operational use and administrative affairs.

Sec. 4.12 Crowd Control Problem: Any situation involving a large crowd of people where the use of planned tactics is necessary to maintain public safety.

Sec. 4.13 Entry and Apprehension Team: Officers, under the direction of a supervisor, specifically trained and equipped in containment, assault and firearm tactics, for the purpose of

apprehending persons who are probably armed and/or barricaded and/or the rescue of hostages or victims.

Sec. 4.14 Firearms Control: Absolute adherence to the principle that there shall be no discharge of firearms unless authorized by the Incident Commander, except in self defense or the preservation of life.

Sec. 4.15 Hostage Situation: Any incident where a suspect(s) is holding a hostage(s) and where the suspect(s) threatens the life of, or great bodily injury to, the hostage(s), with the unlawful intent of evading arrest, escaping, obtaining the release of persons in custody, obtaining money and/or property or attaining any other objective.

Sec. 4.16 Incident Base: Location at the incident where the primary logistics functions are coordinated and administered. The Incident Command Post may be collocated with the Base.

Sec. 4.17 Incident Commander (IC): The Incident Commander (IC) shall be the person with responsibility for the overall management of the incident. Except in multi-jurisdictional or multi-functional Unified Commands, the command function is the responsibility of a single person, who remains in command until formally relieved, or until transfer of command is accomplished. The IC shall be the highest ranking officer present, subject to the provisions of Rule 101, concerning Command and Control. Whenever a District Commander is relieved of the position of Incident Commander by a person of higher rank, the District Commander shall then be the Deputy Incident Commander.

Sec. 4.18 Incident Command Post (ICP): The location at which the primary command functions are executed. The ICP may be collocated with the Incident Base.

Sec. 4.19 Incident Command System (ICS): A system of incident management with the flexibility to expand and contract to meet the needs of any situation. It is a nationally recognized system that was originally mandated for use in Hazardous Materials Incidents. ICS is a model for all multi-jurisdictional events and provides for the proper application of five major management activities - Command, Operations, Planning, Logistics and Finance. It also provides a workable framework for Mobilizations and De-Mobilizations, and in cases of multi-jurisdictional or multi-functional responsibilities, allows for the formation of a Unified Command.

Sec. 4.20 Information Officer: A sworn officer from the Office of Media Relations shall be designated by the IC as the Information Officer, who shall ensure the security of the Press Area and coordinate with the Incident Commander as to what information can be released without jeopardizing the safety of the hostages, the police or the tactical plan.

Sec. 4.21 Liaison Officer: A Superior Officer so designated by the IC who shall act as the command officer of the command post. The Liaison Officer shall serve as the link to outside resources and agencies and coordinate the arrival and placement of resources, both personnel and material with the Staging Area Manager.



Sec. 4.22 Operations Chief (OC): The person in charge of the Operations Section who is responsible for the management of all tactical operations at the incident. Unless otherwise designated by the IC, the Operations Chief shall be the highest ranking officer present from the Special Operations Division.

Sec. 4.23 Operations Section: The Section responsible for all tactical operations at the incident. The Section includes any Branches, Divisions and/or Groups, Task Forces, Strike Teams, Single Resources and Staging Areas necessary to support tactical operations.

Sec. 4.24 Perimeter:

Sec. 4.24.1 Inner Perimeter: Area of containment closest to the situation.

Sec. 4.24.2 Outer Perimeter: Area of containment located immediately outside of the inner perimeter.

Sec. 4.24.3 Traffic Perimeter: Area of containment farthest from the situation, that prevents unauthorized persons from interfering with the situation.

Sec. 4.25 Recording Officer: Until otherwise designated by the IC, the Recording Officer shall be an officer assigned to the original response unit. The Recording Officer shall keep an incident log of all the pertinent facts and details surrounding the incident in chronological order.

Sec. 4.26 Sniper: Any person who causes, attempts to cause or threatens to cause death or bodily injury to other persons by discharging or threatening to discharge a firearm or other lethal weapon from an initially concealed position.

Sec. 4.27 Special Threat Situation: Any situation involving a barricaded suspect, a hostage situation, a threatened suicide or the execution of a search/arrest warrant.

Sec. 4.28 Staging Area: Location(s) at an incident which provide for efficient resource management by providing a specific location(s) beyond the outer perimeter for responding personnel, equipment and units to be placed while awaiting an operational assignment. Unless the Logistics Section has been activated, Staging Areas are managed by the Operations Section under the direction of a Staging Area Manager.

Sec. 4.29 Staging Area Manager: Unless the Logistics Section has been activated, the Staging Area Manager reports to the Operations Section Chief and is the person responsible for checking-in and managing the resources being held in reserve at the Staging Area while they are awaiting an operational assignment. The Staging Area Manager shall be responsible for ensuring that an accurate record is kept of all responding units and/or personnel and that a report of such is provided to the Recording Officer at the conclusion of the incident.

Sec. 4.30 Terrorism: The calculated use of violence or threats of violence by a person(s) or a group(s) to instill fear for the purpose of coercing or intimidating governments or society in the pursuit of goals that are generally political, religious or ideological.

Sec. 4.31 Unified Command: A unified team effort which allows all agencies with responsibility for an incident, either geographical or functional, to manage the incident by establishing a common set of incident objectives and strategies. This is accomplished without losing or abdicating agency authority, responsibility or accountability.

## Sec. 5.0 Critical Incident Types

Response procedures using the Incident Command System shall be utilized for all Critical Incidents, including, but not limited to:

1. Special Threat Situations - Code 99 ([see Addendum A](#));
  1. Barricaded suspect;
  2. Hostage situation;
  3. Threatened Suicide; and
  4. Execution of Search/Arrest Warrants;
2. Crowd Control Incidents - Code 100 ([see Addendum B](#));
3. Fire, Explosion and Structural Collapse Incidents - Code 101 ([see Addendum C](#));
4. Mass Casualty Incidents - Code 102 ([see Addendum D](#));
5. Natural Disasters, e.g., blizzard, hurricane, major snow or ice storm, etc. - Code 103 ([see Addendum E](#));
6. Hazardous Materials (HazMat) and Weapons of Mass Destruction (WMD) Incidents - Code 104 ([see Addendum F](#));
7. Active Shooter Rapid Deployment Protocol Incidents - Code 105 ([see Addendum G](#)).

## Sec. 6.0 Duties and Responsibilities of Responding Officers

The following duties and responsibilities apply in all situations in which the Boston Police Department is the agency with primary responsibility for resolving a particular type of critical incident. The duties and responsibilities of Boston Police Officers at critical incidents that are the primary responsibility of other agencies (EMS, Fire, etc.) shall be to provide support to those agencies by performing duties such as, directing traffic, controlling access (perimeter control) and conducting evacuations and warnings.

### Sec. 6.1 First Responding Officers:

The first officer(s) to arrive at the scene, regardless of rank, shall assume the duties of Incident Commander (IC) until relieved and shall:

1. Determine the type of Critical Incident;
2. Identify and locate any injured persons, rendering first aid as necessary, and evacuate both the injured and any bystanders, if it is safe to do so;
3. Notify the dispatcher and relay the following information:
  1. Appropriate Critical Incident code;
  2. Exact location of the incident;
  3. Location to which responding units should be sent; and
  4. Areas or streets that may be unsafe for units to enter;
4. Request a Patrol Supervisor;
5. Detain witnesses to establish the following:
  1. Crime(s) committed, if any;
  2. Number of suspect(s) and weapon(s), if any;
  3. Number and location of hostage(s), if any; and
  4. Identity of all parties involved;
6. Maintain radio communication with the Dispatch Center keeping the dispatcher informed of progress of the situation; and
7. Keep the radio channel as clear as possible by maintaining appropriate radio discipline.

The response unit originally assigned to the call by the dispatcher is responsible for completing the incident report. Unless otherwise designated by the IC, this unit will be assigned as the Recording Officer for the incident and shall maintain an incident log of all the pertinent facts and details surrounding the incident in chronological order.

#### Sec. 6.2 Patrol Supervisor:

The Patrol Supervisor assigned by the dispatcher shall:

1. If the Patrol Supervisor is the highest ranking officer present, subject to the provisions of Rule 101, concerning Command and Control, announce arrival and assumption of command to all officers on-scene by radio and assume the duties of Incident Commander (IC);
2. Ensure that the Recording Officer maintains an incident log of all responding units, assignments, events, radio traffic and any other pertinent facts and details surrounding the incident in chronological order;
3. Debrief the first responding officer(s);

4. Evaluate the situation, verify the type of Critical Incident and notify Operations to make the appropriate notifications;
5. In coordination with the dispatcher, shift to an alternate communications channel or request a clear channel. Ensure that all officers on scene and in the Staging Area(s) make the shift to the appropriate radio channel;
6. Establish an inner perimeter. (The inner perimeter is to be staffed only by authorized uniformed personnel, excepting Negotiators. Where necessary, personnel shall be deployed or re-deployed based on the degree of danger to officers, bystanders and hostages.);
7. Establish an outer and traffic perimeter and deploy perimeter control personnel. Allow only authorized persons inside the outer perimeter;
8. Ensure injured and bystanders are evacuated, if safe to do so;
9. Establish a forward command post (FCP) and request the mobile command post (MCP) respond to a designated Staging Area;
10. Establish a Staging Area beyond the outer perimeter and ensure that all responding units report to that location. Assign an officer to act as the Staging Area Manager at the Staging Area;
11. Assign personnel to obtain required police information and continue communications, if established;
12. Request additional resources, as necessary; and
13. Ensure containment and isolation of crime scene and perimeter areas.

#### Sec. 6.3 District Commander:

The District Commander shall:

1. Announce arrival and assumption of command to all officers on-scene by radio; evaluate the situation and debrief the Patrol Supervisor;
2. Assume command as the IC unless relieved;
3. Maintain control of the inner perimeter; and
4. Ensure establishment of an Incident Command Post and press assembly area and assignment of a sworn officer as the Information Officer. When available, the person designated as the Information Officer shall be relieved by the Director of the Office of Media Relations, who shall then be designated as the Information Officer.

#### Sec. 6.4 Incident Commander:

The IC shall have absolute command and control over the Critical Incident. The IC has full responsibility and authority over all personnel, equipment and their utilization for the duration of the incident. Additionally, the IC shall:

1. Announce arrival and assumption of command to all officers on scene by radio.
2. Ensure establishment of Command Post and its communications links and assign an officer as Liaison Officer.
3. Maintain liaison with concerned agencies and other affected jurisdictions and establish a Unified Command system if necessary;
4. Debrief the previous Incident Commander involved in the incident to obtain a clear understanding of the situation and evaluate the resources on scene.
5. Appoint and/or designate individuals to fill ICS Command Staff positions as deemed necessary;
6. Call on any other Department or outside resources needed to support and/or resolve the situation.
7. Ensure that only uniformed officers, with the exception of Hostage Negotiators, are at or within the inner perimeter.
8. Obtain maps of the area and a floor plan of the location.
9. In the absence of a Planning Section having been designated, assign officers, preferably Detectives, to obtain background information and gather intelligence.
10. Ensure the availability of persons with necessary technical skills or persons with pertinent knowledge regarding the incident.
11. Ensure contact with Stress Support Unit personnel and assignment of trained peer counselors for the Critical Incident Stress debriefing process, if deemed necessary;
12. After the incident has been resolved, conduct a Technical Debriefing; and
13. In conjunction with a Formal Debriefing, prepare the After Action Report for the Chief, Bureau of Field Services. The Formal Debriefing and After Action Report shall critique the entire operation, including the management of the incident and the units, personnel and equipment involved.

#### Sec. 6.5 Dispatcher - Communications Division:

Upon being notified that a Critical Incident actually exists, the dispatcher shall immediately direct a Patrol Supervisor to respond, if one is not already on the scene.

Additionally, the dispatcher shall:

1. Advise the Operations Duty Supervisor of the situation;

2. Assign a separate radio frequency or clear the channel of the incident and advise all units to maintain radio discipline;
3. Dispatch sufficient units to contain and isolate the area as directed by the IC. Units so deployed will be sent to the Staging Area to check in with the Staging Area Manager and stand by for assignment(s);
4. Determine and advise responding units of streets that may be unsafe to enter;
5. Notify the responding Patrol Supervisor of actions taken and request that the Patrol Supervisor notify Operations of the status of existing conditions and requests for specific needs;
6. Dispatch ambulance and fire apparatus to the Staging Area; and
7. Advise all units not assigned to the incident to remain out of the area.

#### Sec. 6.6 Duty Supervisor: Communications Division

The Duty Supervisor, Communications Division when notified by a dispatcher that a Critical Incident could exist shall:

1. Notify through the most efficient means available, the Commissioner's Office, the Office of the Superintendent-in-Chief, the Chief, Bureau of Field Services, Commander, Special Operations Division, the District Commander and, if applicable, the Area Deputy Superintendent, the on-call Deputy Superintendent and, if applicable, the Night Superintendent.
2. Designate a Communications Division Clerk(s) to begin a log of all radio and telephone communications requests and notifications made relative to the incident.
3. Notify the Telecommunications Management Unit for the Mobile Command Post, and Lighting Unit to respond, as directed by the IC.
4. Establish and maintain telephone contact with the Mobile Command Post as soon as it is on scene.
5. Ensure that all actions required of the Dispatcher have been performed and that appropriate radio discipline is being maintained.
6. Monitor the incident and ensure that all officers involved are advised of changes in command and other important information.
7. Request assistance of support agencies, e.g., Public Utilities, as necessary when requested by IC.

8. Notify the Stress Support Unit's on-call officer that a Critical Incident is in progress and direct them to respond to the Staging Area.

## Sec. 7.0 Support Personnel and Services

Sec. 7.1 Radio Shop/Signal Services: Upon being notified of a Critical Incident, the Radio Shop shall deploy to the scene with the Mobile Command Post, fully equipped for response for Critical Incidents.

Sec. 7.2 Liaison Officer: A Superior Officer shall be designated the Liaison Officer by the IC. The Liaison Officer shall act as the command officer of the command post and shall also be the link to outside resources and agencies and coordinate the arrival and placement of resources, both personnel and material with the Staging Area Manager.

Sec. 7.3 Information Officer: A sworn officer from the Office of Media Relations shall be designated by the IC as the Information Officer. The Information Officer shall ensure the security of the Press Area and coordinate with the Incident Commander as to what information can be released without jeopardizing the safety of the hostages, the police or the tactical plan.

Sec. 7.4 Logistics Section Chief: In the event of a prolonged operation the Incident Commander shall designate a person to assume the responsibilities of Logistics Section Chief, who shall be responsible for the following, when so ordered by the IC:

1. Establish central transportation and supply post at or near the Staging Area;
2. Maintain and issue supplies required for operation;
3. Arrange for feeding and bedding of officers if necessary;
4. Maintain complete record of supplies and equipment issued;
5. Account for expenditures, lost or damaged property and contractual agreements; and
6. Inspection and maintenance of equipment and rehabilitation of personnel.

## Sec. 8.0 Post Incident Procedures

Sec. 8.1 Technical Debriefings: Upon termination of a Critical Incident the IC shall conduct a Technical Debriefing of all personnel involved in the incident and ensure Stress Support Unit personnel make arrangements for Critical Incident Stress Debriefings.

Conducted by the Incident Commander with all personnel directly involved, including Communications Division personnel, the purpose of the Technical Debriefing is to critique the Department's response, both in terms of personnel and resources, while events are fresh in the minds of the participants, for the purpose of learning, evaluating and making recommendations, as well as to aid in preparation of the After Action Report.

Sec. 8.2 Critical Incident Stress Debriefings: Upon termination of a Critical Incident, if deemed necessary by the Director, Stress Support Unit, or designee, incident debriefings of personnel

intensely involved in and/or affected by the incident, for the purpose of post-incident stress evaluation, education and mediation shall be conducted. These debriefings will be conducted by members of the Boston Police Critical Incident Support Team (BPCIST).

The Boston Police Critical Incident Support Team (BPCIST) Coordinator and/or other team members will be dispatched to the appropriate location to conduct a post-incident defusing for the officers involved in a Critical Incident. The on-scene BPCIST members will further assess the situation to determine the need for a formal debriefing and communicate their findings to the BPCIST Coordinator who shall further advise the Director, Stress Support Unit.

Upon being advised by the BPCIST Coordinator, a formal debriefing may or may not be required at the discretion of the Director, BPD Stress Support Unit or their designee.

Whenever a formal Critical Incident Stress Debriefing is deemed necessary, attendance by all officers directly involved shall be mandatory. It is the responsibility of the BPCIST Coordinator, or their designee from the Team, to notify the District or Unit Commander of the time and place the formal CISD will be held. District or Unit Commanders shall ensure that the officers involved in the incident attend.

#### Sec. 8.3 After Action Report/Formal Debriefing

The Incident Commander shall submit to the Chief, Bureau of Field Services, in addition to any other reports required, an After Action Report which shall include an analysis of the personnel, equipment, operation and management of the incident, as well as any recommendations for improvement.

Upon submission of all reports, the Chief, Bureau of Field Services shall hold a Formal Debriefing with the IC, Commander of the Special Operations Division, all involved Unit Commanders and any others he so designates, for the purpose of learning, evaluating and making recommendations.

---

### Addendum A - Code 99 Special Threat Situations

#### 1. Barricaded Subjects/Hostage Situations/Threatened Suicides

##### General Considerations

Special Threat Situations are among the most delicate and sensitive encounters the Department is called upon to handle. Lives are at stake and the actions of the Department will determine the outcome. The success of any Special Threat Situation plan hinges on unity of command, teamwork, communication, coordination of personnel and tactical decision making.



The procedures described herein are designed to address those actual situations which have reached such a serious magnitude that a major Department response is necessary. It does not address those incidents which can and/or must be resolved immediately.

The very nature of barricaded suspect or hostage situations indicates that this is an extremely sensitive area. The following guidelines are intentionally broad in scope, because no two situations are exactly alike. Whether it be the number of hostages and/or suspects, the mental condition of the suspect(s), the geographical location, or any other variable, each situation must be evaluated and acted upon in its own set of circumstances.

### Sec. 1 Negotiation/Use of Force Policy

Once it has been determined that a Special Threat Situation exists, the Communications Division shall be notified that a Code 99 situation exists. It is the policy of this Department that except for situations where exigent circumstances require an immediate forceful response, non-force alternatives will be utilized before resorting to forceful measures. The goal to be pursued in responding to these situations is the successful termination of the operation without injury and/or loss of life. Additionally, it is the policy of this Department that the Boston Police SWAT Team shall be utilized in all Special Threat Situations and that the Critical Incident Negotiation Team shall be utilized in all Special Threat Situations involving Barricaded Subjects, Hostages and/or threatened suicides.

### Sec. 2 Goal of Negotiations

In these situations the primary goal of the Department is to save and preserve the lives of police officer(s), the hostage(s), citizen(s), and hostage taker(s), barricaded suspect(s) and/or threatened suicides.

In order to achieve this goal the Department will pursue the following objective:

1. Establish and maintain complete organizational control on scene.
2. Obtain tactical advantage over the suspect(s).
3. Negotiate safe release of the hostage(s) and apprehension of the suspect(s).
4. Explore every source of intelligence information.

### Sec. 3 Purpose of Negotiations

The primary purpose of negotiation is to slow down the initiative of the suspect(s) and create an atmosphere of trust. Most suspects are in a state of conflict and anxiety: and are emotionally unstable, hypersensitive to their environment, and unable to cope or focus their thoughts. The first objective of the negotiator is to reduce the suspects anxiety and return the suspect(s) to a decision-making state. Communication and stalling for time are the primary tactics used. Time allows the police to prepare alternatives, plan for different eventualities and provides an opportunity for the suspect(s) to make a mistake. Practically all demands are

negotiable, except, demands for weapons and explosive materials, or the exchange of hostages.

#### Sec. 4 Stockholm Syndrome:

During any hostage situation, negotiators and other police personnel should be aware of the Stockholm Syndrome. It consists of one or more of the following behaviors:

1. The hostages begin to have positive feelings toward their captors;
2. The hostages begin to have negative feelings toward the authorities; or
3. The hostage takers begin to develop positive feelings towards their hostages.

Being aware of this syndrome is essential when considering the validity of information from hostages or attempting a rescue assault.

#### Sec. 5 Use of Outside or Third Party Interveners

Third party Interveners, i.e. family, friends, clergy, psychiatrists, etc.: use of such parties must be carefully considered and shall not be allowed unless:

1. The Critical Incident Negotiation Team Coordinator or his designee has interviewed and approved the person, and
2. The IC has approved his/her utilization upon the recommendation of the Critical Incident Negotiation Team Coordinator.

Past experience has demonstrated that family members in particular can cause negative responses and aggravate the situation.

Therefore, before allowing their use as third party Interveners, the Critical Incident Negotiation Team Coordinator will:

1. Determine their identity, background and character.
2. Determine the constructive potential and likely impact of the intervener(s) on the suspect.
3. Establish clear guidelines for intervener's participation.
4. Brief the intervener(s) and agree on what position they will establish with the suspect(s).

#### Sec. 6 Containment and Fire Control

That stabilization of life-threatening situations through containment and fire control creates a tactical environment in which negotiation and problem solving can provide the basis for resolving the incident.

The primary concern of all personnel is the protection of life, whether it be of police officers, hostage(s), suspect(s), or innocent person(s). Therefore, after the initial confrontation is over and the situation is contained, only the Officer-In-Charge can authorize the discharge of weapons. No officer shall discharge a firearm without authorization of the Officer-In-Charge except in an emergency, self-defense or preservation of life.

#### Sec. 7 First Responding Officers:

The first responding officer and/or supervisor must recognize and carefully assess the seriousness and potential threat inherent in a potential barricaded suspect or hostage incident. The first officer(s) to arrive at the scene, usually patrol officers, shall:

1. Respond utilizing controlled - silent response;
2. Determine that a Special Threat Situation exists by determining;
  1. Whether or not a suspect has seized hostages;
  2. If a suspect has contained himself by gaining physical control of the crime scene; and
  3. If this is a threatened suicide requiring the intervention of a trained negotiation team and/or entry and apprehension team.
3. Not return fire or assault the suspect. Officers shall exercise restraint in using firearms. Return fire must be based on the immediate threat to life or great bodily injury by a suspect, the hostage/bystanders must be clear of the line of fire and the armed suspect must be clearly visible and identifiable.
4. Contain the suspect by establishing an inner perimeter and begin isolating the area;
5. Notify the dispatcher and relay the following information;
  1. A Code 99 situation exists;
  2. Exact location of the incident;
  3. Number and location of hostages;
  4. Number and description of suspects and weapons;
  5. Possible avenues of escape;
  6. Location to which responding units should be sent;
  7. Areas or streets that may be unsafe for units to enter.
6. Request the Patrol Supervisor;
7. Evacuate injured and bystanders;
8. Detain witnesses;
9. Develop Required Police Information (RPI) including;

1. Crime committed;
  2. Number of suspects and weapons;
  3. Number and location of hostages;
  4. Injuries;
  5. Identity of all parties involved.
10. Attempt to establish communication with the suspect, but make no attempt to negotiate with the suspect;
  11. Avoid accepting deadlines;
  12. Make no threats; and
  13. Maintain radio communication with the Dispatch Center keeping the dispatcher informed of progress of the situation.

Unless otherwise assigned by the IC, the unit originally assigned to the call by the dispatcher is responsible for completing the incident report, taking charge of prisoners and filing complaints when necessary.

If the originally-assigned unit is re-assigned by the IC or is unable to remain at the scene, the Patrol Supervisor or the IC shall assign a unit to replace the originally assigned unit. The replacement unit shall be responsible for completing the incident report, taking charge of any prisoners and filing complaints when necessary.

#### Sec. 8 Patrol Supervisors:

In addition to the general responsibilities of responding Patrol Supervisors, the Patrol Supervisor assigned by the dispatcher shall:

1. Assume the duties of the IC and announce arrival and assumption of command to all officers on scene by radio;
2. Assign an officer to maintain a log of all responding units, assignments, events and radio traffic;
3. Evaluate the situation and debrief the first responding officers;
4. In conjunction with the dispatcher, shift to an alternate communications channel or request a clear channel. Ensure that all officers on scene are informed and make the shift.
5. Establish an inner perimeter staffed by uniformed personnel only, excepting Hostage Negotiators, until such duties can be assumed by the Boston Police SWAT Team. Deploy

and/or re-deploy personnel based on the degree of danger to officers, bystanders and hostages;

6. Ensure the injured and bystanders are evacuated;
7. Establish an outer and traffic perimeter and deploy perimeter control personnel;
8. Establish a forward command post (FCP) and request the mobile command post (MCP);
9. Establish a staging area beyond the outer perimeter and ensure that all responding personnel and units report to that location for check in. Assign an officer to act as the staging area manager;
10. Assign personnel to develop required police information (RPI), to gather intelligence and to continue communications, if established;
11. If not established yet, establish communication with the suspect, but make no attempt to negotiate;
12. Request that the Boston Police SWAT Team and the Critical Incident Negotiation Team respond;
13. Request that an ambulance and fire apparatus respond to the staging area; and
14. Ensure continued containment and isolation of the area.

#### Sec. 9 District Commanders:

In addition to the general responsibilities of responding District Commanders, the District Commander shall:

1. Assume the duties of the IC and announce arrival and assumption of command to all officers on scene by radio;
2. Evaluate the situation and debrief the previous IC (Patrol Supervisor);
3. Maintain control of inner perimeter until such duties are turned over to the Boston Police SWAT Team;
4. Ensure the establishment of a command post and press assembly area;
5. Assign an officer to be the Liaison Officer to maintain communication with concerned agencies and other affected jurisdictions;
6. Request additional resources and units, as necessary;

7. Ensure that personnel have been assigned to develop required police information (RPI), to gather intelligence and to continue communications, if established;
8. Ensure that an inner perimeter has been established that is staffed by uniformed personnel only, excepting Hostage Negotiators, until responsibility for such duties is taken over by the Boston Police SWAT Team and such other uniformed personnel as may be necessary. Deploy and/or re-deploy personnel based on the degree of danger to officers, bystanders and hostages;
9. Obtain maps of the area and floor plan of the location;
10. Ensure that the Boston Police Critical Incident Support Team has been notified; and
11. At the conclusion of the situation, prepare and submit the After Action Report.

#### Sec. 10 Dispatch Center Dispatcher:

Upon being notified that a Special Threat Situation (Code 99) exists, the dispatcher shall immediately direct a Patrol Supervisor to respond, unless one is already on scene. Additionally, the dispatcher shall:

1. Advise the Dispatch Center Duty Supervisor of the situation;
2. Assign a separate radio frequency or clear the channel for the incident;
3. Dispatch sufficient units to contain and isolate the area. Units so deployed will be sent to the staging area unless directed to specific points by the IC;
4. Advise responding units of streets that may be unsafe to enter or use;
5. Notify the responding Patrol Supervisor of actions taken and request that the PS notify Operations of the status of existing conditions and any requests for specific needs;
6. Dispatch ambulance and fire apparatus to the staging area; and
7. Advise all units not assigned to the incident to remain out of the area.

#### Sec. 11 Dispatch Center Duty Supervisor:

When notified by a dispatcher that a Special Threat Situation exists, the Dispatch Center Duty Supervisor shall:

1. Notify the Commissioner's Office, the Bureau of Field Services, The Bureau of Special Operations, the on-call Deputy Superintendent, the Area and/or District Commander and the Commander of Mobile Operations.

2. Designate a Communications Division Clerk to begin a log of all radio communication requests and notifications made relative to the incident;
3. Notify the Critical Incident Negotiation Team Coordinator and the on-call Critical Incident Negotiation Team;
4. Notify the Commander, Boston Police SWAT Team;
5. Notify the Radio Shop and have the Mobile Command Post and the Lighting Unit respond;
6. Establish and maintain land line contact with the Mobile Command Post as soon as possible;
7. Ensure that all actions required of the dispatcher have been performed;
8. Monitor the progress of the incident and ensure that all officers involved are advised of changes in command and other important information;
9. When requested by the IC, request necessary assistance from other agencies;
10. Notify the Boston Police Critical Incident Support Team that a critical incident is in progress and provide them with the land line number of the Mobile Command Post.

#### Sec. 12 Critical Incident Negotiation Team Coordinator

1. Administrative Responsibilities:
  1. Selection of the Critical Incident Negotiation Team Members.
  2. Planning and scheduling of training programs for newly selected and experienced negotiators.
  3. Maintenance of an on-call system and Team Roster which will be provided to the Commander, Communications Division. The Commander, Communications Division is responsible for posting the list in the Dispatch Center Duty Supervisor notification log.
  4. Evaluation of Critical Incident Negotiation Teams and members. Periodic review of needs and goals in order to maintain proficiency.
  5. Design and development of innovative techniques and equipment for Critical Incident Negotiation Team members.
2. Operational Responsibilities:
  1. Function under the command and control of the Incident Commander, unless an Operations Section Chief has been designated.
  2. Assume responsibility for all Critical Incident Negotiation Team operations.
  3. Use the on-call system and Team Roster to request specific negotiators to respond to the scene.

4. Determine the number of negotiators needed at the scene to efficiently and effectively maintain Critical Incident Negotiation Team (unit) operations.
5. Assign each negotiator at the scene.
6. Act as staff advisor to the IC regarding the status of negotiations, the capabilities and resources of the Critical Incident Negotiation Team and alternative tactics.
7. Evaluate ongoing negotiations and recommend the implementation of various strategies to negotiators.
8. Coordinate Critical Incident Negotiation Team operations with the Entry and Apprehension Team Commander.
9. Evaluate suspects and the suspect's potential for destructive behavior.
10. Secure and determine which persons other than negotiators may speak with the suspect.

#### Sec. 13 Critical Incident Negotiation Team

The Critical Incident Negotiation Team will deploy to the scene upon notification. At the scene, they will be under the command and control of the Critical Incident Negotiation Team Coordinator. Team members will assist the primary negotiator or act as the primary negotiator when so directed. Their duties shall include:

1. Contact the suspect.
2. Keep the suspect in a problem-solving status.
3. Develop alternative tactics and/or options for the peaceful resolution of the suspect(s).
4. Develop intelligence information as to the identity, cause and demands of the suspect(s).
5. Interview all witnesses, police and civilian, who may have relevant information.
6. Assist the Boston Police SWAT Team Commander.
7. Advise and update Critical Incident Negotiation Team Coordinator as to situation status, direction and tactics utilized.

#### Sec. 14 Boston Police SWAT Team:

Responsibilities of the Entry and Apprehension Team are:

1. Respond with adequate personnel when notified by the Communications Division;
2. Be under the command of and act as staff advisor to the IC as to the capabilities and resources of his unit;



3. Supervise and direct all personnel manning the inner perimeter;
4. Limit access to inner perimeter and strictly enforce the policy that only authorized uniformed personnel, except Negotiators, shall be at or forward of the inner perimeter;
5. Have Boston Police SWAT Team personnel in position to ensure the safety of Negotiators and hostages;
6. Ensure the presence of specialized equipment and personnel with the necessary technical skills for the proper use of such equipment are brought to the scene. Deploy special equipment and munitions within established guidelines;
7. Ensure the evacuation of civilians and unauthorized police personnel;
8. Obtain and/or provide maps, floor plans, etc., of locations where hostages are held;
9. Provide scouting reports of location(s) where hostages are held;
10. Deploy sniper/observer teams to cover and observe locations where hostages are held;
11. Ensure the suspect(s) and suspect's location are under constant surveillance;
12. In conjunction with the IC, develop plans that allow decisive action to be taken, if and when conditions provide a tactical advantage;
13. Designate personnel from the Boston Police SWAT Team to take the suspect(s) into custody in the event of a peaceful or negotiated surrender;
14. Designate personnel from the Boston Police SWAT Team to make a forced entry if one is required;
15. Designate personnel from the Boston Police SWAT Team to follow the hostage movement vehicle if one is negotiated and contain the perimeter at the new location;
16. Initiate tactical and operational plans upon being so directed by the IC or a designated Operations Section Chief.

#### Sec. 15 Mobility/Relocation

The movement of a hostage location is an extremely hazardous operation requiring precision, coordination and control. Therefore, due to the inherent dangers involved in a change of location, the relocation of the hostage-takers and hostages(s) should be executed only when all other alternatives have failed and the relocation will:

1. Improve the safety of the hostage(s);
2. Result in the reduction of the number of hostages held.

The movement of the hostage-taker(s) and hostage(s) should include electronic surveillance, vehicle surveillance of front, rear and parallel streets and air cover. The movement shall be controlled. All major roadways, parallel streets and intersecting streets shall be closed to allow the unobstructed passage of the convoy. If possible, the relocation site should be selected in advance and secured by Boston Police SWAT Team personnel.

#### Sec. 15.1 Change in Jurisdictional Responsibility

If the relocation movement involves intra-state, interstate or international boundaries, the state Police, FBI, FAA and IC of the new jurisdiction shall be notified and included in the planning at the earliest possible moment.

In Special Threat Situations where the hostage/victim is a foreign official or an official guest of the United States, or which involves a federal crime, such as bank robbery, jurisdiction is shared concurrently by the FBI and Boston Police Department. If control of the situation was initiated by the Boston Police Department, primary jurisdiction shall be retained by the Boston Police Department until or unless the FBI clearly states that they are assuming command of the situation. In such instances, the FBI is then responsible for bringing the situation to a successful conclusion.

If the Special Agent-in-Charge of the FBI Boston Office, or his designee, states that jurisdiction of the situation will remain concurrent, decisions will be made jointly between the Boston Police Department IC and the senior FBI Special Agent on scene by establishing an ICS Unified Command.

#### Sec. 15.2 Post-relocation Consolidation and Negotiation

Unless exigent circumstances develop which require an immediate forceful response, upon establishment of the suspect(s) and the hostage(s) at a new location, the IC shall re-evaluate the situation and attempt to re-establish negotiations.

#### Sec. 16 Post-Incident Procedures

Post-Incident procedures (after-action reports, debriefings, et al) will be conducted in accordance with standard critical incident post-incident procedures.

---

### Addendum B - Code 100 Crowd Control Situation

Introduction:

In the United States of America, as in the City of Boston, all people have a First Amendment right of free speech and assembly guaranteed by both the federal and state constitutions. The Boston Police Department not only recognizes the right of free speech, but also will actively protect people in the exercise of this right. It is the policy of the Boston Police Department that during marches, demonstrations, protests or rallies, whether they are planned or unplanned and/or possess parade permits or lack such permits, to preserve the peace while protecting the rights of all those assembled and protecting the property of all.

Along with guaranteeing the right to exercise certain freedoms or liberties, the Constitution places duties and obligations on both demonstrators and non-demonstrators – including members of law enforcement. Those who exercise their right to march, demonstrate, protest, rally or exercise any other First Amendment activity are obligated to respect and not abuse the civil and property rights of others. Likewise, police officers are obligated not to let their own personal, political or religious views affect their actions, regardless of the race, gender, sexual orientation, physical disabilities, appearance or affiliation of anyone exercising their lawful First Amendment rights.

Whenever it becomes necessary to control the actions of a crowd that has become an “unlawful assembly,” the Department shall do so with optimal efficiency, minimal impact upon the community and using only such force as is reasonable and necessary.

In crowd control situations where the demonstrators are engaged in unlawful conduct, the Department shall make reasonable efforts to employ “non-arrest” methods of crowd management as the primary means of restoring order. Such methods can be, but are not limited to, establishing contact with the crowd and obtaining voluntary compliance with police directives to minimize enforcement actions. Should such methods prove unsuccessful, arrests shall be made for violations of the law in order to restore and maintain order, protect life and property and protect vital facilities and infrastructures.

#### General Considerations:

Incident Command at the scene of a crowd control problem within the City shall reside with the Boston Police Department. In addition to the general responsibilities described previously, the duties of officers at a crowd control situation are to perform the following tasks within the limits of their training and personal protective equipment. A crowd is quick to sense fear, indecision, poor organization and training on the part of police officers and will take instantaneous advantage of it. The responsibilities placed on officers are important if they are to maintain the public tranquility and well being.

In managing a crowd control situation or civil disturbance, the policy of this Department is to use the least stringent phase of force necessary to accomplish the objective in the safest possible manner for all involved. The application of force is determined by the escalating levels or potential escalating levels of force faced by the officers in a crowd control situation or civil disturbance. Any and all use of force by the Boston Police Department and those law enforcement agencies called upon to assist the Boston Police Department shall be determined by the authorized Command and Control structure put in place for a particular crowd control or civil disturbance event – planned or unplanned.

As outlined above, it may not be feasible to apply each phase of the Use of Force Continuum in the order written. Circumstances may require that one or several of the phases be discarded depending upon the level of opposition encountered. The situation, use of force or violence used by the crowd, amount of damage being done to property that the Incident Commander or Tactical Commander encounters will dictate the phase and use of force by the police.

No two crowd control situations or civil disturbances are the same. This can be due to some of the following: type of event, location, weather, size of the crowd, make up of the crowd, mood of the crowd, time of day or night and any incidents that may have led up to the event or situation. The Incident Commander or Tactical Commander must consider the number of officers present to police the event and the type of equipment available to them at the time. The Incident Commander or Tactical Commander must also consider the amount of time it will take for the equipment or additional officers to arrive to deal with the crowd control problem at hand.

The appropriate level of force will be determined and authorized only by the Incident Commander and/or the on-scene Tactical Commander.

#### **Sec. 1 Types of Crowd Control Situations:**

- A. Organized Marches & Demonstrations (orderly crowd) – defined as a march or demonstration that takes place where the participants do no damage to property or injure any persons and do not materially interfere with the civil or property rights of others. In some cases, the participants will work with the police to move the march or demonstration along to its completion. Such marches or demonstrations may be planned or unplanned and could have a parade permit or lack a parade permit.

As long as the situation does not escalate, the responsibility of the police is limited to monitoring crowd activities. The police presence could be in platoon formation or in

individual officers strategically placed in and around the area, including motorcycle escorts. Normal patrol and use of force policies and responsibilities would apply.

- B. Peaceful Civil Disobedience – defined as a march or demonstration that takes place where some or all of the participants engage in some form of civil disobedience. This type of situation could manifest itself as a peaceful building takeover, a “sit-down” that blocks the entrance to a building or roadway or marching against the traffic on public streets. Demonstrators will sometimes ask to be arrested and/or will try to get arrested, and will assist and/or cooperate in the arrest process. Events such as these will usually not result in property damage and will involve only a limited infringement of the civil and property rights of others.

The initial response of the police at the scene of an unlawful, but non-violent march or demonstration will be to monitor the crowd’s activities and to provide a uniformed police presence while evaluating the situation. The Incident Commander or Tactical Commander on scene will determine whether or not to deploy crowd control tactics and formations and/or the use of force to make mass arrests based on the fluid scenario and the degree of disruption.

- C. Non-Peaceful Civil Disobedience – defined as a march or demonstration, whether they possess a parade permit or lack such a permit, that could be static or moving where the participants engage in unlawful behavior that causes damage to property and/or injury to themselves or others. This type of march or demonstration significantly infringes on the civil or property rights of others and/or causes major disruption to the city’s infrastructure, parks, roadways, traffic or commerce.

The presence of police officers at the scene of a civil disturbance or crowd control situation will not necessarily prevent an unruly crowd from committing acts of violence or destruction of property. During non-peaceful acts of civil disobedience, violent marches, violent rallies or violent demonstrations, the Incident Commander will monitor the crowd’s behavior and direct law enforcement personnel to engage persons involved in any violent and/or criminal activities as appropriate. The Incident Commander or the Tactical Commander on scene will decide to what degree the Use of Force Continuum for Crowd Control Situations or Civil Disturbances

outlined below shall be utilized, up to and including the employment of mass arrests to restore order.

## Sec. 2 Use of Force Continuum for Crowd Control Situations and Civil Disturbances

The five phases of force described below do not alter or change the Use of Force policies of the Boston Police Department as described in BPD Rules 303, 303A and 304 and, to the extent possible, any and all law enforcement agencies working with the Department. These five

phases of control are meant to give officers guidelines as to what weapons systems or tools are appropriate for particular situations and when to apply them.

Listed below in Section 8, (F), are the four levels of Department response to crowd control situations or civil disturbances and who should respond. Note that Level III (and higher) authorizes the Public Order Platoons, made up of members of the Special Operations Division the Youth Violence Strike Force and Drug Control Unit. Each to be equipped with less lethal weapons systems and chemical munitions and equipment and to utilize them as deemed necessary to neutralize the situation.

- A. Constructive Force – mere uniformed police presence. This presence may be in the form of individual officers assigned to posts or officers assigned to crowd control formations. Officers may be in soft uniforms (standard police uniforms) or outfitted in authorized crowd control equipment. Generally, there is no physical contact between police and demonstrators at this level of force.
- B. Physical Force – in accordance with the provisions of BPD Rule 304, this is reasonable force, which is defined as the least amount of force that will permit officers to subdue or arrest a subject while still maintaining a high level of safety for themselves and the public. Such force may involve hands-on touching, but does not include the use or deployment of tools or weapons systems. The decision to use physical force may include the deployment of officers in squads or platoons whether they are on foot, motorcycles, bicycles, or in cruisers. Such deployment may involve the use of approved crowd control formations such as skirmish lines, wedge formations, crossbow formations and arrest teams (with or without protective shields) that are capable of dispersing a crowd or making arrests.
- C. Mechanical Force – Force within this area is broken down into two stages of tools and/or weapons systems:
  - 1. Stage I – In accordance with Rule 304 §5, the Department currently authorizes several baton-type or impact implements for use as non-lethal weapons against assailants, i.e., 24" police baton, 36" riot batons, et cetera. Additionally, within this level Department issued incapacitating spray (OC spray), as well as the Jay-Cor pepper ball system and/or smoke canisters may be utilized.
  - 2. Stage II – Includes the use of Less-lethal projectiles, i.e., FN 303 projectile system, sting balls, 12 Gauge CTS Super Sock BeanBag Munitions, 37mm or 40mm launched munitions, noise flash diversionary devices and smoke canisters. Less-lethal munitions consist of projectiles launched or otherwise deployed for the purpose of overcoming resistance, preventing escape, effecting an arrest or reducing serious injury. Less-lethal munitions are meant to significantly reduce the likelihood of causing serious injury or death and are divided into three (3) broad categories:

- a. Target Specific – Involves a situation where there is an identified individual target who is involved in unlawful or criminal activities. In tactical situations, any and all of the above weapons may be used by the Boston Police SWAT Team. Likewise, any and all of the above weapons systems may be authorized for use in a crowd control situation or civil disturbance. However, only officers who have been trained and certified in their use may use the above weapons.
  - b. Group Specific – Involves a situation where there is no identified individual target or where group behavior must be modified. In such situations, Department authorized less-lethal weapon systems would be utilized against a crowd in order to move them from an area, to prevent injury to civilians and/or officers or to prevent damage or destruction of property. As noted above, only officers who have been trained and certified in their use may use the above weapons.
  - c. Tactical Discharge – Involves a pre-planned operation. Most such situations will involve the Entry and Apprehension Team in situations such as warrant service against a high risk offender, neutralization of a barricaded subject, a high risk take-down arrest (either static or mobile), disarming an emotionally disturbed person that is doing or threatening harm to themselves or others, et cetera. In such situations, Department authorized less-lethal weapon systems would be utilized under the direction and supervision of the on scene Tactical Commander, but only by officers who have been trained and certified in their use.
- D. Chemical Force – Tools or weapons systems that disperse chemical irritants or incapacitating spray. Such force includes, but is not limited to, the use of OC spray, hand-held MK-9 or MK-46 canisters, OC sting ball munitions, Jac-Cor OC and FN 303 OC projectile systems, 12ga. launched munitions, 37mm and 40mm launched chemical munitions and hand-held and launchable CS agents.
- E. Deadly Force – Deadly force may only be used in accordance with the provisions of BPD Rule 303. There is no exception to the Department's use of force policy regarding the use of deadly force during crowd control situations and/or civil disturbances. Such situations do not alter the Department's use of force policy regarding the use of deadly force.

It is the responsibility of the Incident Commander or, when designated, the Operations Section Chief (on scene Tactical Commander) to evaluate the crowd control situation or civil disturbance to determine the level of force to be utilized and to authorize its use.

### Sec. 3 Definitions

- A. Containment – to confine unlawful disorder to the smallest possible area.

- B. Isolation – to prevent growth of the unlawful disorder and to deny access to others who, for their own safety, are not involved.
- C. Dispersal – to disperse the crowd and to take appropriate action against law violators

#### Sec. 4 Tactical Objectives

- A. Control the crowd, march or moving protest with safety and with minimal injury, taking into consideration the sworn officers, the protesters and the uninvolved bystanders.
- B. Establish order and traffic control points as directed by the Incident Commander.
- C. Respect the rights of all citizens to peacefully protest and/or march.

#### Sec. 5 Duties of First Responding Officer

In addition to any general responsibilities described previously, first responding officers shall:

- A. Evaluate the situation and notify the Communications Division of the existence of a Code 100 event including its type, nature and/or cause. Possible types are not limited to:
  - 1. Peaceful stationary protest;
  - 2. Moving protest or march on city streets, parks or private property;
  - 3. Building take-over or blocking of entrances or exits;
  - 4. Sit-down protest in the city streets or on private property;
  - 5. Demonstration at a government facility or transportation facility; and
  - 6. Crowd control problem at a fire, structural collapse, HazMat incident, concert or sporting event;
    - B. Estimate the size of the crowd and their intentions, if known, and notify the Communications Division;
    - C. Request a Patrol Supervisor respond to the scene;
    - D. Assume the role of Incident Commander until relieved, including the following duties:
      - 1. Identify a staging area for responding units;



2. Notify the Communications Division as to the best route for additional responding units;
3. Notify the Communications Division of the locations of streets that will need to be blocked, diverted or closed;
4. Request the Communications Division contact other agencies if impacted, e.g., MBTA Police, State Police, Federal Agencies and MBTA bus routes, if affected;
5. Begin an incident log; and
6. Prepare to brief the Patrol Supervisor.

#### Sec. 6 Duties of Communications Division

- A. Notify the Patrol Supervisor responsible for that Sector;
- B. Make all requested notifications and pages to Command Staff, the District Commander and any impacted outside Agencies; and
- C. Prepare to open a clear channel for communications and assign a dispatcher for the incident, if requested.

#### Sec. 7 Duties of Patrol Supervisor

In addition to any general responsibilities described previously, upon arrival the Patrol Supervisor shall:

- A. Announce arrival and assumption of the duties of the Incident Commander by radio;
- B. Get a briefing from the first responding officer and re-evaluate the crowd control situation;
- C. Re-evaluate the staging area and notify the Communications Division if the staging area will remain the same or be re-located due to the changing situation;
- D. Assign someone to the staging area to act as the staging area manager;
- E. Re-evaluate the size and/or number of people in the crowd and update the Communications Division;
- F. Ensure that an incident log is being maintained, either by the first responding officer or another designee;
- G. Assign or re-assign responding units and brief them as to their duties;

- H. Attempt to make contact with the protest organizers and find out their intentions, their route of march and/or the length of their protest;
- I. Attempt to determine if the event has been issued a permit by the City or another organization;
- J. Meet with other agency representatives if on the scene (MBTA Police, State Police, Campus Police, Boston Transportation Department, et cetera);
- K. Request that Mobile Operations respond, if deemed necessary;
- L. Evaluate the need for further resources from the Bureau of Special Operations;
- M. Request the activation of the Emergency Deployment Team (EDT), if deemed necessary;
- N. Upon their arrival at the staging area, ensure that the EDT is properly equipped and are organized into equal squads under the command of a supervisor;
- O. Evaluate the need to have prisoner transport wagons respond to the staging area; and
- P. Prepare to brief the District Commander or other higher ranking officer who responds and assumes command.

#### Sec. 6 Duties of District Commander and/or Incident Commander

In addition to any other duties described previously, the District Commander or other higher ranking officer on scene shall:

- A. Announce their arrival and assumption of the duties of the Incident Commander by radio;
- B. Receive a briefing from the previous Incident Commander;
- C. Re-evaluate the staging area and notify the Communications Division if the staging area will remain the same or be re-located due to the changing situation;
- D. Ensure that a staging area manager has been designated;
- E. Ensure that an incident log is being maintained either by the first responding officer or another designee;
- F. Identify the appropriate level of Department response needed, such as:
  - 1. Level I – The first level of deployment in accordance with the District Commander's plans is made up of district personnel. This deployment is in anticipation of a small

to medium-sized group with little or no violence or disruption to the event. Level I response will be under the direct command of the District Commander;

2. Level II – The second level of deployment will be to utilize the Department's Emergency Deployment Team (EDT). The escalation to Level II will depend on the escalation of size of the crowd, their behavior and the violence and disruption being caused. The decision to escalate to Level II will be made by the District Commander, or in the case of an emergency prior to the arrival of the District Commander, the Incident Commander. If the EDT is to be used, the Incident Commander will ensure that they are properly equipped and are organized into equal squads under the command of a supervisor.
  3. Level III – the third level of deployment will consist of the activation of the Public Order Platoons (POP). The POP's will be made up of personnel from the Special Operations Division and the Youth Violence Strike Force and Drug Control Unit. The POP's will be deployed in cases of extreme violence and disruption or when the potential exists for such a situation to develop. The POP's will be equipped with "less lethal" weapons, chemical munitions and any other equipment deemed necessary to neutralize the situation. The decision to escalate to Level III will be made by the Incident Commander.
  4. Level IV – The fourth level of deployment will consist of full deployment of Department resources, as well as other agencies, i.e., mutual aid. The escalation to Level IV should be considered prior to full scale rioting and in cases where the loss of control of the situation is imminent. The decision to escalate to Level IV will be the responsibility of the Incident Commander after consultation with the Emergency Operation Center (EOC).
- G. Make such assignments as necessary under the Incident Command System to ensure the safe and timely resolution of the incident;
  - H. Be aware of the limits of the training and personal protective equipment possessed by the responding officers;
  - I. Give timely updates on conditions to the Communications Division for dissemination to the Emergency Operations Center and the Command Staff;
  - J. Evaluate the need for prisoner transport wagons to respond to the staging area and/or request additional prisoner transport wagons;
  - K. Request a representative from the Office of Media Relations respond to the scene to act as the Information Officer;
  - L. Request units from Boston Emergency Medical Service respond to the staging area;

- M. Request Special Operations K-9 and/or Mounted units respond to the staging area in anticipation of performing security and crowd control duties, if deemed necessary;
- N. Request the Video Unit respond to the staging area;
- O. If not already on scene, request the Intelligence Unit respond to the staging area; and
- P. If the situation has been upgraded to a Level II, Level III or Level IV response, designate an Operations Section Chief to be in charge of the tactical response.

Addendum C - Code 101  
Fire and Structural Collapse  
Incidents

- 1. Fires
- 2. Structural Collapse

I. FIRES

Incident Command at the scene of a working fire within the City resides with the Boston Fire Department. The general duties of police officers at Fire incidents is to perform the following tasks within the limits of their training and personal protective equipment:

Provide personnel to secure the area and the Incident Command Post during an incident;

Establish access control and traffic control points as directed by the Incident Commander; and

Evacuate or notify affected populations and assist in making other warnings as directed by the Incident Commander.

Sec. 1 Duties of First Responding Officer

In addition to the general duties of first responding officers described previously, officers shall:

- 1. Notify the Communications Division of the conditions found on scene and confirm the existence of a Code 101 event, including;
  - 1. The type of fire and its extent;
  - 2. The intensity of the smoke;
  - 3. Wind direction and approximate speed; and

4. Whether or not there are victims inside the fire zone;
2. Determine a safe route of entry (uphill, upwind) for other responders and advise if personal protective equipment is needed for a safe response;
3. Begin an Incident Log;
4. Unless the Fire Department is already on scene, assume Incident Command and prepare to secure the area immediately adjacent to the fire;
5. Maintain radio communications with the Communications Division and keep them advised as to the progress of the situation;
6. Detain any witnesses to establish if a crime has been committed and identify any suspects and/or weapons utilized; and
7. Prepare to brief the Patrol Supervisor and/or responding Fire Department personnel.

## Sec. 2 Communications Division

1. Notify the Boston Fire Department;
2. Notify Emergency Medical Services;
3. Notify the Patrol Supervisor responsible for that Sector;
4. Dispatch sufficient units to control and isolate access to the scene; and
5. Make such other notifications as may be required.

## Sec. 3 Duties of Patrol Supervisor

In addition to the general responsibilities described previously, responding Patrol Supervisors shall:

1. In the absence of Fire Department personnel, announce their arrival and their assumption of the duties of the Incident Commander by radio;
2. If Fire Department personnel are on scene, establish liaison with their Incident Commander and render any assistance required within the limits of training and personal protective equipment;
3. Ensure that the first responding officer or another designee is maintaining an Incident Log;
4. Identify a staging area for responding law enforcement assets and designate a staging area manager;
5. Secure the perimeter and the Incident Command Post;
6. Establish access control and traffic control points as directed by the Incident Commander (Ranking on-scene Fire Department Officer);

7. Begin planning evacuation routes for implementation (only upon receipt of a lawful order to do so); and
8. Prepare to brief the District Commander.

#### Sec. 4 District Commander

In addition to the general responsibilities described previously, District Commanders shall:

1. Announce their arrival and their assumption of command of all law enforcement assets on-scene by radio;
2. Respond to the Incident Command Post and receive a briefing from the Patrol Supervisor;
3. Designate a Superior Officer to work with the Fire Department Operations Chief;
4. Make such assignments as necessary under the Incident Command System to ensure the safe and timely resolution of the incident;
5. Be prepared to render any assistance required within the limits of the training and personal protective equipment possessed by responding officers; and
6. Give timely updates on conditions to the Communications Division for dissemination to the Command Staff.

## II. STRUCTURAL COLLAPSE

Incident Command at the scene of a Structural Collapse within the City resides with the Boston Fire Department. The duties of Police at Structural Collapse incidents is to perform the following tasks within the limits of their Training and Personal Protective Equipment:

1. Provide personnel to secure the area and the Incident Command Post during an incident;
2. Establish access control and traffic control points as directed by the Incident Commander; and
3. Evacuate or notify affected populations and assist in making other warnings as directed by the Incident Commander.

#### Sec. 1 First Responding Officer

In addition to the general duties of first responding officers described previously, officers shall:

1. Notify the Communications Division of the conditions found on scene and confirm the existence of a Code 101 event, including;
  1. The type of structure and extent of collapse;

2. The presence of any significant hazard; and
3. Whether or not there are victims inside the structure;
2. Determine a safe route of entry for other responders and advise of areas or streets that are deemed unsafe for units to enter or use;
3. Begin an Incident Log;
4. Unless the Fire Department is already on scene, assume Incident Command and prepare to secure the area immediately adjacent to the structure;
5. Maintain radio communications with the Communications Division and keep them informed as to the progression of the incident;
6. Render first aid to injured persons if able to do so; and
7. Prepare to brief the Patrol Supervisor and/or responding Fire Department and Emergency Medical Service personnel.

#### Sec. 2 Communications Division

1. Notify the Boston Fire Department;
2. Notify the Emergency Medical Service;
3. Notify the Patrol Supervisor responsible for that Sector; and
4. Dispatch sufficient units to isolate and control access to the scene and make such other notifications as may be required.

#### Sec. 3 Duties of Patrol Supervisor

In addition to the general responsibilities described previously, responding Patrol Supervisors shall:

1. In the absence of Fire Department personnel, announce their arrival and their assumption of the duties of the Incident Commander by radio;
2. If Fire Department personnel are on scene, establish liaison with their Incident Commander and render any assistance required within the limits of training and personal protective equipment;
3. Ensure that the first responding officer or another designee is maintaining an Incident Log;
4. Identify a staging area for responding law enforcement assets and designate a staging area manager;
5. Secure the perimeter and the Incident Command Post;
6. Establish access control and traffic control points as directed by the Incident Commander (Ranking on-scene Fire Department Officer);
7. Prepare to brief the District Commander.

#### Sec. 4 District Commander

In addition to the general responsibilities described previously, District Commanders shall:

1. Announce their arrival and their assumption of command of all law enforcement assets on-scene by radio;
  2. Respond to the Incident Command Post and receive a briefing from the Patrol Supervisor;
  3. Designate a Superior Officer to work with the Fire Department Operations Chief and Emergency Medical Services;
  4. Make such assignments as necessary under the Incident Command System to ensure the safe and timely resolution of the incident;
  5. Be prepared to render any assistance required within the limits of the training and personal protective equipment possessed by responding officers; and
  6. Give timely updates on conditions to the Communications Division for dissemination to the Command Staff.
- 

Addendum D - Code 102  
Mass Casualty Incident

#### General Considerations

Incident Command at the scene of a Mass Casualty Incident within the City resides with the Boston Fire Department. The duties of Police at Mass Casualty incidents is to perform the following tasks within the limits of their training and personal protective equipment:

1. Provide personnel to secure the area and the Incident Command Post during an incident;
2. Establish access control and traffic control points as directed by the Incident Commander; and
3. Assist in making warnings and notifications as directed by the Incident Commander.

#### Sec. 1 First Responding Officer

In addition to the general duties of first responding officers described previously, officers shall:

1. Notify the Communications Division of the conditions found on scene and confirm the existence of a Code 102 event, including;
  1. The type of incident and approximate number of casualties;
  2. The presence of any significant hazard;
  3. The presence of an obvious vapor plume; and
  4. Whether or not there are victims and an estimate of their number;
2. Determine a safe route of entry for other responders and advise if personal protective equipment is needed for a safe response;



3. Begin an Incident Log;
4. Unless the Fire Department is already on scene, assume Incident Command and prepare to secure the immediate area; and
5. Prepare to brief the Patrol Supervisor and/or responding Fire Department and Emergency Medical Service personnel.

## Sec. 2 Communications Division

1. Notify the Boston Fire Department;
2. Notify the Emergency Medical Service;
3. Notify the Patrol Supervisor responsible for that Sector; and
4. Make such other notifications as may be required.

## Sec. 3 Duties of Patrol Supervisor

In addition to the general responsibilities described previously, responding Patrol Supervisors shall:

1. In the absence of Fire Department personnel, announce their arrival and their assumption of the duties of the Incident Commander by radio;
2. If Fire Department personnel are on scene, establish liaison with their Incident Commander and render any assistance required within the limits of training and personal protective equipment;
3. Have the ranking officer of the Hazardous Materials Unit respond and be guided by the advice of the Hazardous Materials Officer as to personnel safety considerations and methods of deployment of Law Enforcement Assets;
4. Ensure that the first responding officer or another designee is maintaining an Incident Log;
5. Identify a staging area for responding law enforcement assets and designate a staging area manager;
6. Secure the perimeter and the Incident Command Post;
7. Establish access control and traffic control points as directed by the Incident Commander (Ranking on-scene Fire Department Officer);
8. Begin planning evacuation routes for implementation (only upon receipt of a lawful order to do so); and
9. Prepare to brief the District Commander.

## Sec. 4 District Commander

In addition to the general responsibilities described previously, District Commanders shall:

1. Announce their arrival and their assumption of command of all law enforcement assets on-scene;

2. Respond to the Incident Command Post and receive a briefing from the Patrol Supervisor;
  3. Designate a Superior Officer to work with the Fire Department Operations Chief;
  4. Designate a Superior Officer to work with the Emergency Medical Service Operations Chief;
  5. Make such assignments as necessary under the Incident Command System to ensure the safe and timely resolution of the incident;
  6. Be prepared to render any assistance required within the limits of the training and personal protective equipment possessed by responding officers; and
  7. Give timely updates on conditions to the Communications Division for dissemination to the Command Staff.
- 

Addendum E - Code 103  
Natural Disasters  
(e.g., hurricane, major storm, etc.)

#### General Considerations

Incident Command at the scene of a Natural Disaster Incident (e.g., hurricane, major storm, etc.) within the City resides with the Boston Emergency Management Agency (BEMA) who will activate the Boston Emergency Operations Center (EOC) whenever necessary.

With the possible exception of tornadoes or earthquakes, a Code 103 - Natural Disaster event usually has sufficient lead time for adequate preparation. The Department would maintain liaison with the agency having primary jurisdiction of the event and provide such law enforcement resources as are requested.

Generally, the duties of the Police Department at natural disaster incidents is to perform the following tasks within the limits of their training and personal protective equipment:

1. Maintenance of law and order;
2. Coordination of all law enforcement activities in Boston;
3. Providing crowd control and traffic control;
4. Providing access control to restricted areas;
5. Protecting key facilities;
6. Warning support (loudspeakers, radios, etc.)
7. Maintaining liaison and coordination with other law enforcement agencies;
8. Providing damage assessment support;
9. Evacuating, relocating and housing of prisoners;
10. Supporting aerial search and rescue operations;

11. Supporting medical rescue operations;
12. Providing policy, coordination and operations group staff support; support to the EOC for 24-hour operation during an emergency; and
13. Providing security for reception centers, lodging and feeding facilities and emergency shelters.

The Police Commissioner, Superintendent-in-Chief or their designee shall establish liaison with the EOC and provide such support and resources as are required.

---

### **Addendum F - Code 104**

#### **Hazardous Materials (HazMat) and Weapons of Mass Destruction (WMD) Incidents**

1. Hazardous Materials (HazMat)
2. Weapons of Mass Destruction (WMD)

#### **I. HAZARDOUS MATERIALS**

##### **General Considerations**

Incident Command at the scene of a Hazardous Materials (HazMat) incident within the City resides with the Boston Fire Department. The duties of Police at HazMat incidents is to perform the following tasks within the limits of their Training and Personal Protective Equipment

1. Provide personnel to secure the area and the Incident Command Post during an incident;
2. Establish access control and traffic control points as directed by the Incident Commander; and
3. Evacuate or notify affected populations and assist in making other warnings as directed by the Incident Commander.

#### **Sec. 1 First Responding Officer**

In addition to the general duties of first responding officers described previously, officers shall:

1. Notify the Communications Division of the conditions found on scene and confirm the existence of a Code 104 event, including;

1. The type of materials involved, if possible, and whatever indications of a release are visible from a safe distance;
  2. Wind direction and approximate speed;
  3. The presence of an obvious vapor plume; and
  4. Whether or not there are victims;
2. Determine a safe route of entry for other responders and advise if personal protective equipment is needed for a safe response;
3. Begin an Incident Log;
4. Unless the Fire Department is already on scene, assume Incident Command and prepare to secure the immediate and downwind hazard areas;
5. Maintain radio communications with the Communications Division and keep them informed of the progression of the situation;
6. Render first aid to any victims if it can be done without becoming contaminated; and
7. Prepare to brief the Patrol Supervisor and/or responding Fire Department and Emergency Medical Service personnel.

## Sec. 2 Communications Division

1. Notify the Boston Fire Department;
2. Notify the Boston Police Hazardous Materials Unit;
3. Notify the Emergency Medical Service;
4. Notify the Patrol Supervisor responsible for that Sector;
5. Dispatch sufficient units to control and isolate access to the scene; and
6. Make such other notifications as may be required.

## Sec. 3 Duties of Patrol Supervisor

In addition to the general responsibilities described previously, responding Patrol Supervisors shall:

1. In the absence of Fire Department personnel, announce their arrival and their assumption of the duties of the Incident Commander by radio;
2. If Fire Department personnel are on scene, establish liaison with their Incident Commander and render any assistance required within the limits of training and personal protective equipment;
3. Have the ranking officer of the Hazardous Materials Unit respond and be guided by the advice of the Hazardous Materials Officer as to personnel safety considerations and methods of deployment of Law Enforcement Assets;
4. Ensure that the first responding officer or another designee is maintaining an Incident Log;
5. Identify a staging area for responding law enforcement assets and designate a staging area manager;
6. Secure the perimeter and the Incident Command Post;

7. Establish access control and traffic control points as directed by the Incident Commander (Ranking on-scene Fire Department Officer);
8. Begin planning evacuation routes for implementation (only upon receipt of a lawful order to do so); and
9. Prepare to brief the District Commander.

#### Sec. 4 District Commander

In addition to the general responsibilities described previously, District Commanders shall:

1. Announce their arrival and their assumption of command of all law enforcement assets on-scene by radio;
2. Respond to the Incident Command Post and receive a briefing from the Patrol Supervisor;
3. Be guided by the recommendations made by the Hazardous Materials Officer;
4. Designate a Superior Officer to work with the Fire Department Operations Chief;
5. Make such assignments as necessary under the Incident Command System to ensure the safe and timely resolution of the incident;
6. Be prepared to render any assistance required within the limits of the training and personal protective equipment possessed by responding officers; and
7. Give timely updates on conditions to the Communications Division for dissemination to the Command Staff.

#### Sec. 5 Hazardous Materials Unit

1. An officer from the Hazardous Materials (HazMat) Unit shall respond to the scene of all HazMat incidents and report to the highest ranking Department officer on scene.
2. The HazMat officer shall confer with Fire Department personnel, make his own assessment as to the safety of law enforcement responders and make recommendations for the safe staging and assignment of these assets to the Ranking Boston Police officer on scene.
3. The HazMat officer shall be responsible for making continuous site assessments and conducting timely briefings of the Ranking Officer on-scene, as well as the Duty Supervisor of the Communications Division.
4. If an unsafe condition exists which unduly threatens the lives and safety of law enforcement assets, the HazMat officer shall bring it to the attention of the Ranking Officer on-scene, who shall be guided by his recommendations to re-deploy or suspend operations.
5. HazMat officers shall act according to the limits of their training and personal protective equipment.

## II. WEAPONS OF MASS DESTRUCTION (WMD)

### General Considerations

Weapons of Mass Destruction (WMD) events would likely be terrorist events that usually target locations of special significance at times when a large population would be present in order to obtain the greatest amount of casualties. Using Chemical, Biological or Radiological agents, WMD events may seriously affect both the short term and long term health, infrastructure and economic welfare of the City.

The primary jurisdiction and lead-investigating agency will be the FBI, whose field office will set up a Joint Operations Center (JOC). BEMA will set up their EOC in order to support the JOC. The duties of the Boston Police are to perform the following tasks within the limits of their training and personal protective equipment:

1. Provide Security personnel to limit access to the "exclusion zone" and incident command post during the incident;
2. Establish access control and traffic control points as directed by the Incident Commander (IC);
3. Evacuate or notify affected populations to shelter in place, and assist in making other warnings as directed by the IC;
4. Assist the FBI with intelligence gathering and crime scene services;
5. Provide EOD services in search of secondary devices; and
6. Provide tactical response team services.

#### Sec. 1 First Responding Officer

In addition to the general responsibilities described previously, first responding officers shall:

1. Notify the Operations of conditions found including and confirm the existence of a Code 104 event, including:
  1. Identifying the type of materials involved if possible and whatever indications of a release are visible from a safe distance;
  2. Determining wind direction and approximate speed;
  3. The presence of an obvious vapor plume;
  4. Signs and symptoms of any victims;
2. Identify safe routes of entry (Uphill, Upwind) for other responders and advise the Communications Division of areas and streets that are unsafe for units to enter;
3. Advise if Personal Protective Equipment is needed for a safe response;
4. Begin incident log;
5. Unless the Fire Department is already on scene, assume Incident Command and prepare to secure the immediate and downwind hazard area;
6. Request and prepare to brief the Patrol Supervisor and responding Fire Department personnel;
7. Maintain radio communications with operations informing of progression of situation;
8. Assist with victims if it can be done without becoming contaminated; and

9. If it can be done without becoming contaminated, detain witnesses so as to establish if a crime was committed, the number and description of any suspects, and a description of any dissemination devices used.

## Sec. 2 Communications Division

1. Notify Boston Fire Department;
2. Notify Boston Emergency Medical Services;
3. Notify the Boston Police Hazardous Materials Unit;
4. Notify the Patrol Supervisor responsible for that Sector;
5. Dispatch sufficient units to isolate and control access to the scene; and
6. Secure a clear channel for incident operations.

## Sec. 3 Patrol Supervisor

1. Unless Fire Department personnel are already on scene, announce arrival and assumption of Incident Command by radio;
2. If Fire Department Personnel are on scene, establish liaison with the Incident Commander and render any assistance required within the limits of training and personal protective equipment;
3. Have the ranking officer of the Hazardous Materials Unit respond to his location and be guided by the advice of the Hazardous Materials Officer as to personnel safety considerations and methods of deployment of Law Enforcement Assets;
4. Assign an officer to maintain an incident log if the First Responding Officer is to be assigned other duties;
5. Identify the most appropriate pre-designated Staging Area for responding Law Enforcement Assets and assign a Staging Area Manager;
6. Secure the "Hot Zone" and Incident Command Post;
7. Establish Access Control and Traffic Control Points as directed by the Incident Commander (Ranking on-scene Fire Department Officer if JOC not in place);
8. Begin planning evacuation routes and be ready for implementation upon receiving a lawful order to do so; and
9. Request and prepare to brief the District Commander.

## Sec. 4 District Commander

1. Announce arrival and assumption of command of all Law Enforcement Assets on-scene by radio;
2. Respond to Incident Command Post, receive a briefing from the Patrol Supervisor;
3. Be guided by recommendations made by the Hazardous Materials Officer;
4. Identify and appoint a Superior Officer to work with the ICS Operations Section Chief;
5. Make such assignments as are necessary under the Incident Command System to ensure the safe and timely disposition of the incident;

6. Be prepared to render any assistance required within the limits of the training and personal protective equipment possessed by responding officers; and
7. Give timely updates on conditions to the Communications Division for dissemination to the Command Staff.

#### Sec. 5 Hazardous Materials Unit

1. An officer from the Hazardous Materials (HazMat) Unit shall respond to the scene of all HazMat incidents and report to the highest ranking Department officer on scene.
2. The HazMat officer shall confer with Fire Department personnel, make his own assessment as to the safety of law enforcement responders and make recommendations for the safe staging and assignment of these assets to the Ranking Boston Police officer on scene.
3. The HazMat officer shall be responsible for making continuous site assessments and conducting timely briefings of the Ranking Officer on-scene, as well as the Duty Supervisor of the Communications Division.
4. If an unsafe condition exists which unduly threatens the lives and safety of law enforcement assets, the HazMat officer shall bring it to the attention of the Ranking Officer on-scene, who shall be guided by his recommendations to re-deploy or suspend operations.
5. HazMat officers shall act according to the limits of their training and personal protective equipment.

---

### **Addendum G – Code 105** **Active Shooter Incident Rapid** **Deployment Protocol**

---

**Sec. 1 Purpose:** The primary mission in an active shooter incident is to save as many lives as possible. The only way to accomplish this is to locate the threat and neutralize it as quickly as possible.

**Sec. 2 General Considerations:** Active shooter incidents present complex problems for the Boston Police Department as well as for law enforcement in general. Active shooter cases may involve a suspect or suspects with multiple weapons, high caliber weapons and, in some cases, automatic weapons. Active shooter scenarios can happen at any time and at any place. The common factor in all the cases is that there is “ongoing shots fired” and the suspect(s) is actively engaged in creating death or great bodily injury. Immediate Action Rapid Deployment tactics are not a substitute for conventional response tactics to a barricaded gunman.



### **Sec. 3 Definitions:**

A. Active Shooter – Suspect(s) activity is immediately causing death and serious bodily injury. The activity is not contained and there is immediate risk of death or serious injury to potential victims.

B. Rapid Deployment Protocol – The swift and immediate deployment of law enforcement resources to on-going, life-threatening situations where delayed deployment could otherwise result in death or great bodily injury to innocent persons.

### **Sec. 4 Duties of the First Responding Officer:**

- A. Assess the situation.
- B. Until relieved by a supervisor, assume the duties of the Incident Commander (IC) and establish an Incident Command.
- C. Request appropriate resources:
  - 1. Supervisor
  - 2. Additional Patrol Units
  - 3. Boston Police SWAT Team
  - 4. Hostage Negotiation Team
  - 5. Emergency Medical Services
  - 6. Bomb Squad
  - 7. Fire Department
  - 8. Outside agency support if needed
- D. Determine if Rapid Deployment Protocol (Move to Contact) action is necessary.
- E. Broadcast Situation to Responding Units:
  - 1. Location of incident and address with cross street, if possible.
  - 2. Type of location involved, School, Business Private Home Playground etc.
  - 3. Safest approach for responding units.
  - 4. Location & number of suspect(s) (if known).
  - 5. Type(s) of weapon(s) involved (if known).
- F. Establish a Command Post location.
- G. Designate a staging area for responding units.
- H. Designate the members of the Contact and/or Rescue Team(s) ensuring that each team consists of a minimum of four (4) officers.

### **Sec. 5 Contact Team:**

- A. Contact Teams consist of a minimum of four (4) Officers:
  - 1. Team Leader:
    - a. Formulates & implements a plan.
    - b. Makes deployment decisions and delegates team member responsibilities.

2. Assistant Team Leader:
    - a. Communicates with responding units.
    - b. Acts as additional Contact or Rescue Officer.
  3. Point Officer:

Provides cover for area of responsibility and engages suspect(s), if necessary.
  4. Rear Guard Officer:

Provides cover for area of responsibility and engages suspect(s), if necessary.
- B. The Contact Team(s) shall:
1. Move to make contact with the threat and neutralize it.
  2. Limit suspect(s) movement by containment.
  3. Prevent escape.
  4. Continue to move past any victims.
  5. Communicate progress (location and situation).
  6. Provide preliminary assessment:
    - a. Victim(s) – location & medical needs (prioritize if possible –dead vs. living and condition).
    - b. Explosive(s) – type(s) and location, if known.
    - c. Suspect(s) – description and location, if known.
    - d. Weapon(s) – type(s) and number, if known.

## **Sec. 6 Rescue Team:**

- A. Only the Incident Commander may determine when and/or whether to deploy a Rescue Team(s). The first responding officer shall wait for a supervisor to assume command and make this decision.**
- B. When deployed, a Rescue Team shall consist of a minimum of four (4) officers:
- 1. Team Leader:**
    - a. Formulates & implements a plan.
    - b. Makes deployment decisions and delegates team member responsibilities.
  2. Assistant Team Leader:
    - a. Communicates with responding units.
    - b. Acts as additional Contact or Rescue Officer.
  3. Point Officer:

Provides cover for area of responsibility and engages suspect(s), if necessary.
  4. Rear Guard Officer:

Provides cover for area of responsibility and engages suspect(s), if necessary.
- C. The Rescue Team shall:

1. Rescue and recover the victim(s).
2. Extract victim(s) to a designated safe area.
3. Notify Command Post of the number of victims, the types of injuries, if any, and the seriousness of injuries, if any.
4. Report suspect(s) location to Contact Teams.
5. Emphasize custody and control of victims or potential victims.
6. Initiate identification and accountability of victims.
7. Coordinate all actions with Contact Team Leader and the Command Post.

D. When multiple victims are present the Rescue Team shall request that the IC expand the Rescue Team size or number of teams operating in the building.

## **Sec. 7 Tactical Considerations:**

### **A. Contact/Rescue Team Concerns:**

1. Element of surprise
2. Maintaining offensive initiative
3. Security
4. Flexibility of planning/thought
5. Maneuverability
6. Economy of force
7. Deployment of multiple teams:
  - a. Crossfire/Backdrop.
  - b. Target identification.
  - c. Maintenance of radio communication.
  - d. Movement in unfamiliar surroundings.
  - e. Task saturation.
  - f. Lack of direct supervisory control.

### **B. Approach of Contact/Rescue Teams - Use cover and concealment**

whenever you can:

1. Cover – vehicles/other solid objects, etc.
2. Concealment – lighting, fog, smoke, etc.

### **C. Approach Considerations:**

1. Number of suspect(s).
2. Last known location of suspect(s).
3. Type of suspect(s) weapons.
4. Size & layout of structure.
5. Windows & glass doors – approach from the “Cold” angle or side if possible.
6. Floor plans of building.
7. Try to locate the property manager or custodian to obtain plans or information about the building.

### **D. Entry Considerations:**

1. Confusion – victims hiding and frightened and not responding to law enforcement officer directions.
2. Remember that in the Boston School system they are taught to use the B.R.A.C.E. system. The acronym stands for:

**B - Barricade**

**R – Report**

A – Assess

C – Control & Communicate

E - Evacuation

Refer to Boston Public School Safety Contingency Plans for further information about the actions of school administrators and students.

3. Transmit entry point to dispatcher and supervisor if on scene.
4. Update dispatcher and supervisor of location regularly
5. Transmit location of injured victims by using Room numbers or other landmarks within building.
6. Base further movement on the location & direction of other contact Teams if being used.
7. Divide location by levels, wings, floor or groups of smaller buildings.
8. Contact/Rescue Teams shall use the 360-degree coverage formation when moving. The strength of this formation is the firepower moving toward the threat.

**Sec. 8 Boston Police SWAT Team:**

- A. Boston Police SWAT Team personnel are generally better equipped and trained to resolve a crisis scenario. However, continued assistance by the first responding officers is critical. As soon as is practical after Entry and Apprehension Team personnel arrive on scene, the IC shall ensure that first responding officers:
  1. Coordinate and relinquish contact responsibility from the first Contact Teams to Entry and Apprehension Team personnel.
  2. Assist with containment responsibilities, if necessary and if it can be done in a safe manner.
  3. Assist with Rescue Teams, if necessary.
  4. Act as a “pathfinder” for the Entry Team:
    - a. Direct to last known location of suspect(s).
    - b. Report location of explosive, if known.
    - c. Report location of victims if known.
    - d. Provide any pertinent information such as suspect(s) description, weaponry etc.

- e. If relieved, safely leave the building and report to the Incident Commander at the Command Post for debriefing.
  - B. Inner perimeter and Outer perimeter shall be maintained in the manner prescribed in Rule 200, Critical Incident Management.
- 

## **ADDENDUM H**

### **EMERGENCY DEPLOYMENT TEAM**

#### **Purpose:**

To ensure a uniform response to Emergency Deployment Team call-outs for critical incidents within the City of Boston.

#### **General Considerations:**

The Emergency Deployment Team (EDT) is used to assemble a large group of police officers when an immediate response is required. The EDT may be used for, but not limited to, demonstrations, missing children, major fires or explosions, terrorist assaults, security for large crime scenes, etc.. Since the call-out of the EDT usually occurs during times of critical incidents, a swift but safe response is imperative. While an immediate response is expected, officers are reminded that regardless of the emergency, they must adhere to M.G.L. c. 89 § 7B (Operation of Emergency Vehicles).

EDT call-outs will be governed by Rule 200 - Critical Incident Management by using the Incident Command System (ICS).

#### **Section 1**

The Duty Supervisor of each shift will, before roll call, choose three officers from that District to be part of the EDT. One Patrol Supervisor from each Area will also be selected for the EDT. District Commanders in each Area will design a schedule so that one supervisor from that Area is assigned to the EDT each tour. The Supervisor and Police Officers assigned to the EDT will be so noted on that shift's batting order. Batting orders will be faxed to the Dispatch Center immediately after roll call. The Dispatch Center Duty Supervisor will review the batting orders from each District to make sure each District and Area has fulfilled its requirements as it relates to the EDT. Dispatchers shall contact each EDT officer assigned to their channel to confirm their EDT status for that shift.

#### **Section 2**

During times when the District Commander or the Night Commander is not available and the

Incident Commander has requested an EDT call-out, the Dispatch Center Duty Supervisor shall determine if an officer above the rank of sergeant is needed as the platoon commander. If so warranted, the Dispatch Center Duty Supervisor shall ensure the dispatch of a lieutenant from a district other than the district of incident occurrence. The responding lieutenant shall arrive and assume control as the EDT platoon commander. Normally, a lieutenant would not be needed when the EDTs are activated for traffic control or lost children incidents. However, a lieutenant shall be required to respond to all call-outs for critical incidents and actual or anticipated large crowd disturbances.

### Section 3

An Incident Commander is authorized to request an EDT call-out. The Incident Commander should do so by notifying the Dispatcher to activate the EDT. The Incident Commander requesting the EDT should immediately choose a safe staging area and identify safe routes for officer response. The staging area should be outside the inner perimeter and particular attention should be paid to wind direction and topography, when relevant to the situation.

### Section 4

Officers and Supervisors responding to a call-out for an EDT shall respond to the staging area with their Emergency Deployment Team equipment. Whenever a Police Officer assigned to the EDT is unable to immediately respond to an EDT call-out, the officer will immediately notify the Dispatcher. The Dispatcher will immediately notify the Dispatch Center Duty Supervisor, who will assign another unit to respond. For this reason, ALL District Patrol Supervisors and response units assigned to motor vehicles will carry their Emergency Deployment Team equipment in their assigned police vehicle. All other sworn personnel shall have this equipment available to them in the District.

### Section 5

Emergency Deployment Team Equipment shall consist of: a ballistic vest, gas mask, 36" baton, riot helmet with face shield, protective work gloves, dust mask, nitrile gloves, gear bag and any other equipment issued or authorized by the Police Commissioner. Emergency Deployment Team Equipment shall be inspected every Sunday by the District Duty Supervisor at each roll call. This inspection shall be recorded in the administrative detail book.

---

## **Addendum I**

### **CORPORATE EMERGENCY ACCESS SYSTEM (CEAS)**

Sec. 1 Purpose: CEAS is designed to reduce the potential impact of economic injury to a municipality following a serious or catastrophic event by providing quick access to affected work-sites by critical organization employees after an area has been designated as safe. Rapid

facilitation of business recovery activities in an impacted area will allow organizations to assess damage, maintain core IT systems, meet regulatory obligations, and secure or remove critical records and data. Department personnel will assist the Mayor's Office of Emergency Preparedness (MOEP) to ensure that the objectives of this program are met.

**Sec. 2 Process:** Department personnel shall use the following guidelines for determining authorized access to restricted areas during a critical incident.

- A. Access is accomplished by providing a credential, recognized by law enforcement, to essential employees and critical service providers selected by the employer. (Please see attached example)
- B. Credentials are issued pre-event to participating individuals in order to streamline access, eliminate confusion, and give authorities increased control after a disaster event.
- C. Credentials only become valid when public safety officials activate the program, usually following an incident or where control of a specific area is required.
- D. Law enforcement officials control access into restricted areas once immediate safety concerns have been mitigated, and may expand or restrict access at anytime.
- E. There are five levels of access within the system that can be activated at the discretion of officials and are associated with CEAS:
  - a. **Level X - Prohibited Access.**
  - b. **Level D - Direct Involvement only**– Cardholders directly involved in mitigating the emergency.
  - c. **Level C - Critical Industries Only Access** – Critical industries identified by MOHS for priority access based on National Infrastructure Protection Center (NICP) guidelines as well as unique local needs. Cardholders represent the industries deemed “critical” to the economic welfare of the city.
  - d. **Level B - All Industries for basic functions.** Cardholders represent employees of all other participating businesses.
  - e. **Level A - All permitted with possible vehicular limitations.** There are no cards issued with Level A access. Level A is a condition that may be initiated in the event vehicular restrictions must be enacted. Only CEAS cardholders will be able to drive motor vehicles into the City during a Level A activation.
- F. Utility workers and health care professionals with proper employee identification are treated as “emergency responders” and do not require a CEAS credential.
- G. Working press will have press credentials, giving them access to designated areas. The media industry is considered a “Critical Industry,” (Level C).

### **Sec. 3 Program Administration:**

- A. Businesses may apply for credentials based on the number of employees at each of their worksites.
- B. Credentials are issued using a photo ID. (Please see attached example)
- C. The system is self-governed by its participants, who are responsible for identifying their own essential employees, managing turnover, and any title and responsibility changes.
- D. All administrative aspects of the program are handled by the Business Network of Emergency Resources (BNet), a NYS not-for-profit corporation:

Business Network of Emergency Resources, Inc.  
President: Dr. Robert H. Leviton  
11 Hanover Square  
New York, NY 10005  
Phone: 888-353-BNET  
Email: [support@bnetinc.org](mailto:support@bnetinc.org)  
[www.CEAS.com](http://www.CEAS.com)

### **Corporate Emergency Access System (CEAS) Card Composition**

**Rear of**



## Rear of Card

### Note:

- Amended by SO 07-018, issued April 5, 2007, adding Addendum I.
- Amended by SO 07-038, issued June 29, 2007, addendum G (edit to Section 7, subsection D #8).
- Amended by SO 07-056, issued October 3, 2007, "Entry and Apprehension Team" or "Entry Team" in Boston Police Rules and Procedures and Special Orders changed to "Boston Police SWAT Team" in the following sections:

Sec. 4.13

Addendum "A" Code 99

Sec. 1

Sec. 8 - line 5 & 12

Sec. 9 - line 3 & 8

Sec. 11- line 4

Sec. 13- line 6

Sec. 14- Title / line 5, 13, 14 &15

Sec. 15- Mobility/relocation

Addendum "B" Crowd Control

Sec. 2 C- line 2 sub-paragraph "a".

Addendum "G" Code 105 Active Shooter

Sec. 4 - line C Sub-line 3

Sec. 8 - Title / Line "A" sub-line 4

## Rules and Procedures

### Rule 205

October 22, 1998

#### Rule 205 - DEATH INVESTIGATION

The following Rule is issued to establish procedures for Department personnel responding to and/or investigating all reports of the death of a person. The Suffolk County District Attorney, by statute ([M.G.L. c. 38, § 4](#)), is in charge of all death investigations conducted in the County of Suffolk. This Rule also includes the investigation of certain other types of incidents that may or may not result in a death.

#### Sec. 1 GENERAL CONSIDERATIONS

In order to standardize procedures and ensure that each investigation is conducted in a fixed, orderly manner, the following procedures shall serve as a guide to the responding officer and investigator to be followed in all cases. These guidelines are to be construed in a general sense and in no way relieve an investigator from completing any other steps that may be required by a particular case. These procedures should be considered the basic, essential steps for a **preliminary** investigation. The investigator is encouraged to use judgment and initiative in determining what each case demands in the way of additional or **follow-up** investigations. Where there is a doubt or question as to how to proceed in the investigation, the investigator is to consult his/her supervisor.

Beginning with the police call taker who initially takes the call and obtains a crucial piece of information - to the first responding officer - to the investigator - a complete, detailed, practical and thorough investigation is based on team work, cooperation, documentation and compliance with basic crime scene and investigative procedures. The first fifteen (15) to twenty (20) minutes at any incident is decisive in controlling and managing the crime scene.

#### Sec. 2 DEFINITIONS

**Next of Kin:** A relative of a victim who will be recognized in order of priority as follows: 1) spouse, 2) son or daughter, 3) father or mother, 4) legal guardian, 5) grandson or granddaughter, 6) brother or sister, 7) aunt or uncle.

**Personal Property:** May include, but is not limited to: currency, jewelry, bankbooks, wills, negotiable bonds and securities, firearms, et cetera.

**Sudden Death:** The death of a person due to natural causes involving neither violence nor suspicion of violence, but without a physician in attendance (unattended natural death).

### **Sec. 3 RESPONSIBILITIES OF THE PERSON RECEIVING NOTIFICATION**

The **person receiving notification** shall make every effort to obtain and record the following information:

- Exact time the notification was received
- Exact location of the incident;
- Condition of the victim(s);
- Whether suspect(s), or suspect(s)'s vehicle(s) is known
- Locations and descriptions of suspect(s) or suspect(s) vehicle
- Means and direction of flight of suspect(s) or suspect(s)'s vehicle(s);
- Location of the person who first notified the police, if the person will remain there, or the location where the person can be met; and
- Name, address and phone number of the person who first notified the police.

### **Sec. 4 RESPONSIBILITIES OF THE POLICE DISPATCHER**

The **police dispatcher** shall:

- Dispatch sufficient personnel and equipment to handle the situation based on available information,
- Dispatch a District Patrol Supervisor,
- Dispatch a District Detective,
- Dispatch medical and other assistance; and
- Notify the Operations Duty Supervisor.

### **Sec. 5 RESPONSIBILITIES OF THE FIRST OFFICER ON THE SCENE**

The **first officer(s)** on the scene, regardless of rank, has three (3) main objectives which are listed below in order of priority, as applicable:

- Determine whether the victim is alive or dead and initiate the necessary response; ▪ Determine if a crime has been committed, apprehend the perpetrator if still present, or give the appropriate descriptions to the dispatcher; and
- Secure and protect the crime scene and identify any witnesses, suspects and other persons present.

### **Sec. 6 RESPONSIBILITIES OF THE FIRST RESPONDING OFFICER**

The **first responding officer(s)** assigned to the call or incident shall be responsible for performing the following duties, as applicable:

- Request a **Patrol Supervisor** and other assistance as necessary;
- Take accurate, detailed, and complete notes;
- Address and determine the entire area of the crime scene including paths of entry and exit and any areas that may include evidence;
- Isolate the area and refrain from entering the crime scene and/or disturbing, touching, or using any item found therein. **If an object must be moved**, note its exact location, position, and consider the possibility that the object may contain fingerprints. Outside crime scenes require specific steps to protect the scene. At an outside crime scene, a

police line shall be established fifty (50) feet in all directions where appropriate or at such distances as required to freeze the crime scene;

- Prohibit all unauthorized persons from entering the crime scene, including police personnel;
- Restrict police vehicles so they are parked away from the crime scene until the boundaries of the crime scene can be definitively established;
- Instruct medical personnel as to how to enter the crime scene so as to disturb the crime scene as little as possible. The officer should observe the medical personnel and note what objects they move and/or touch;
- Initiate a chronological log (in/out) containing names, titles, and identification numbers of any police, medical, and/or technical personnel entering and leaving the crime scene. **(The log sheet shall be turned over to the investigator-in-charge after the crime scene is vacated and shall be kept in the case file.);**
- Prohibit anyone from smoking at or on the crime scene;
- Prohibit anyone from using any telephone(s) located at or on the crime scene; ▪ Locate and identify the person who first notified police;
- Separate the witnesses while obtaining preliminary statements;
- Brief the **Patrol Supervisor** and the **investigator-in-charge** of the investigation; ▪ Complete incident reports and other reports, as applicable;
- All officers responding to a death investigation shall submit a separate written report (BPD Form 26). District Commanders shall ensure that the original of all such reports is forwarded to the Homicide Unit within twenty-four (24) hours; and
- Vacate the crime scene only at the direction of the **investigator-in-charge** as relayed through the **Operations Duty Supervisor**.

## **Sec. 7 RESPONSIBILITIES OF THE PATROL SUPERVISOR**

**The Patrol Supervisor** on arrival at the crime scene shall be responsible for performing the following duties, as applicable:

- Take charge of the crime scene and assign personnel as deemed appropriate; ▪ Assign an officer to accompany the victim(s) to the hospital;
- Assign an officer to accompany any vehicle(s) which are being towed and held for evidence or for later processing;
- Debrief the first responding officer so as to ascertain the facts surrounding the incident; ▪ Ensure that the duties of the first responding officer are being performed satisfactorily with particular attention to: initiating and keeping up to date a chronological log; isolating and protecting the crime scene; and identifying and separating any witnesses; ▪ Establish a Command Post **outside** of the inner perimeter of the crime scene, if applicable;
- Establish an outer perimeter;
- Brief the **investigator-in-charge**;
- Assist the **investigator-in-charge** with crime scene management during the **preliminary** investigation, utilizing whatever personnel are deemed necessary;

- Update the **Operations Duty Supervisor**;
- Ensure that all incident reports and other reports are completed and typed;
- Ensure that separate reports (Form 26) are submitted and signed by each member of the unit in which both the first officer on the scene and the first responding officer are assigned; and
- Ensure that the crime scene is vacated only at the direction of the **investigator-in-charge** as relayed through the **Operations Duty Supervisor**.

#### **Sec. 8 RESPONSIBILITIES OF AN OFFICER ASSIGNED TO ACCOMPANY VICTIM TO HOSPITAL**

If victim is moved to the hospital, the victim should be accompanied by a police officer. The officer accompanying a victim to the hospital is responsible for attempting to ascertain the condition of the victim; for attempting to identify possible witnesses and family members of the victim; and, for the handling and custody of the victim's clothing and other evidence on the victim's person. Such clothing and other evidence should not be mixed together, but should be separated and held as evidence pending the arrival of **homicide investigators, District investigators or Patrol Supervisors**, depending upon which unit is appropriate. Officers are responsible for obtaining the name of the attending physician and, if applicable, the time the victim(s) is pronounced dead.

#### **Sec. 9 ADDITIONAL RESPONSIBILITIES OF PATROL SUPERVISOR IF DEATH IS SUSPECTED TO BE A SUDDEN DEATH**

Only the **Medical Examiner** may rule that the death of a person is a **Sudden Death**, decline jurisdiction, and order the release of the body. In any case where a **Patrol Supervisor**, after assisting the **investigator-in-charge** at any preliminary investigation, suspects that the death may be ruled a **Sudden Death**, the following responsibilities, considerations, and duties shall be in addition to those listed in the previous section.

The **Patrol Supervisor** shall:

- Contact the **Medical Examiner** with all pertinent information gathered in the preliminary investigation;
- Ensure that the Department of Health and Hospitals Emergency Medical Technicians (EMTs) are summoned to the scene of each reported death where there is no physician in attendance. If the EMTs make a determination that the victim has no vital signs in accordance with guidelines issued to them, they shall indicate this information on a report form and a copy of their report is to be given to the **investigator-in-charge**;
- Ensure that the reporting officer includes the names and Unit designation of the responding EMTs on the incident report;
- Ensure that if the **Medical Examiner** accepts jurisdiction of the body, the body not be removed, except at the direction of the **Medical Examiner**;
- Ensure that the scene remains protected until the investigation at the scene is completed; and
- Ensure that if the decedent was under the care of a physician, that an attempt was

made to contact the physician to find out the nature of the illness, and whether the physician will sign the death certificate.

#### **Sec. 10 RESPONSIBILITIES OF THE OPERATIONS DUTY SUPERVISOR**

**The Operations Duty Supervisor** shall be responsible to notify the following:

- District Duty Supervisor;
- Homicide Unit **(from on call list)**;
- District Attorney's Office **(from on call list)**;
- Medical Examiner's Office;
- Identification and Photography Unit; District Commander;
- Crime Lab **(if requested by the investigator-in-charge)**;
- Ballistics Unit **(if requested by the investigator-in-charge)**; and
- Any other Department resources as necessary **(as requested by the investigator-in charge)**.

#### **Sec. 11 ASSIGNMENT OF INVESTIGATIVE RESPONSIBILITIES**

The assignment of investigative responsibilities detailed below applies only to those homicides and sudden deaths occurring within the City of Boston where the Suffolk County District Attorney has designated the Boston Police Department Homicide Unit as the "law enforcement representative". The assignment of investigative responsibilities detailed below specifically does not apply to homicides or sudden deaths which occur in areas or locales wherein the Suffolk County District Attorney has designated the State Police, or any other agency, to be the "law enforcement representative."

**a) A Homicide Unit Investigative Team Supervisor** shall be designated as the **investigator-in charge** and has the responsibility for the investigation of all incidents involving any: ▪  
Homicide;

- Violent, suspicious or sudden death when the cause is unknown;
- Any suicide that occurred in a police facility, or by a person in police custody, or in a Suffolk County correctional facility (M.G.L. c. 40, § 36A and Rule 318);
- Unidentified dead bodies, irrespective of the cause of death;
- Aggravated battery where the victim is in critical condition and there is a likelihood that the victim will die; and
- Incident at the direction of the **District Attorney** or the **Medical Examiner** (e.g., physician-assisted suicides, etc.).

The **Homicide Unit Investigative Team** is responsible for the collection, processing and custody procedures for any evidence gathered. In those investigations conducted by the **Homicide Unit Investigative Team**, the Homicide Unit Commander is responsible for overseeing the follow-up investigation. In all homicide cases, the Area Detective Commander is responsible for the assignment of a District Detective to assist the **Homicide Unit Investigative Team** that will coordinate the investigative effort within their District.

- b) The District Detective **investigator-in-charge** as designated by the **Area Detective Commander** shall be responsible for investigations on their District involving:
- Accidental deaths, sudden deaths and suicides, except for those which are listed above and are assigned to the Homicide Unit; and
  - Other investigations, distinct from those ruled homicides, as directed by the **District Attorney or the Medical Examiner.**

The **District Detective** is responsible for the collection, processing and custody procedures for any evidence gathered. In those death investigations conducted by **District Detectives, the Area Detective Commander** is responsible for overseeing the follow-up investigation.

## **Sec. 12 RESPONSIBILITIES OF INVESTIGATOR-IN-CHARGE**

The **investigator-in-charge** shall ensure that the following steps are taken, **as applicable**:

- Record date, time, and by whom assigned to case;
- Confirm with the **Operations Division Duty Supervisor** that proper notifications are being made;
- Record arrival on crime scene and make note of those present;
- Evaluate the adequacy of the inner and outer perimeters and ensure the crime scene is protected;
- Ensure witnesses have been located and identified;
- Debrief the **Patrol Supervisor, the first officer(s) on the scene** and the **first responding officer(s)**;
- Record condition of crime scene in notes;
- Obtain name of next of kin and ensure that they are notified in-person, if possible. For out of state or out of jurisdiction notifications, arrange for the local police department to make an in-person notification;
- Arrange for identification of body;
- Interview witnesses and suspect(s) and obtain statements;
- Supply the **Medical Examiner** with any additional information that may have been obtained as a result of interviews;
- Search the crime scene (with warrant, if necessary);
- Photograph the crime scene. Use photographs and/or videotapes (eliminate any unnecessary background noise);
- Sketch the crime scene;
- Record the processing of the crime scene while collecting and preserving evidence;
- Collect relative hand-written documents, such as suicide notes, as evidence with the original to remain a part of the case file and copies to be provided to the **District Attorney and Medical Examiner**. Copies of suicide notes may be provided to family members or a relative after the investigation is completed and there has been a finding that the death is a suicide;
- Examine scene for any medication and forward to **Medical Examiner** (obtain signed

receipt for medication forwarded);

- Interview next of kin and/or close friends and obtain past medical history, name of doctor, and note any recent illness and/or hospitalization;
- Obtain a copy of the responding EMT's report;
- Compile a history of victim's mental health and physical condition for the **Medical Examiner** and include in the case report;
- Record condition and position of body, clothing worn, condition of hands, etc.;
- Record any trauma, rigor mortis, lividity, body temperature (by touch) and any other observable conditions of the body;
- Arrange for removal of body when processing is complete at the direction of the **Medical Examiner**;
- Consult with the **District Attorney** or their designee to determine when the crime scene may be vacated;
- Notify the **Operations Duty Supervisor** with instructions to vacate the crime scene; ▪ Prepare investigative reports;
- Review all other reports, statements and forms for completeness and accuracy; ▪ Conduct re-enactment, if deemed appropriate;
- Conduct line-ups or photo arrays when necessary, in cases which require victim or witness identification of a suspect;
- Review case with **District Attorney** or their designee; and
- Arrange for arrest warrant and/or search warrants and the formal charging of the suspect(s) with the approval of the Homicide Unit Commander (BPD), and the Chief of the Homicide Division of the District Attorney's Office, unless impractical.

### **Sec. 13 REMOVAL OF DEAD BODIES**

A dead body shall only be moved at the direction of the **Medical Examiner** or the **District Attorney** or their designee (M.G.L. c. 38, § 4). The **Medical Examiner** must be notified of the known facts concerning the time, place, manner, circumstances, and suspected cause concerning any person who has died. The **Medical Examiner** has the lawful right to take charge of the body (M.G.L. c. 38, § 4).

Once the **District Attorney** or their designee arrive at the scene or is notified of the discovery of the dead body, the **District Attorney** shall have authority to direct and control the criminal investigation of the death and removal of the body and coordinate the investigation with the police (M.G.L. c. 38, § 4).

Transportation of bodies of persons who have died from any disease dangerous to public health must be in accordance with the rules and regulations of the Department of Public Health (M.G.L. c. 111, § 107).

If a body is found in water, it may be moved to the nearest shelter. Prior to moving the body, the location and position shall be carefully recorded and if possible, marked and photographed.



If a body in a public place is moved, it should be placed on a stretcher in the exact position it is found. The area should be marked, the body outlined on the ground, and the location photographed. Particular attention must be given to the body's position and to blood or fluid secretions.

If the **Medical Examiner** declines jurisdiction but there is no known next of kin or relative of the deceased to make funeral arrangements, personnel from the **Medical Examiner's** office shall remove the body to the Office of the Chief **Medical Examiner**.

If the Medical Examiner declines jurisdiction and there are next of kin or relatives to make funeral arrangements, the District detectives SHALL be required to do the following: A. If the next of kin CAN be notified prior to the completion of the original 1. 1 incident report, the name of the deceased shall be recorded in Box #11, and the name of the next of kin will be recorded in the narrative section of the 1. 1 incident report. B. If the name of a next of kin can be determined, but CANNOT be notified before the original 1. 1 report is completed the deceased name shall not be recorded in box 411. The District detectives shall conduct a follow-up investigation and submit a supplementary report, recording the name of the deceased in Block 411, and the name of the next of kin in the narrative section of the report.

In **all** cases, officers shall remain on scene until such time as the body is removed, either by personnel from the **Medical Examiner's** office or by an undertaker.

#### **Sec. 14 BODIES REMOVED FROM FIRE SCENES**

The EMTs are responsible for examining the victim and making on-scene pronouncements. The **Medical Examiner's** office will be notified immediately and requested to respond.

Fire Department personnel will handle the removal of the victim(s) and placement into the Police Department wagon and from the wagon to the Office of the Chief **Medical Examiner**. All equipment necessary for the removal will be provided by Health and Hospitals or the Fire Department. **Police Department wagons will be used only to transport the victim to the mortuary and police personnel shall not handle the victim(s).**

#### **Sec. 15 VEHICLES REMOVED FROM CRIME SCENES**

Whenever possible all vehicles will be processed at the crime scene. If it becomes necessary to remove a vehicle prior to processing, evidence shall only be removed after being photographed and latent print processing has been completed.

Vehicles held as evidence or for processing **shall only be towed on a flatbed tow truck** and shall be towed for safekeeping to the station house of the District of occurrence or to a secured

location at the direction of the Homicide Unit Investigative Team Supervisor or, where appropriate, the District **investigator-in-charge**. The reporting officer ordering the tow is responsible for completing the tow slip receipt, the MN inventory (BPD Form 2012) and recording the tow on the original incident report. Such incident report shall include the name of any officer assigned to accompany a vehicle towed for evidence or for later processing.

The vehicle should be clearly marked as evidence and the District **Duty Supervisor** shall be notified as to the vehicle's whereabouts. **In order to maintain the chain of custody, officers assigned to accompany such vehicles shall stay with the vehicle until relieved.**

#### **Sec. 16 CRIME SCENE SEARCH GUIDELINES**

Officers should be alert to important details or evidence which are transient in nature and which may be subject to chemical changes or which may be moved. The officer must be crime scene conscious and attempt to assess and determine the entire area of the crime scene. **Crime scene processing must continue until complete.** It should be kept in mind that once a crime scene is abandoned, if only for a short period of time, it is often impossible to legally gain possession of the premises again.

a) Except for consent searches which have received the **prior** approval of both the Commander of the Homicide Unit and the Chief of the Homicide Division of the District Attorney's Office, a search warrant shall be obtained prior to searching a crime scene **in any case where individual property rights guaranteed by the Fourth Amendment to -the U.S. Constitution and/or Article 14 of the Massachusetts Declaration of Rights could be violated or infringed upon.**

b) The **Homicide Unit Investigative Team Supervisor** shall review the affidavit and submit the affidavit to an Assistant District Attorney from the Homicide Division of the District Attorney's office for approval.

c) **The Homicide Unit Investigative Team Supervisor** shall directly supervise the service and return of the warrant.

#### **Sec. 17 NON-CRIMINAL DEATH SCENE SEARCH GUIDELINES**

The primary role of any officer involved in a Death Investigation on scenes of accidental, suicide and sudden deaths is to establish the circumstances surrounding the death and to determine whether criminal misconduct took place.

If a preliminary investigation reveals with reasonable certainty that no criminal misconduct took place, it is only necessary to search those areas that directly relate to the circumstances and cause of death.

There will be no independent cursory searches of the decedent's property outside of what is discovered in plain view on or near the body of the decedent, unless the **Medical Examiner** orders a search. **This search shall be the responsibility of the Patrol Supervisor.** The search

shall be conducted in the presence of a police officer who shall record all items impounded.

#### **Sec. 18 IMPOUNDING PROPERTY PROCEDURES**

All bulk property shall be secured, locked and sealed with the crime scene.

Keys to premises occupied by the deceased shall be delivered to the **Medical Examiner** unless he authorizes them to be retained by the police. No police officer shall admit any person into premises of the deceased or surrender keys to such premises without the authorization of the **Medical Examiner** or his representative.

In all cases in which the **Medical Examiner** accepts jurisdiction of a dead body, the **Medical Examiner** is responsible for the property of the deceased person. The **Medical Examiner** shall, **unless such money or property is required as evidence**, deliver it to the person entitled to its custody or possession or, if not claimed within sixty (60) days, to a public administrator (M.G.L. c. 38, § 18).

In all cases in which the **Medical Examiner** declines jurisdiction of an unattended natural death, all personal property discovered on or near the body of the deceased shall be taken to the station house of the District of occurrence, inventoried and turned over to the Duty Supervisor. Upon receiving a receipt for such property from the next of kin, the Duty Supervisor shall release such property.

In either case, no property shall be released until it is inventoried, itemized, and recorded on a property receipt. The property receipt must be signed by the person accepting the property before the property may be released. This release shall be recorded on a supplementary incident report, including the identification of the person accepting the property.

A copy of the property receipt shall be attached to the original incident report and also to the District copy. The original property receipt shall be attached to the District Property Receipt Book. A copy shall also be delivered to the **Medical Examiner**.

#### **Sec. 19 ALL DEATH INVESTIGATION REPORTS**

Police officers are required to write reports for all deaths that occur in their jurisdiction **without a physician in attendance**. However, the **District Attorney** or the **Medical Examiner** may direct that a report be written and an investigation be conducted in cases involving a suspected physician-assisted suicide. The basic report requirements are the same for any such death, regardless of the age of the deceased (including infants and apparent still-borns), the apparent health or mental condition of the deceased prior to death and/or the possible cause of death.

**ALL DEATH REPORTS SHALL BE TYPED.**

The incident report also must indicate whether or not the **Medical Examiner** accepted jurisdiction of the body. When the name of the undertaker is available, it should also be recorded on the incident report.

Police officers shall not take it upon themselves to determine the cause of death, nor shall they put any such assumptions in their reports. The **Duty Supervisor** shall classify all such deaths as "death investigations" and shall ensure that those words are typed in the block on the incident report (1. 1) labeled "Type of Incident." Upon an investigation being classified or re-classified by the **Medical Examiner** as a homicide, or otherwise, the **investigator-in-charge** shall be responsible for submitting a supplementary incident report (1. 1) which shall include the **Medical Examiner's** finding.

Original incident reports shall include **only** the following information, with all other pertinent information included only on the Form 26 report:

- Describe the exact address and floor where the body was found;
- List the name and area of assignment of the officer who found the body; ▪ List the names and unit numbers of ALL persons responding to the crime scene, including, but not limited to: Police, Fire, Health and Hospitals, Medical Examiner's Office and the District Attorney's Office;
- List the time the EMTs determined the deceased person could not be resuscitated; ▪ In the event the victim is transported to a hospital, list the name of the attending physician and the time the victim was pronounced; and
- Include whether or not the **Medical Examiner** accepted jurisdiction of the body, where the body was taken and who removed it.

## **Sec. 20 INFORMATION NECESSARY FOR FORM 26 REPORTS**

**Form 26 reports shall be typed and shall be as detailed and complete as possible.** They shall include the following information, as applicable:

- Include the name of the victim, if known;
- Describe the exact place where the body was found (this should be specific as ▪ possible, giving, if necessary, both the address and the location within that address, such as: bathroom in Apt. 3 on the second floor, 123 Main Street);
- Describe the position of the body;
- Describe the clothing or any other covering on the body;
- Describe any visible injuries or discolorations on the body;
- List the names of all other persons present, and/or those who may have knowledge of the incident;
- List the name and area of assignment of the officer who found the body; ▪ List the names of the responding EMTs and their unit number;
- List the time of the EMT's determination that the deceased person could not be resuscitated;
- List the name of any physician who was recently caring for the deceased; ▪

List any known illnesses or diseases of the deceased;

- List any prescription medications found in the name of the deceased or known to be currently used by the deceased;
- List the name of the next of kin, include addresses, telephone numbers, etc.; ▪ Include the time of notification of family or friends of the death, or what efforts were made, or are being made, to make such notification;
- Include the identity of any member of the Clergy who was called; and ▪ Include where the body was taken and who removed it.

## **Sec. 21 INVESTIGATOR-IN-CHARGE REPORTS IN DEATH INVESTIGATIONS**

**Investigator-in-charge** Investigative Reports (Form 26) in Death Investigations will describe the investigation in the following sequence and format, as applicable: ▪

Give a narrative summary;

- Describe in detail, who, what, where, when, why and how;
- When witnesses are interviewed or statements taken, they shall be listed numerically, (i.e. 1,2,3,). Include a short paragraph summarizing the statement given. Statements of witnesses and subjects must contain sufficient personal history and data so that they may be located in the future;
- If an area canvass is conducted, all persons interviewed and/or addresses visited must be listed. State time, identifying persons name, address, telephone number, and what information was obtained. If no one was at home at address, state no contact was made and give time. All reports must be signed by officer preparing report;
- Briefly describe the scene of the crime and body position, condition, clothing, trauma, disposition of body, etc.;
- List personal data on the victim/subject of the investigation;
- List any medical history of the victim/subject;
- List any past history of the victim/subject;
- List the name(s) of the next of kin, include addresses, telephone numbers, etc.; ▪ List all property secured and its location;
- List any vehicle(s) and location, including tow receipt numbers, if applicable; and ▪ List any additional information.

## **Sec. 22 FILING FOR INQUEST AND/OR CRIMINAL CHARGES**

**The Homicide Unit Investigative Team Supervisor** shall consult with an Assistant District Attorney from the Homicide Division of the District Attorney's Office outlining all evidence and probable cause to support charges prior to the filing of any criminal charges. If a suspect has been arrested on any criminal charge, criminal charges are considered filed when the application for complaint has been properly completed and filed with the court. The **District Attorney** or their designee shall determine the cases in which a direct indictment will be sought.

The **Homicide Unit Investigative Team Supervisor** investigating an unidentified dead body is

responsible for ensuring that all pertinent information is completely and accurately entered into the National Crime Information Center (NCIC) Unidentified Person File in a timely manner.

Any warrants for the arrest of a suspect will be sought from a Judge, Grand Jury or Clerk Magistrate subsequent to the review and approval of the **District Attorney** or their designee. Upon issuance of an arrest warrant or indictment warrant, the **Homicide Unit Investigative Team Supervisor** assigned to investigate the case is responsible for ensuring that all computer entries are complete and accurately entered. Discrepancies noted in any of the information entered into the Warrant Management System shall immediately be brought to the attention of the Clerk of Court for the court of issue so they may be corrected.

If there is reason to believe a suspect has fled from the jurisdiction, an Unlawful Flight to Avoid Prosecution (UFAP) federal warrant will only be sought if deemed appropriate by the **District Attorney** or their designee.

The **District Attorney** will determine when it is appropriate to institute procedures for an inquest before a justice of the court of jurisdiction ([M.G.L. c. 38, § 8](#)).

Paul F. Evans  
Police Commissioner



### **OFFICE OF MEDIA RELATIONS - RELEASE OF OFFICIAL INFORMATION**

This rule is issued to establish the policy of the Police Department with regard to releasing official public information to members of the news organizations or to other persons outside the department. The rule clearly recognizes the rights of news media personnel to obtain information and photographs at the scene of emergencies or other police activities. Its provisions are effective immediately, superseding all previously issued Rules, Orders, Bulletins, Memoranda and directives regarding communication with the news organizations or release of official information.

**Sec. 1 GENERAL CONSIDERATIONS:** The relationship between the police and the news organizations in a democratic society is based upon complementary rather than conflicting interests. News organizations have a legitimate need for information about public safety activities and provide a wide reaching opportunity to inform the public about matters involving crime, quality of life and public safety.

Crime, and police efforts to prevent it, is a matter of public concern. The Boston Police Department is regularly involved in events about which members of the news media legitimately need information or photographs. Under such circumstances, the members of the Department, both sworn and civilian, have three responsibilities: 1) to bring the police operation at hand to a successful conclusion, 2) to protect the constitutional rights of accused persons, and 3) to cooperate with media efforts to obtain and disseminate factual timely information.

The Boston Police Department actively seeks to establish a cooperative climate in which information involving matters of public interest may be obtained in a manner that does not hamper police operations or abridge the rights of the accused.

**Sec. 2 THE OFFICE OF MEDIA RELATIONS (OMR):** The Office of Media Relations is the central source of information for release by the Department and responds to requests for information by the news media and the community. Members of OMR provide information and updates to the media at major incident scenes, prepares and distributes news releases, coordinates and assists at news conferences, coordinates and authorizes the release of information about victims, witnesses and suspects, assists in crisis situations within the agency and coordinates the release of authorized information.

Members of the OMR also update the Department's blog ([www.BPDNews.com](http://www.BPDNews.com)); and are responsible for posting messages on the Department's Official Social Media sites. The Office of Media Relations is open seven days a week from 8:00 a.m. to 11:00 p.m.

**Sec 3 PUBLIC RECORDS:** Members of the Department should understand the provisions of M.G.L. c. 4 § 7 and M.G.L. c. 66 § 10. These sections define public records. These statutes give the public access, including the right to inspect and copy, all records made or received by any public agency except those exempted from disclosure by other statutes. Included among those documents that the public has a right to inspect and copy is BPD Form 1.1, Incident Reports, except those portions of the report that fall within one of the following enumerated exemption clauses:

- ☐ **CORI Records:** Except for information that is released contemporaneous with an arrest, specifically exempted from disclosure are all records that come under the Criminal Offenders Record Information law (CORI) which prohibits disclosure of any information about an arrest including the summaries of criminal records or probation records whether obtained from Boston Police files or by Boston Police from other agencies.
- ☐ **Victim and Juvenile Identities:** Prohibited by law is the disclosure of the names of victims in sexual assault cases, as well as details of sexual assaults. Prohibited by Departmental policy is the disclosure of the names of juveniles. (Juveniles are considered those persons less than 18 years of age.)
- ☐ **Investigative Information:** The Public Record Law also provides that "investigative materials necessarily compiled out of the public view by law enforcement or other investigative officials, the disclosure of which would probably so prejudice the possibility of effective law enforcement that it would not be in the public interest," are exempt from public disclosure. **It is the policy of the Department to release such information to news media personnel, contemporaneous with an incident and consistent with sections 3 and 4 of this Rule, if such release does not interfere with police investigations.** The Police Commissioner will make final decisions on release of such information after consultation with the Legal Advisor.

**Sec. 4 INFORMATION THAT DEPARTMENT MEMBERS MAY NOT RELEASE:**

- ☐ The existence or contents of a prior criminal record of the accused (C.O.R.I.). Character or reputation of the accused.
- ☐ Existence or contents of any confession or statement of the accused. The accused person's participation in, or refusal to submit to, any examination or test and/or the results thereof.
- ☐ Possibility of a guilty plea.
- ☐ Opinions as to the guilt or innocence of the suspect.
- ☐ Opinions as to the quality of the evidence of the case.
- ☐ Identity of known witnesses or possible witnesses.
- ☐ Statements or testimony of witnesses except as part of the record of a public court proceeding.



- ☐ Police pictures of persons arrested, or pictures that have been made a part of a criminal record (unless published to aid in the capture of a wanted suspect; or authorized by an appropriate bureau chief or his/her designee).
- ☐ Names or addresses of rape or attempted rape victims and any details of sexual assaults, or attempts to commit such offenses.
- ☐ Information contained in an officer's Internal Affairs file; exceptions are noted in Section 5.
- ☐ Photographs of police personnel, **unless** permission is given by the individual involved, the individual's immediate family, or in special cases, the Police Commissioner.
- ☐ Specific addresses (other than home towns), family data, or other personal data regarding police personnel, **unless** the person involved gives permission (information that can be released is noted in Section 5).

**Sec. 5 INFORMATION THAT DEPARTMENT MEMBERS MAY RELEASE CONTEMPORANEOUS WITH AN INCIDENT OR WITH THE APPROVAL OF THE OMR:**

- ☐ Nature of charges.
- ☐ Basic facts and circumstances of an arrest.
- ☐ Identity of investigating and arresting officers.
- ☐ Length of the investigation leading to the arrest.
- ☐ Description of physical evidence seized unless release of such information would unduly jeopardize a case.
- ☐ Identity of the arrestee, if 18 years of age or older.
- ☐ The age, sex, and hometown (but not the name) of the accused if under 18 years of age.
- ☐ Schedule of and/or results from any stages of the judicial process (including quotations from public records of the court).
- ☐ An officer's age, date of appointment, hometown, and date of retirement or resignation, awards or commendations.
- ☐ Any criminal charges pending against an officer.
- ☐ Results of a completed IAD investigation, only with the approval of the Superintendent of BII or the Police Commissioner.
- ☐ Nature of charges against an officer in an on-going IAD investigation. Identities of persons killed; only after obtaining confirmation that the next-of kin have been properly notified.

**Sec. 5.1 DISPLAYS OF EVIDENCE:** The Department will on occasion display drugs, weapons, and other evidence seized at crime scenes or during arrests. Evidence including: drugs, drug paraphernalia, weapons, money and other items may be displayed at news conferences and allowed to be photographed only after clearance by the OMR.

**Sec. 6 PHOTOGRAPHING PRISONERS:** News organizations have the right to photograph persons in police custody. However, officers will not pose prisoners for news photographs nor will they allow prisoners to be photographed by media outlets inside

police buildings.

**Sec. 7 ACCESS OF NEWS MEDIA PERSONNEL:** A newsperson's primary responsibility is to report the news by gathering information and/or taking photographs. Since the opportunity to do so is often of a momentary or transitory nature, especially at an emergency scene, an officer should not obstruct a newsperson in the performance of his or her duties. **However, to preserve the integrity of a crime scene while evidence is being collected; members of news organizations will not be permitted within 50 feet of an active crime scene.**

Newspersons may photograph or report anything they observe at an emergency scene. When publication or broadcast of such coverage could interfere with an investigation or place a victim, suspect, witness or other person in jeopardy, withholding publication is dependent upon the willingness of the news organization. In the event of a conflict with news organization members, officers shall immediately advise a supervisor to notify the OMR. Officers shall not, however, interfere with or obstruct news media personnel as long as their activities remain within the confines of the law. Any violations of this procedure should be immediately reported to the OMR. On public streets, news photographers and their equipment have the right to be free from assaults and unnecessary interference or obstruction while engaged in the lawful performance of their duties at the scene of a crime or other major event. Members of the news media are not exempt from any municipal, state or federal statute.

**Sec. 8 NEWS MEDIA ACCESS AND CROWD CONTROL:** In order to ensure public safety and to prevent citizens from entering a restricted area, police personnel will establish police lines where necessary at all major events. It is the policy of the Department to allow duly accredited representatives of any news service, newspaper, television, or radio station to enter areas normally closed to the public by police lines. **ALLOWING NEWSPERSONS INTO SUCH AREAS IS, HOWEVER, DEPENDENT UPON THE TACTICAL SITUATION AND THE LIKELIHOOD THAT THE SUCCESS OF THE POLICE RESPONSE WILL NOT BE JEOPARDIZED. IN CERTAIN SITUATIONS, THERE MAY BE A SEPARATE AREA SET ASIDE FOR NEWS MEDIA REPRESENTATIVES TO ALLOW THEM TO COVER AN EVENT.**

The decision to assume the risk of danger remains with the individual newsperson involved and it is not the responsibility of the police to provide for the safety of those members of the news media who voluntarily choose to subject themselves to danger. It is the responsibility of department personnel assigned at events where police lines are established to ensure that only news media members **WITH THE APPROVED IDENTIFICATION** are allowed to cross police lines or enter areas set aside for the news media. **THIS WILL REQUIRE CHECKING NEWS MEDIA MEMBERS FOR APPROVED NEWS MEDIA CREDENTIALS AND REQUIRING THEM TO WEAR THESE CREDENTIALS ON THEIR OUTERMOST GARMENT.**

Officers shall direct questions relative to credentials to the ranking supervisor at the scene or an OMR representative. It is the responsibility of all news media personnel to clearly

Page 4 of 7

display their media credentials at emergency scenes or special events. Failure to do so can cause the police to request that person to leave the restricted area immediately.

**Sec. 8.1 RULE 200 ADDENDUM A – HOSTAGE AND BARRICADED SUSPECT SITUATIONS:** In order to bring hostage and barricaded suspect situations to a successful conclusion, protect the constitutional rights of accused persons and cooperate with media efforts to obtain and disseminate factual information, the media and the department must adhere to established procedures. In any hostage or barricaded situation the media will:

- ☐ Collectively designate a ground level pool camera and one pool helicopter camera for shared coverage. The Department's Chief Hostage Negotiator reserves the right to exclude aerial coverage if he/she deems it hazardous to the situation;
- ☐ Refrain from airing critical ground or aerial videotape until the situation has been resolved;
- ☐ Refrain from interfering with the negotiation process. This includes contacting, by any means, suspects or other persons involved in the situation without the guidance of the Chief Hostage Negotiator.

In any hostage or barricaded situation the Department may, under the direction of the Chief Hostage Negotiator:

- ☐ Provide the ground level camera man, accompanied at all times by an officer from OMR, a location within the inner perimeter;
- ☐ Provide frequent informational reports during the incident, as well as access to critical personnel after the incident;
- ☐ Provide a media station in the outer perimeter of the incident where reporters can obtain information safely during the incident without interfering in the tactical operations. Provided information shall include live remote stand-ups, interviews and informational updates without including deployment information or video footage concerning tactical operations.

**Sec. 9 OMR NOTIFICATION:** Officers shall direct all requests for information and interviews to the OMR. Duty Supervisors, on-scene Supervisors, and Supervisors assigned to the Operations Division shall make every effort to get pertinent information on any unusual (newsworthy) incident/arrest to OMR as soon as possible. This will allow the OMR to disseminate the facts to the media in a timely manner while removing this obligation from other Districts/Units, which are receiving similar requests.

In addition, an OMR representative is always on call. Officers shall contact the on-call Media Relations Officer through the Operations Division for major incidents occurring during hours when the Office is closed. The highest-ranking Superior Officer on scene shall make a determination as to whether or not an incident is classified as major.

The following types of incidents require notification of the Office of Media Relations by the Operations Division:

- ☐ An incident involving a potential Civil Rights Law violation. Information shall be released only with the approval of the Superintendent of the Bureau of Investigative Services or his/ her designee.
- ☐ An on-going trial or upcoming court case, Department policy, hiring practices, deployment of personnel, internal investigations of Department personnel or **any legal matter or potential legal matter**. Information shall be released only after clearance by the OMR in consultation with the Legal Advisor, when applicable.
- ☐ Homicide or serious shooting or stabbing.
- ☐ Homicide with multiple victims.
- ☐ Suicide in a district cell.
- ☐ Multiple deaths (motor vehicle accident, fire, etc.).
- ☐ Police officer shot.
- ☐ Police officer seriously injured.
- ☐ Police officer involved in a shooting.
- ☐ Police officer involved in a serious IAD incident.

**Sec. 10 RELEASE OF ROUTINE INFORMATION:** When OMR is closed, and the incident is of a routine nature, such as a Part One Crime (except a Sexual Assault), the basic information, except for information outlined in Sections 3 and 4, may be given to members of the media by the Duty Supervisor or Senior Officer of the Operations Division. Any information given to the media from the Duty Supervisor or Senior Officer of the Operations Division must be forwarded to OMR.

If necessary on routine police matters in order to answer a legitimate request for information that may be released, the Operations Duty Supervisor will call the Unit or District involved, obtain the information and call the news media back. In all cases OMR should be notified as soon as possible.

**Sec. 11 REQUESTS FOR INTERVIEWS:** The news media and members of the public frequently direct inquiries to the Department seeking interviews on a variety of general police subjects or to request a departmental member as a guest. The decision to release such information or to grant interviews will be made, according to the facts of each situation, by the OMR. This does not apply to requests for routine information discussed above in Section 10. If you are uncertain whether information requested by the media constitutes a "Request for Interview," check with the OMR.

Only Command Staff members are authorized to speak on behalf of the Department. The Director of Media Relations or other Command Staff members may provide information of a

factual nature to the media at a crime scene, as governed by this policy. If a Command Staff member speaks on camera or releases information to a newsperson, he/she must alert as soon as possible, the OMR, as to the content of the information given. **Only ONE member of the Department's Command Staff is authorized to speak at any one event or crime scene.** Any investigative information released must be vetted by the Chief of the Bureau of Investigative Services or his/her designee.

**Sec. 12 TOURS OF POLICE FACILITIES:** Requests for tours of police facilities should be directed to the OMR for approval and assignment based upon the tactical and operational needs of the Department.

**Sec. 13 ENDORSEMENT OF COMMERCIAL PRODUCTS:** The Department does not endorse commercial products or allow its facilities to be used for such endorsements. Department personnel shall not make any endorsements of commercial products in their capacity as members of the Department without specific permission from the Police Commissioner.

**Sec. 14 PARTICIPATION IN MOVIES, COMMERCIALS, ETC.:** All requests for the use of Boston Police Department personnel and/or equipment in movies, documentaries, docudramas, commercials, advertisements, television shows, or similar projects must be cleared through the Director of Media Relations with approval from the Police Commissioner.

The Department will not normally grant permission for its equipment or police facilities to be used for television, motion pictures, or other similar productions. However, representatives from the news media may be allowed to operate their cameras and recording equipment **inside** police facilities only after authorization is given by the Director of OMR.

News media representatives have the right to be present outside police facilities at any time as long as they are not interfering with officers performing their duties.

William B. Evans  
Police Commissioner



**Police Commissioner's Special Order**

Number: SO 21- 18

Date: May 19, 2021

Post/Mention: Indefinite

**SUBJECT: RULE 303 Use of Deadly Force**

Rule 303, Use of Deadly Force, is hereby amended superseding all previous rules, special orders, memos and directives on this subject and is effective immediately.

Changes have been made to:

**Statement on Use of Force**

**Sections 1, 2, 5, 6, 7, 8, 10, 11, 12.**

Commanding Officers shall ensure that this order and the attached Rule are posted on Department bulletin boards.

Gregory P. Long  
Superintendent In Chief

**Boston Police Department**

**Rules & Procedures**

**Rule 303**

**May 19, 2021**

**USE OF DEADLY FORCE**

Statement on Use of Force:

The Boston Police Department is committed to de-escalating incidents to negate the need for the use of force. When force is necessary the Boston Police Department is committed to using only the amount of force that is reasonably necessary to overcome the resistance offered. The Boston Police Department is equally committed to preventing unnecessary force, ensuring accountability and transparency, and building trust with our community. The Boston Police Department respects the inherent life, liberty, dignity, and worth of all individuals by preserving human life, and minimizing physical harm and the reliance on use of force.

**Pursuant to *An Act Relative to Justice, Equity and Accountability in Law Enforcement in the Commonwealth (Chapter 253 of the Acts of 2020) Section 30 (14) (a,b,c):***

a. “A law enforcement officer shall not use physical force upon another person unless de escalation tactics have been attempted and failed or are not feasible based on the totality of the circumstances and such force is necessary to:

- Effect the lawful arrest or detention of a person;
- Prevent the escape from custody of a person; or
- Prevent imminent harm and the amount of force used is proportionate to the threat of imminent harm:
  - Provided, however, that a law enforcement officer may use necessary, proportionate and non-deadly force in accordance with the regulations promulgated jointly by the POST Commission and the municipal police training committee *(and taught at the Boston Police Academy)*.

b. A law enforcement officer shall not use deadly force upon a person unless de-escalation tactics have been attempted and failed or are not feasible based on the totality of the circumstances and such force is necessary to prevent imminent harm to a person and the amount of force used is proportionate to the threat of imminent harm.

c. A law enforcement officer shall not use a chokehold. A law enforcement officer shall not be trained to use a lateral vascular neck restraint, carotid restraint or other action that involves the placement of any part of law enforcement officer’s body on or around a person’s neck in a manner that limits the person’s breathing or blood flow.”

The Boston Police Department is committed to de-escalation tactics pursuant to **MGL Chapter 6E Section 1:**

**“De-escalation tactics”**, proactive actions and approaches used by an officer to stabilize a law enforcement situation so that more time, options and resources are available to gain a person’s voluntary compliance and to reduce or eliminate the need to use force including, but not limited to, verbal persuasion, warnings, slowing down the pace of an incident, waiting out a person, creating distance between the officer and a threat and requesting additional resources to resolve the incident, including, but not limited to, calling in medical or licensed mental health professionals, as defined in subsection (a) of section 51½ of chapter 111, to address a potential medical or mental health crisis.

When tactically safe and feasible, officers should give verbal warnings or commands when deadly force is going to be used. In some cases there may not be an opportunity to give verbal warnings or commands.

Duty to Intervene:

1. Police officers are reminded of Rule 113 Public Integrity Policy, Sec. 5 Canon of Ethics, Number Nine; and
2. **An Act Relative to Justice, Equity and Accountability in Law Enforcement in the Commonwealth (Chapter 253 of the Acts of 2020) Section 30 (15) (a,b):**
  - a. “An officer present and observing another officer using physical force, including deadly force, beyond that which is necessary or objectively reasonable based on the totality of circumstances, shall intervene to prevent the use of unreasonable force unless intervening would result in imminent harm to the officer or another identifiable individual.
  - b. An officer who observes another officer using physical force, including deadly force, beyond that which is necessary or objectively reasonable based on the totality of the circumstances shall report the incident to an appropriate supervisor as soon as reasonably possible but not later than the end of the officer’s shift. The officer shall prepare a detailed written statement describing the incident consistent with uniform protocols. The officer’s written statement shall be included in the supervisor’s report.”

## INTRODUCTION

This rule is issued to provide guidelines and regulations governing the use of deadly force by members of the Department, to ensure the safety of our police officers and the public, and to establish procedures for the orderly investigation of firearm discharges. Its provisions are effective immediately, superseding all previously issued rules, regulations, orders, bulletins and directives regarding the use of deadly force by Boston police officers.

In the establishing of these regulations it is understood that they will not likely cover every conceivable situation which may arise. In such situations officers are expected to act with intelligence and sound judgment, attending to the spirit of the rule. Any deviations from the



provisions of Sections 5, 6, 7, or 8 of this rule shall be examined on a case by case basis.

**Note:** Weapons and ammunition coming into the custody of Police Department personnel shall be handled in accordance with the provisions of Rule No. 311, Procedures for the Firearms Analysis Unit.

**Sec. 1 Definitions:** For the purpose of this rule, the following definitions will apply:

Deadly Force is that degree of force likely to result in death or great bodily injury. The discharge of a firearm toward a person constitutes the use of deadly force even if there is no express intent to cause great bodily injury or death.

Great bodily injury means bodily injury which creates a substantial risk of death or which is likely to cause serious injury, permanent disfigurement or loss, or extended impairment of the function of any bodily member or organ.

Immediate danger of death or great bodily injury includes circumstances under which (1) such a danger exists in reality, or (2) such a danger is apparent, and the officer is unable to affirm or disaffirm its actual existence.

Prudence means using cautious, discreet or shrewd action and having due regard for the rights of citizens while maintaining an awareness of the responsibilities of acting as a police officer. Reasonableness is moderate and/or fair action within reason, suitable to the confrontation.

The Investigating Officer in Charge (IOIC) is the Detective Superior Officer of the Firearm Discharge Investigation Team so designated by the FDIT Incident Coordinator and assigned to investigate the facts of the incident and to determine if the use of deadly force was justifiable.

**Sec. 2 General Considerations:** The primary purpose for which a sworn member of the Department is issued a firearm and trained in its use is the protection of life and limb, both theirs and that of every other person needing such protection. Although the firearm is a necessary weapon for present-day policing, it's potential to inflict death or great bodily injury mandates that it be used within clearly-defined limits. This rule establishes those limits.

In the interests of personal safety, police officers must seek to gain and maintain a tactical advantage over persons known or suspected to be armed. Officers seeking to maintain the advantage over a subject suspected of being armed are in a difficult position; they must be prepared to use a firearm should it be necessary, yet show the restraint required to ensure the propriety of their actions.

The situation demands the utmost ability to think clearly, quickly and decisively and to use the firearm in a safe and effective manner.

The Boston Police Department recognizes its legal duty to protect the rights of all individuals to due process of law and a fair trial. Its members are thereby bound to refrain from any use of force that unnecessarily tends to administer punishment at the hands of a police officer.

The responsibility for punishment of criminal offenders rests solely with duly constituted courts of law and penal institutions and is by no means extended to the police.

**Sec. 3 Training and Qualification:** Police officers in this Department will be held accountable for proficiency as well as compliance with Department policy in the use of firearms. All sworn members of the Department are responsible for maintaining a degree of expertise in the use and handling of all firearms approved for their carrying. Specifically, sworn members authorized to carry a firearm shall qualify with their issued firearm(s) on a course of instruction approved by the Massachusetts Criminal Justice Training Council at least twice each year – once during the period from January 1st – June 30th and once during the period from July 1st – December 31st. A qualifying score of 80% or higher is required. When members of the Department are issued a new weapon, they shall qualify at the Department range in the use of that weapon prior to resuming street duties. This shall not apply to the emergency use of a comparable spare weapon issued on a temporary basis.

In the event an officer fails to qualify, the officer will be temporarily re-assigned to the Department Range. It will be the responsibility of the Commanding Officer of the Department Range to ensure that the officer's firearm is taken from them until such qualification is achieved. Any officer who, after such intensive training as determined by the Commanding Officer of the Department Range, has still failed to qualify will be subject to reevaluation as to their fitness to continue to perform the duties of a police officer. Under no conditions shall an officer who fails to qualify be allowed to perform any street police duties. Frequently, officers have activated themselves during off-duty situations where there is a need to draw a personal firearm and the possibility exists to use such weapon. On self activation, the officer's actions are guided by all Departmental rules and regulations, hence there is a need to show familiarization with any personal weapon which is carried while off-duty.

Members of the Department who are licensed to carry firearms pursuant to M.G.L. c. 140, § 131 and who own and carry a personal firearm while off-duty shall fire a familiarization course as designed by the Commanding Officer of the Department Range. This course will be fired during regular qualification times and police officers shall provide their own ammunition.

Officers complying with this portion of the rule will notify their Commanding Officer of their intent to do so and shall be authorized to carry more than one weapon while on duty for the sole purpose of attending the familiarization course at the Department Range.

This authorization shall be temporary and will only allow the officer to carry the off-duty weapon to and from the range. The off-duty weapon shall be secured in the District gun locker prior and subsequent to completion of the familiarization course.

**Sec. 4 Security and Maintenance of Department Firearms:** Members of the force shall take all reasonable precautions to ensure that weapons issued to them by the Department are protected from loss, misuse or theft.

Members are responsible for keeping their issued weapons clean and in good working order. A

weapon which malfunctions shall be returned to the Boston Police Range forthwith.

**Sec. 5 Pointing Firearms:** Officers shall only point a firearm at a person when reasonably justified under the totality of the circumstances. While officers should not point a weapon unless they are prepared to use it, the fact that they have done so must not be interpreted as an obligation to fire.

**Sec. 6 Discharge of Firearms:** The law permits police officers to use reasonable force in the performance of their duties but only to the degree required to overcome unlawful resistance.

**Boston Police officers are instructed, when tactically safe and feasible, to exhaust all alternatives before using deadly force. This includes de-escalation and verbal commands.**

This doctrine of “reasonable use of force” applies to the use of firearms as well as to non lethal force. Also, because of their destructive potential, the use of firearms must be further restricted to the purpose for which they are issued, that of protecting life and limb. The discharge of a firearm by a member of the Department is permissible only when:

A. There is no less drastic means available to defend oneself or another from an attack or imminent attack which an officer has reasonable cause to believe could result in death or great bodily injury, or

B. There is no less drastic means available to apprehend a fleeing suspect when the officer has probable cause to believe that: (1) the suspect has committed a felony during the commission of which they inflicted or threatened to inflict deadly force upon the victim, or (2) that there is substantial risk that the suspect in question will cause death or great bodily injury if their apprehension is delayed, or

C. There is no less drastic means available to kill a dangerous animal or one so badly injured that humanity requires its removal from further suffering.

Officers who find it necessary, under the provisions of this rule, to discharge firearms shall exercise due care for the safety of persons and property in the area and shall fire only when reasonably certain that there is no substantial risk to bystanders.

**Sec. 7 Warning Shots and Signals:** Firearms shall not be used as a signaling device. A firearm shall not be used to summon assistance or to give signals or to warn a fleeing suspect to stop. This does not mean that officers may not discharge their firearm without the intent to cause death or disable if in their best judgment there is no alternate method of convincing a would-be attacker that they are ready and able to defend themselves or others if the potential threat is not discontinued.

**Sec. 8 Moving/Fleeing Vehicles:** Firearms shall not be discharged from a moving vehicle.

Pursuant to **An Act Relative to Justice, Equity and Accountability in Law Enforcement in the Commonwealth (Chapter 253 of the Acts of 2020) Section 30 (14) (d):**

“A law enforcement officer shall not discharge any firearm into or at a fleeing motor vehicle

unless, based on the totality of the circumstances, such discharge is necessary to prevent imminent harm to a person and the discharge is proportionate to the threat of imminent harm to a person.”

**Sec. 9 Permissible Weapons, Magazines and Ammunition:** Officers shall carry on duty only weapons, magazines and ammunition authorized and issued by the Department. Officers must carry all weapons with a fully loaded magazine, in addition to having one round in the chamber.

Officers shall keep spare magazines fully loaded. Approved Department weapons, and their respective magazine capacities, include, but are not limited to:

- Glock Model 22 – 15 Rounds
- Glock Model 23 – 13 Rounds
- Glock Model 27 – 9 Rounds with flat floorplate, 10 rounds with extended floorplate ▪ Glock Model 43 - 6 rounds with flat floorplate, 8 rounds with extended floor plate (for use only by personnel in an investigative capacity).
- Sig Sauer P320RX 9mm Pistol with Optional Sig Romeo 1 PRO Red Dot, one 17 and two 21 round magazines
- Sigarms .45 Caliber Pistol – 8 Rounds – Officers shall carry this weapon with the manual safety engaged at all times, except just prior to discharge, or if necessary to disengage the safety to facilitate the loading and unloading process.

The Department may selectively issue other weapons to qualified personnel, if they are deemed necessary to ensure the safety and effectiveness of police operations. Officers armed with such weapons shall use those weapons in accordance with the provisions of this rule as well as any additional guidelines given at the time of issuance.

No police officer shall accept a Department issued weapon unless he/she has qualified in its proper use. No Superior Officer shall issue a Department weapon to any other officer without first asking if the officer is qualified in its use.

A Department armorer or a Department approved armorer, at the discretion of the Commanding Officer of the Boston Police Range, are the only persons allowed to perform all repairs or modifications to Department issued firearms, magazines or other weapons.

**Sec. 10 Reporting Firearms Discharges:** All firearm discharges, except discharges which occur during Department authorized or approved firearms training, while lawfully engaged in target practice or while hunting (unless a discharge occurring during one of these three exceptions results in death, personal injury or property damage), require the submission of an incident report (1.1) which includes information relative to injuries and damage to property. ▪ An officer who discharges his firearm during the course of his duties shall immediately notify the Operations Division that they have been involved in a “Code 303” and request that a Patrol Supervisor respond to the scene. The officer shall make a verbal report of the discharge to the responding Patrol Supervisor. In the event that someone has been injured, officers will request medical assistance. The supervisor shall request that Operations make all appropriate

notifications including the Firearm Discharge Investigation Team.

- An off-duty officer discharging a firearm in the City of Boston shall immediately notify an Operations Division Supervisor. The Operations Division shall notify the Officer in Charge of the District in which the discharge took place and the Firearm Discharge Investigation Team. The officer involved in the firearm discharge shall submit the necessary reports without delay to a Superior Officer assigned to the Firearm Discharge Investigation Team.
- An officer who discharges a weapon outside of the City of Boston shall immediately notify and make a report of the discharge to the Police Department which has jurisdiction where the discharge occurred, identify themselves as being a Boston police officer and notify an Operations Division Supervisor as soon as possible. The Operations Division shall immediately notify the officer's Commanding Officer and the Firearm Discharge Investigation Team.

Officers who have discharged a firearm shall complete a BPD Form 2415 (Firearms Discharge Report) in its entirety.

**Sec. 11 Investigation of Firearm Discharges:** The manner in which police officers use firearms is an extremely critical issue to the Department, one in which the community and the courts allow little margin for error. To ensure that proper control in this area is maintained, all reported discharges of firearms by officers of this Department will be thoroughly investigated by the Firearm Discharge Investigation Team.

The Firearm Discharge Investigation Team has sole responsibility for investigating firearm discharges involving a member of the Department. Failure to cooperate with the investigation shall be grounds for disciplinary action. The foregoing does not prevent an officer from exercising their constitutionally protected rights to remain silent or to speak with legal counsel.

The District Commander of the District wherein a police officer discharges a firearm shall be responsible for assigning a Superior Officer to assist the Firearm Discharge Investigation Team in their investigation into the discharge.

In those incidents where the use of deadly force results in death, the District Attorney's Office, pursuant to the terms of M.G.L. c. 38, § 4, will assume control of the investigation. The statute reads, in part, "The District Attorney or his law enforcement representative shall direct and control the investigation of the death and shall coordinate the investigation with the office of the chief medical examiner and the police department within whose jurisdiction the death occurred."

In all instances where a Boston police officer discharges a firearm resulting in injury, the District Attorney's Office will be notified and his or her designees from the Boston Police Department will conduct an independent investigation to determine the facts of the case.

**Patrol Supervisor:**

- Shall respond immediately to a reported use of deadly force, Code 303, within his District and

assume command of the investigation pending the arrival the District Commander and/or the Firearm Discharge Investigation Team.

- Shall notify the Operations Division of the firearm discharge. In turn, the Operations Division shall be responsible for making all necessary notifications.
- Shall initiate such preliminary steps as are necessary to conduct a thorough investigation and hold himself in readiness to assist the District Commander and the Firearm Discharge Investigation Team upon their arrival. In this respect, the Patrol Supervisor shall have the authority to order as many units to the scene of the firearms discharge as is deemed necessary or to take any other appropriate action to complete the task.
- Shall establish an outside perimeter around the area of the incident. • Shall ensure that the scene is preserved pending the arrival of the Firearm Discharge Investigation Team in a manner pursuant to Rule 309, Procedures for Handling Physical Evidence and Other Property Coming into Police Custody.
- Shall take possession of the firearm which has been discharged and ensure that it is turned over to a designated FDIT investigator as soon as possible. In so doing, the Patrol Supervisor shall preserve all firearms in the condition in which they are found. The Patrol Supervisor must use extraordinary care in this respect as the firearm may still be loaded.
- In the event that more than one officer is present at a shooting incident, the Patrol Supervisor, as soon as circumstances allow, shall collect all firearms which belong to the officers who were at the scene and store them until a designated FDIT investigator can ascertain which have been fired.

Firearms determined not to have been discharged, by a Department Ballistician, will then be returned to the police officers to whom they were issued as soon as possible.

Pursuant to Rule 405 Body Worn Camera, Sec 6.3 Collecting and Securing BWC Footage Following an Officer Involved Death, Officer Involved Shooting, or Other Use of Deadly Force (Rule 205 and/or Rule 303 Investigations):

- In accordance with Rule 205 and Rule 303, the Patrol Supervisor shall respond immediately to a death investigation or reported use of deadly force within his/her District.
- The Patrol Supervisor, as soon as circumstances allow, shall collect all BWC equipment, including department-issued mobile devices, which belong to the officers who: (1) were involved in the incident, (2) discharged their weapon, and/or (3) witnessed during the time of the officer involved death, officer involved shooting or other use of deadly force, and store the equipment in a secure compartment of his/her vehicle until the Homicide Unit or FDIT personnel arrives on scene. Once on scene, the Homicide Unit or FDIT personnel shall secure any remaining BWC equipment from involved officers and witness officers, as well as equipment already secured by the Patrol Supervisors, at the earliest opportunity. The Homicide Unit or FDIT personnel will transport the cameras to the involved officer's assigned district or the Homicide Unit for upload into the system. The BWC equipment will be returned to the officer as soon as possible following the event.
- Once uploaded, the Video Evidence Unit shall restrict video access from all users except for the Homicide Unit and/or FDIT investigators assigned to the case.

**The District Commander:**

Will respond to the scene and assume overall command of the situation pending the arrival of the Firearm Discharge Investigation Team.

Assign a Superior Officer to assist the Firearm Discharge Investigation Team and ensure that any and all District resources are made available to complete the investigation. The District Commander will have the flexibility to assign any Superior Officer to fulfill this task. Ensure that full cooperation is extended to the Firearm Discharge Investigation Team and any designated investigators from the District Attorney's Office.

**FDIT Commander:**

Shall be responsible for ensuring that a Firearm Discharge Investigation Team is assigned to investigate all reported firearm discharges by Department personnel except discharges which occur during Department authorized or approved firearms training, while lawfully engaged in target practice or while hunting (unless a discharge occurring during one of these three exceptions results in death, personal injury or property damage).

The FDIT Commander shall have the flexibility and discretion to assign any investigators deemed appropriate as being members of the Firearm Discharge Investigation Team.

The FDIT Commander shall have ultimate responsibility for ensuring the thoroughness of any investigation regarding a firearm discharge or the use of deadly force by Department personnel.

**Firearm Discharge Investigation Team:**

- Shall respond to the scene as expeditiously as possible and immediately meet with the Patrol Supervisor and be briefed relative to the known facts surrounding the incident. • Shall notify the Operations Division that they are taking control of the scene and the investigation. Notifications must be done "on-air."
- Shall be allowed any resources they deem necessary to conduct a complete investigation. • Shall conduct a thorough investigation to determine the facts of the incident. • Shall coordinate with any other simultaneous investigations.
- Shall submit a preliminary report within ten (10) days to the FDIT Commander, the Bureau Chief of the appropriate command and to the Superintendent-In-Chief. The Superior Officer in Charge of the Firearm Discharge Investigation Team shall make a recommendation in the preliminary report, based upon an assessment of the facts known, as to the justification for the use of deadly force, whether or not the firearms discharge was accidental and whether or not it involved personal injury, death or damage to personal property.

Pending this report, the Officer involved will be assigned to administrative duties in their unit of assignment. However, if the preliminary investigation indicates that the firearm discharge was justified, the Officer may be restored to regular duties, with the approval of their Commanding Officer, the Bureau Chief of the appropriate command, the Superintendent-in Chief and the concurrence of the Police Commissioner.

The FDIT Incident Coordinator shall submit a complete and detailed report with

recommendations to the FDIT Commander and to the Superintendent-in-Chief.

**Sec. 12 Disposition:** Upon receiving a report pertaining to a firearms discharge and investigation by the FDIT Incident Coordinator, the Superintendent-in-Chief may accept it or return the report with a request for further information or clarification. In every case, the authority and responsibility for final Departmental disposition of a firearms discharge incident rests solely with the Police Commissioner. Upon accepting a report and making a final disposition in a firearm discharge case, copies of the Police Commissioner's decision shall be sent to the appropriate District, Unit and Bureau Commanders.

Gregory P. Long  
Superintendent In Chief



## Rules and Procedures

### Rule 307

November 27, 2007

#### **Rule 307 - SECURITY OF CRIMINAL OFFENDER RECORD INFORMATION (CORI) AND THE PUBLIC RECORD LAW (PRL)**

This rule is issued to ensure compliance with Massachusetts General Laws Chapter 6, Sections 167-178 and the Code of Massachusetts Regulations, Title 803, Chapter 2.04. These statutes and policies outline the regulations and liabilities associated with Criminal Offender Record Information (CORI). This rule is effective immediately, superseding all rules, orders, bulletins and other directives previously issued in connection with the release of CORI. In conjunction with this rule, members of the Department shall also adhere to the guidelines issued in Rule 300, News Media Relations – Release of Official Information.

**Sec. 1 GENERAL CONSIDERATIONS:** The policy of the Boston Police Department with regard to the release of official information to the news media and other persons interested in Departmental activities has been set forth in Rule 300, News Media Relations – Release of Official Information. However, since the Acts of 1973, Chapter 1050, gives the public the right of access to certain public records, and M.G.L. Chapter 6 exempts Criminal Offender Record Information from public access, the Department is obliged to protect its personnel from civil and criminal liabilities that may result from the improper disclosure of protected records. All Boston police officers are eligible to receive Criminal Offender Record Information in the course of their official duties. However, having obtained such information, no police officer shall give, furnish, or disseminate, directly or indirectly, any probation records or other criminal offender record information except as authorized by this rule. The Department will thoroughly investigate any and all instances of the unauthorized release of CORI information, as conveying the contents of an individual's probation or police record to any unauthorized person or agency may result in civil and criminal liability.

**Sec. 2 DEFINITIONS:** For the purposes of this rule, pursuant to M.G.L. c. 6 §§ 168-178 and 803 C.M.R. 2.00 – 9.00, the following definitions shall apply:

**A. Criminal Justice Agencies** – those agencies at all levels of government which perform as their principal function, activities relating to crime prevention, including research or the sponsorship of research; the apprehension, prosecution, adjudication, incarceration, or rehabilitation of criminal offenders; or the collection, storage, dissemination or usage of CORI.

**B. Criminal Offender Record Information** – records and data in any communicable form compiled by a criminal justice agency which concern an identifiable individual and relate to the nature or disposition of a criminal charge, an arrest, a pre-trial proceeding, other judicial proceedings, sentencing, incarceration, rehabilitation, or release. This includes

photographs and fingerprints, which are recorded as a result of the initiation of a criminal proceeding. CORI does not include:

- **Statistical Records and Reports** – CORI shall not include statistical data in which individuals are not identified and from which identities are not ascertainable. •

- **Juvenile Data** – CORI shall not include information concerning a person who is under the age of 17 years unless that person is prosecuted criminally as an adult. •

- **Intelligence Information** – CORI shall not include records and data compiled by a criminal justice agency for the purpose of criminal investigation, including reports of informants, investigators or other persons, or from any type of surveillance associated with an identifiable individual. Intelligence information shall also include records and data compiled by a criminal justice agency for the purpose of investigating a substantial threat of harm to an individual, or to the order or security of a correctional facility. This information may still be protected from public disclosure, per the investigatory exemption to the Public Records Law. Contact the Office of the Legal Advisor prior to releasing this information to a member of the public.

- **Information Regarding Minor Offenses** - CORI shall not include information concerning offenses that are not punishable by incarceration.

- **Photographs or Fingerprints of an Unidentified Individual** – CORI shall not include photographs, fingerprints, or other identifying data of an individual used for investigative purposes if the individual is not identified. This information may still be protected from public disclosure, per the investigatory exemption to the Public Records Law. Please contact the Office of the Legal Advisor prior to releasing this information to a member of the public.

- **Information of a Deceased Individual** – CORI shall not include information regarding a deceased individual. Restrictions on the access to and dissemination of an individual's CORI terminate upon his / her death.

**C. Criminal History Systems Board (CHSB)** – the entity which is given the duty of promulgating regulations regarding the collection, storage, dissemination and usage of CORI.

**Sec. 3 AGENCIES ALLOWED TO RECEIVE CORI:** M.G.L. Chapter 6, Section 172 provides that CORI may be disseminated, whether directly or through an intermediary, only to: **A.** Criminal justice agencies;

**B.** Other agencies and individuals required to have access to such information by statute including US Armed Forces recruiting offices for the purpose of determining whether a person enlisting has been convicted of a felony;

**C.** The active or organized militia of the commonwealth for the purpose of determining whether a person enlisting has been convicted of a felony; and **D.** Any other agencies and individuals where the CHSB has determined that the public interest in disseminating such information to these parties clearly outweighs the interest in security and privacy.

**Sec. 4 PUBLIC DISSEMINATION OF CORI:** The public dissemination of CORI is allowed under the following circumstances:

**A. Victim receipt of CORI** – M.G.L. Chapter 6, Section 178A provides that a victim of a crime, a witness, or a family member of a homicide victim, all as defined by M.G.L. Chapter 258B, Section 1, shall be certified by the CHSB, upon request, to receive CORI, provided that the request for said information relates to the offense in which the person was involved;

**B. Contemporaneous with investigation** - A criminal justice agency with official responsibility for a pending criminal investigation or prosecution may disseminate CORI that is specifically related to and contemporaneous with an investigation or prosecution;

**C. Contemporaneous with search for person** - A criminal justice agency may disseminate CORI that is specifically related to and contemporaneous with the search for or apprehension of any person; and

**D. Information regarding incarceration / custody status** – A criminal justice agency with jurisdictional responsibilities for an offender shall release information regarding an individual's custody status and placement within the criminal justice system where:

- The individual named in the request or summary has been convicted of a crime punishable by a term of imprisonment of 5 years or more or has been convicted of any crime,
- Sentenced to any term of incarceration, and
- At the time of the request:
  - o Is serving a sentence of probation or incarceration; or
  - o Is under the supervision of the Parole Board; or
  - o Having been convicted of a misdemeanor has been released from all custody or supervision for not more than one year; or
  - o Having been convicted of a felony has been released from all custody or supervision for not more than two years; or
  - o Having been sentenced to the custody of the Dept. of Correction has finally been discharged there from, either having been denied release on parole or having been returned to penal custody for violation of parole, for not more than three years.

**Sec. 5 LIABILITY FOR UNAUTHORIZED DISCLOSURE OF CORI:**

**A. Civil Liability** – M.G.L. Chapter 6, Section 177 sets forth the civil liabilities that may be incurred by those who willfully communicate CORI to anyone not authorized to receive it.

**B. Criminal Liability** – M.G.L. Chapter 6, Section 178 states “[a]ny person who willfully requests, obtains or seeks to obtain CORI under false pretenses, or who willfully communicates or seeks to communicate CORI to any agency or person except in accordance with the provisions of sections 168-175, inclusive, or any member, officer, employee or agency of the board or any participating agency, or any person connected

with any authorized research program, who willfully falsifies CORI, or any records relating thereto, shall for each offense be fined not more than \$5000.00, or imprisoned in a jail or house of correction for not more than one year, or both."

**Sec. 6 PROCEDURES:** Members of the Department shall strictly adhere to the following procedures to maintain the security of CORI:

- A.** Members of the Department who are not assigned to the Identification Unit shall not give, furnish or disseminate, directly or indirectly, any CORI to any individual or agency outside the Department. However, members of the Department may disseminate CORI to criminal justice agencies with whom the Department is engaged in a criminal investigation. Members shall refer any agency or individual seeking such information to the Identification Unit.
- B.** The Attorney General of Massachusetts has notified all local licensing bodies and all other non-criminal justice agencies authorized to receive CORI by the CHSB not to make record requests through local police departments or the Massachusetts State Police. Department personnel who furnish CORI to such non-criminal justice agencies may be subject to the civil and criminal sanctions of M.G.L. Chapter 6, Sections 177 and 178. Personnel shall refer all non-criminal justice agencies to the CHSB for access to CORI.

**Sec. 7 REQUESTS FOR CORI BY OUTSIDE AGENCIES:** Identification Unit personnel shall only honor requests for CORI from non-federal outside criminal justice agencies certified by CHSB when the requests are in writing, whether by Teletype or US Mail. The Identification Unit will also honor e-mails with confirmed government URL and faxes with appropriate agency letterhead. The Identification Unit will not honor walk-in requests. Identification Unit personnel shall provide CORI to federal law enforcement agents on a walk-in basis upon proof of identity. Identification Unit personnel in doubt as to the eligibility of a person(s) to receive CORI shall contact the Office of the Legal Advisor for guidance.

**Sec. 8 RECORD OF CORI REQUESTS:** M.G.L. Chapter 6, Section 172 mandates that each agency holding or receiving CORI shall maintain, for such period as the board shall determine, a listing of the agencies or individuals to which it has released or communicated such information. From time to time, the CHSB or council may review such listings, or reasonable samples thereof, to determine whether any statutory provisions or regulations have been violated.

Except as otherwise provided, each time Department personnel request criminal or non criminal records or photographs from the Identification Unit's Records Section, they shall complete BPD Form 0032-BIS-0107. The Records Section shall provide this form and after completion, shall maintain it in Section files. This applies to telephone (intradepartmental) and walk-in requests.

**Sec. 9 REQUESTS TO THE IDENTIFICATION UNIT BY BOSTON POLICE PERSONNEL:** Requests by

members of the Department for CORI and/or photographs can be made in person or by telephone. In all cases of telephone requests in which the requesting officer is unknown to the Identification Unit/Records Section person receiving the call, the Identification Unit/Records Section person shall return the call to verify the identity of the requesting officer before any information is released. He/she shall call the place of assignment of the requesting officer, or his/her assigned department cell phone to verify the officer's identity, not his/her home or a private telephone number. Identification Unit/Records Section personnel shall complete a copy of BPD Form 0032-BIS-0107 each time Boston Police personnel request information and maintain this form in Section files.

**Sec. 10 SPECIAL SEARCHES:** The Identification Unit's Record Section' files may be searched by the following persons without the assistance of the Section's personnel. They shall not be required to sign for necessary information; however, records shall not be removed from the file room:

§ Chief, Bureau of Professional Standards and Development, and his/her designee ▪  
Commanding Officer, Homicide Unit, and his/her designee

**Sec. 11 CJIS ACCESS:** The data stored in the CJIS is documented criminal justice information and must be protected to ensure correct, legal, and efficient dissemination and use. Only law enforcement and criminal justice personnel in the performance of their authorized criminal justice activities can obtain information from or through CJIS.

Department personnel must be certified by the Criminal History Systems Board to access Board of Probation (BOP) records electronically through the CJIS Mobile Data Terminal System. In addition, all CJIS terminal and Mobile Data terminal operators must be re-certified once every two years.

The CJIS Automated Board of Probation file was created to provide users with on-line access to both the adult and juvenile arraignment and disposition data maintained by the Office of the Commissioner of Probation. Information provided in response to a BOP query is CORI.

**Sec. 12 PUBLIC RECORDS LAW:** M.G.L. Chapter 4, Section 7 (26) provides that every record of a city, town or state agency is deemed public, unless an exemption under the Public Records Law (PRL) applies. M.G.L. Chapter 66, Section 10 states that if the agency can demonstrate that any of the PRL exemptions apply to a record, the specific information must be redacted and the remaining information is deemed public and must be disclosed. CORI falls within the "statutory exemption" of the PRL. **All PRL requests must be referred to the Public Information Office in Headquarters, or to the Office of the Legal Advisor.**

Edward F. Davis  
Police Commissioner

## Rule 322 – Department Property

---

**May 20, 2020**

Rule 322, Department Property establishes the duties and responsibilities of Police Department employees concerning Police Department property. It is effective immediately, superseding all previously issued directives.

Sec. 1 All property, as defined in Sec. 2, owned or controlled by the Police Department, whether for general purposes or in use by individual members, shall be managed by the Commanding Officer of the Office, Bureau, District, Division, or Unit occupying or using such property; such custody over the headquarters building and the property therein shall be exercised by the Commissioner.

Sec. 2 Department Property and the Issuing Authorities are defined as follows:

<b>Equipment</b>	<b>Issuing Authority</b>
Department Issued Firearm & Holster	Department Range
Ammunition & Magazines	
Badge OC Spray & OC Spray Holder Body Armor Handcuffs Gas Masks Helmet Batons Emergency Equipment Bag Issued Uniforms & Clothing	Central Supply Division
Radios/Chargers Pagers Mobile Devices IPads	Telecommunications Unit
Body Worn Cameras	Bureau of Administration and Technology
Laptop Computers	Informational Technology Division
Vehicles and Equipment	Fleet Management Division

Department Identification Cards	Human Resources Division
Department Parking Permits	Office of the Police Commissioner

Sec. 3 Property supplied by the department to individual members shall be furnished by the Issuing Authority, as defined in Sec 2. The Issuing Authority is charged with the responsibility of keeping accurate records relating to the acquisition, issuance, disposition and return of such property.

Sec. 4 Every employee will be required to sign a receipt from the Issuing Authority for department property which is issued for use while the employee is a member of the department. Employees are responsible for ensuring that Department property assigned to them is secured at all times. If Department property is left in a motor vehicle it must be stored in the trunk or another secure location out of sight of passers by.

Sec. 5 When a department employee is transferred from one Office, Bureau, District, Division, or Unit to another they shall retain all the department property in their possession unless the Commander directs otherwise. The Commander shall ensure that all department equipment and property that was specifically issued for use by the employee while assigned to the Unit/Division is returned to the Issuing Authority. An employee surrendering any department property in their possession to a Commander shall receive a copy of department form 2980 as a receipt for such property surrendered. It shall be the responsibility of the employee to insure that any property surrendered by them is properly and completely identified on the form 2980 which they accept. Employees should maintain copies of receipts for their records.

Sec. 6 Commanders shall ensure that all department property is returned to the Issuing Authority upon the suspension for more than 7 days, retirement, termination of employment or death of an employee under their command and that Department Form 2980 has been completed and forwarded to the Human Resources Division.

Sec. 7 When any member of the force is disabled or hospitalized while on duty it shall be the responsibility of their immediate Superior Officer to take possession of their Department Issued Firearm, ammunition and magazines and store them in the district /unit gun locker.

Sec. 8 District and Unit Commanders are charged with the responsibility of taking possession of Department Issued Firearms, ammunition and magazines, department radios and chargers, OC spray and OC spray holders issued to an employee of their command and forwarding them to the Issuing Authority for custodial purposes under the following conditions:

A. When an employee has been reassigned to the Human Resources Divisions' Medically Incapacitated Section.

B. When an employee, in the opinion of the Commander, is suffering from an emotional illness or condition which renders them unfit for duty.

Sec. 9 District and Unit Commanders are charged with the responsibility of taking possession of the employees' Badge and Department Identification Card, Department Issued Firearm, Ammunition and magazines, Department Radio and charger, OC spray and OC spray holder, and forwarding them to the Issuing Authorities;

A. When a member of their command has been reassigned to the Human Resources Divisions:

- Administrative Leave Section
- Extended Leave Section
- Leave of Absence Section, (except when the member is assigned to Military Leave, per Commissioner' Memo 08-034; for both active duty and annual training, commanders should not collect the employee's Badge or Department Identification Card.)
- Suspended Section

Sec. 10 District and Unit Commanders may take possession of other Department property issued to employees absent from duty because of any of the foregoing reasons when they determine that it is in the Department's best interest. When a Commander takes possession of Department property, under the conditions outlined in Sections 6, 7, 8 or 9 they shall forward them to the Issuing Authority for custodial purposes, complete Department Form 2980 and forward to the Human Resources Division.

Sec. 11 The Issuing Authority shall not re-issue Department property, taken into custody under the provisions of the previous sections of this Rule, without consent of the Commander who forwarded the property with the exception of the Department Issued Firearm which shall be returned only with the approval of the Police Commissioner.

Sec. 12 Prior to retiring from, or terminating their service with the Department, officers shall deliver their Department Issued Firearm, Ammunition and Magazines to the Department Range and their OC spray and OC spray holders and other issued equipment as defined in Sec. 2 to the Central Supply Division where Department Form 2980 shall be initiated. They shall also deliver all other Department property which has been issued to them to the Issuing Authority where Department Form 2980 shall be completed. Employees shall maintain a copy of their Department Form 2980, the original shall be submitted to the Human Resources Division.

Sec. 13. The Human Resources Division of this Department shall not certify any employee for retirement or termination of service until the original copy of Department Form 2980 has been received in the Human Resources Division. A copy of the completed form 2980 shall be attached to all retirement or termination of service paperwork being processed through the Department.



Sec. 14 Whenever any Police Department property which has been issued to an employee, which is in the custody of an employee or under their control or is being utilized by said employee, is lost, stolen, damaged or destroyed, the employee shall report promptly and in writing to their Commander a complete statement which shall contain all of the facts concerning the property. The Commander shall forward their report, together with their recommendations as to who shall bear the expense occasioned by such loss, theft, damage or destruction of Department property, to the Chief of the Bureau of Administration and Technology.

Sec. 15 When the determination has been made that an employee is liable for the loss, damage or destruction of Department property and the recommendation has been made that the employee shall bear the expense of replacing or repairing the property, the Director of Finance shall forthwith send the officer or employee a bill specifying the amount of money to be paid to the Police Department.

If such bill is not paid within sixty (60) days thereafter or arrangement for payment has not been negotiated, the Finance Division shall forward written notification of that fact to the Bureau Chief and the Commander of the employee involved. The Chief, Bureau of Administration and Technology, after consultation with the Department Legal Advisor, shall notify the Bureau Chief of the employee involved to institute immediate disciplinary action.

William G. Gross  
Police Commissioner

**Notes:**

Amended by SO 07-016, issued April 2, 2007, update the organization names to reflect the new BPD organizational structures. Section 2, 14 and 15.

Amended by SO 20-18, issued 5/14/2020, Section 2 of this rule has been amended to include IPads and Body Worn Cameras. The Issuing Authority of Department Parking Permits has been amended to the Office of the Police Commissioner.

Amended by SO 20-19, issued 5/20/2020, Section 9, Leave of Absence (military)

## **Rules and Procedures**

### **Rule 322A**

**January 28, 2003**

#### **Rule 322A - RETENTION AND DESTRUCTION OF RECORDS AND MATERIALS**

##### **Purpose:**

This Rule is established in order to ensure Department compliance with M.G.L. c. 66, § 8, regarding retention of certain Department records and the destruction of certain other records, and such higher standards for retention and destruction as the Department may require.

##### **GENERAL CONSIDERATIONS:**

This Rule does not apply to the following records which shall be retained permanently and are not subject to any city or state mandated retention schedule:

- criminal records;
- material which may be used as evidence;
- records relating to an event for which legal processes have been issued and are pending against a person; and
- Records of the Identification Section which come under the Criminal Offender Records Act.

##### **Sec. 1 Definitions:**

Intra-Departmental Records - shall be defined as records covered by M.G.L. c. 66, § 8, but not specifically subject to state retention schedules.

Non-sensitive Records - shall be defined as those records referred to in Sections 3, 4, 5 and 6 of this Rule.

Record Series - shall be defined as a set of records organized or filed in accordance with a single filing system.

Retention Schedule - shall be defined as the minimum period of time that records must be retained as determined by the Secretary of State, Supervisor of Public Records, Records Management Section and/or such other standards as may be set by ordinance, law or Department policy.

Sensitive Records - shall be defined as those records listed below in Section 2 of this Rule.

##### **Sec. 2 RECORDS TO BE MAINTAINED PERMANENTLY:**

The originals of the following records shall be permanently retained (Note: Parenthetical notation indicates the Division or Unit that is responsible for retention of the listed record or records):

- Arrest Reports (Field Reports Unit)
- Auctioneer's License (Licensing Unit)
- Auto Theft, Recovery & Verification Reports (Insurance Reports Unit) •  
Bicycle Registration (Licensing Unit)
- Death Report (Suicides, Sudden Deaths, Unexplained) (Field Reports Unit) •  
Departmental Annual Report (One Mint Copy) (Office of Research & Evaluation) •  
Drug Control Log (Districts)
- Equipment Inventory (Units/Districts)
- Equipment Maintenance Logs (Central Supply)
- Fatal Motor Vehicle Accident Report (Auto Investigators, Districts)
- Firearm Identification Card (Licensing Unit)
- Firearm, License to Carry (Application) (Licensing Unit)
- Firearm, License to Carry (Licensing Unit)
- Firearm, License to Sell (Licensing Unit)
- Firearm, Wound Report (Field Reports)
- Firearm, Report of Discharge by Police Officer (Internal Affairs)
- Gunsmith License (Licensing Unit)
- Incident Report (Field Reports Unit)
- Investigation Report, Murder (Homicide Unit)
- Journal Log (Districts)
- Junk Collector's License (Licensing Unit)
- Junk Shopkeeper's License (Licensing Unit)
- License to Buy, Sell, Exchange or Assemble Secondhand Motor Vehicles... (Licensing Unit)
- License to Deal in Secondhand Articles (Licensing Unit)
- License to Keep a Public Lodging House (Licensing Unit)
- License to Sell Ammunition (Licensing Unit)
- Pawnbroker's Daily Report (Pawn Unit)
- Pawnbroker's License (Licensing Unit)
- Personnel Orders (Human Resources Division), Special Orders and Commissioner's Memoranda (Office of Research & Evaluation) & Training Bulletins (Training & Education Division)
- Personnel Records

Appointment Certificate and Civil Service Records (Records & Central Attendance Management Unit)

Employment History Record (Records & Central Attendance Management Unit) Detail and Time Books (a/k/a Payroll-Departmental) (Payroll Unit)

- Property Receipt Books (Districts/Central Supply Division)

- Rules and Regulations (a/k/a Rules & Procedures) (Office of Research & Evaluation) •
- Secondhand Dealer's Daily Report (Pawn Unit)
- Supplementary Incident Report (Field Reports Unit)

If any of the above records are microfilmed by the Department, they may then be destroyed after written permission has been granted by the Chief, Bureau of Administration and Technology in accordance with this Rule.

Sec. 3 Records Maintained for Seven Years:

- Overtime Slips (Payroll Unit)

Sec. 4 RECORDS MAINTAINED FOR THREE YEARS:

The originals of the following records shall be retained for a period of three (3) years before seeking written permission to destroy or dispose of them:

- All records pertaining to moneys, collected as licensing fees and other administrative cash receipt books and cash disbursements (One year after they have been released by the Auditor) (Central Cashier)
- Bicycle Courier's License (Licensing Unit)
- Bicycle Courier's Service License (Licensing Unit)
- Correspondence with non-Departmental individuals and agencies: if of no informational or evidential value (Individual Authors)
- E-911 Call Detail Record (Operations Division)
- Evidence Control Form (Central Supply Division)
- Leave Reports (Records & Central Attendance Management Unit)
- Licensed Premise Inspection Notice (Licensing Unit)
- Missing Person Card (Missing Person Unit)
- Motor Vehicle Citation (Districts)
- Motor Vehicle Citation Audit Sheet (Districts)
- Notice of Sale of Unclaimed Property (Central Supply Division)
- Overtime Report (Payroll Unit)
- Parking Violation Ticket (Districts)
- Prisoner Inspection Record (Districts)
- Protective Custody Report (Districts)
- Radar Log (Districts)
- Roll Call Report (Districts)
- Traffic Ticket Distribution Control Logs (Districts)
- Vacation Report (Records & Central Attendance Management Unit)

Sec. 5 RECORDS MAINTAINED FOR ONE YEAR:

The originals of the following records shall be retained for a period of one year before seeking

written permission to destroy or dispose of them:

- Collective Musician's License (One year after expiration of license) (Licensing Unit)
- Cruiser Maintenance Report (One year after retirement of vehicle) (Fleet Management Division)
- Itinerant Musician License (One year after expiration of license) (Licensing Unit)

#### Sec. 6 Tape Recordings:

The following shall be eligible to be disposed of or reused 60 days after disposition of the case, provided no litigation is pending, unless an inquiry or request has been made for a specific tape. Any such tape which is the subject of any inquiry, request, investigation or litigation, may not be disposed of or reused without first obtaining the prior written approval of the Commander, Operations Division. The Commander, Operations Division shall ensure that a separate tape recording has been made of any tape which is the subject of any inquiry, request, investigation or litigation, prior to authorizing its disposal or reuse.

- Dispatch Tapes
- Tape Recordings of Phone Calls (E-911, etc.)

#### Sec. 7 DESTRUCTION OF SENSITIVE RECORDS:

Sensitive records shall be destroyed or otherwise disposed of only in compliance with the following procedures:

- A. The contents of the records to be destroyed or disposed of shall be duplicated in some fixed form (i.e., microfilm).
- B. The respective Bureau Chiefs shall submit a report in writing, semi-annually, or sooner if the necessity arises, to the Chief, Bureau of Administration and Technology, or their designee, detailing all sensitive records which have been duplicated in compliance with the above paragraph.
- C. The Chief, Bureau of Administration and Technology, or their designee, shall notify in writing, through the Superintendent-in-Chief, any and all concerned Districts and Divisions of the pending destruction of the records. All concerned District and Division Commanders or Directors shall notify the Chief, Bureau of Administration and Technology, or their designee, through the Superintendent-in-Chief, of the approximate cubic feet of records in each series of sensitive records.
- D. The Chief, Bureau of Administration and Technology, or their designee, shall total the cubic feet in each series of records to be destroyed for the Department. The Chief, Bureau of Administration and Technology shall then prepare a written request for the destruction of the records. The request shall include a description of the record by series, date and quantity. The request shall also reference the approved City retention schedule and include a notification of the intended time, place and method of disposal. This request shall be made to the City Archivist who will forward it to the City Clerk,

Corporation Counsel and the Commonwealth of Massachusetts Supervisor of Public Records.

- E. Upon receipt of the written approval from the City Clerk and Corporation Counsel, the Chief, Bureau of Administration and Technology shall inform the Property Clerk of said approval. The Property Clerk shall arrange to have the records destroyed in conformance with procedures established by the Bureau of Administration and Technology and approved by the Police Commissioner. Said records shall be destroyed within 90 days of receipt of the written approval from the City Clerk.
- F. The Chief, Bureau of Administration and Technology shall submit a certificate of disposal to the City Archivist listing all records destroyed within thirty (30) days of such destruction.

#### Sec. 8 DESTRUCTION OF NON-SENSITIVE RECORDS:

Non-sensitive records shall be destroyed or otherwise disposed of only in compliance with the following procedures:

- A. Each District and Division Commander or Director, seeking to dispose of non-sensitive records in compliance with applicable retention schedules, shall notify the Chief, Bureau of Administration and Technology, or their designee, through their respective Bureau Chief, of the record(s) series which they intend to destroy and of the approximate cubic feet of the records in each series.
- B. The Chief, Bureau of Administration and Technology, or their designee, shall total the cubic feet in each series of records to be disposed of for the Department. The Chief, Bureau of Administration and Technology shall then prepare a written request for the disposal of the records. The request shall include a description of the record by series, date and quantity. The request shall also reference the approved City retention schedule and include a notification of the intended time, place and method of disposal. The request shall be made to the City Archivist who will forward it to the City Clerk, Corporation Counsel and the Commonwealth of Massachusetts Supervisor of Public Records.
- C. Upon receipt of the written approval from the City Clerk and Corporation Counsel, the Chief, Bureau of Administration and Technology, through the Superintendent-in-Chief, shall inform the concerned Districts and Divisions of said approval. The District and Division Commanders or Directors shall dispose of the records through established Departmental procedures within 90 days of receipt of the written approval from the City Clerk. After having destroyed said records, District and Division Commanders or Directors shall give notification of such destruction, through their respective Bureau Chiefs, to the Chief, Bureau of Administration and Technology.
- D. The Chief, Bureau of Administration and Technology shall submit a certificate of disposal listing all records disposed of to the City Archivist within thirty (30) days of such destruction.

#### Sec. 9 INTRA-DEPARTMENTAL RECORDS:

Intra-Departmental records shall be destroyed or otherwise disposed of in compliance with the following procedures after having been retained for a minimum of six (6) months:

- A. Each District and Division Commander or Director seeking to dispose of Intra Departmental records shall notify the Chief, Bureau of Administration and Technology, through their respective Bureau Chiefs.
- B. Upon receipt of the written approval of the Chief, Bureau of Administration and Technology, the District and Division Commanders or Directors shall dispose of the records through established Departmental procedures.

Notes:

- Amended by SO 07-016, issued April 2, 2007, update the organization names to reflect the new BPD organizational structures. Sections 2, 7, 8 and 9.



**February 20, 1998**

**Rule 324A - TWO-WAY RADIO AND MOBILE DATA TERMINAL PROCEDURES**

This Rule is issued to establish Department procedures for the management of response to incidents through the two-way radio and Mobile Data Terminal (MDT) systems as an integral part of the Enhanced 9-1-1 system, hereinafter referred to as the 9-1-1 system.

It is important to remember that the two-way radio and the MDT represent an officer assigned to the field's primary contact with Headquarters. Officers assigned to the field rely on this for assistance and protection.

In order to ensure uniformity, all Bureaus, Divisions, Districts and Units will use their radio call signs in conformance with this Rule. This Rule shall be utilized to ensure the effective and efficient use of the Boston Police Department radio system and the Mobile Data Terminal (MDT) system in a manner that is compatible with the Computer Aided Dispatch (CAD) system. Any changes, additions, or deletions of call signs must be approved by the Chief of the Bureau of Field Services (BFS).

**Sec. 1 GENERAL CONSIDERATIONS:**

**Confidentiality of Callers:** MDTs will allow officers assigned to the field access to the name, address and phone number of the person who called 9-1-1. However, citizens who call 9-1-1 do not always want to be identified for fear of retaliation or for other reasons. Officers should be aware of the confidentiality issue and take extra precautions to protect the identity of the caller at all times. In the event responding officers need additional information regarding a particular call, they shall request the Dispatcher contact the caller via the callback number to obtain such information instead of approaching the caller themselves. Additionally, officers shall avoid two-way radio transmission of a caller's name, address and/or phone number. Whenever possible, officers shall clear information from their MDT computer screens prior to exiting their cruisers by pressing the CLR key.

**LEAPS and NCIC Information:** As in all circumstances, information obtained via MDT from the Law Enforcement Agencies Processing System (LEAPS) and from the National Crime Information Center (NCIC) should be treated as confidential information for the use of police personnel only. Officers are reminded that all Criminal Offender Record Information (CORI) is confidential and protected by state law (M.G.L. c. 6, § 172).

**Updated CAD Information:** Officers responding to an MDT 9-1-1 call should be aware that CAD information is routinely supplemented and modified. Therefore, to be certain that their actions are based on the most recent information, officers should use the "Recall" command to obtain and read such information before exiting their cruisers.

**Premise Information:** In the upper right hand corner of a 9-1-1 call on the MDT computer screen, officers may see two letters, such as AH, PW, or OC indicating that the address they are responding to has Premise Information. The Address History (AH) feature of the CAD cross



## Appendix N

references Central Complaint (CC) numbers of 9-1-1 calls to that address for the last thirty (30) days. Police Warning (PW) may contain information about recent gang or drug activity. Occupant Information (OC) may inform officers about a handicapped person who lives at an address and may not be able to answer the door. All officers should use the "Recall" command to obtain and read any Premise Information associated with an address before they exit their cruisers to enter that address.

### Sec. 2 COMMUNICATIONS CONDUCT:

Any officer(s) assigned a vehicle shall examine the two-way radio and MDT to ensure that they are functioning properly. Defective two-way radios and MDTs shall be noted on the vehicle's Motor Vehicle Inspection Form and brought to the attention of the Patrol Supervisor prior to leaving the station to begin patrol.

Courteous and judicious use of transmission time is imperative in order to ensure the efficient and effective operation of the two-way radio and MDT system. Only essential information shall be transmitted by two-way radio or MDT, as excessive and unnecessary communications can be confusing and may cause misunderstandings. All transmissions must be clear, concise and accurate.

All officers are advised that all two-way radio and MDT transmissions are recorded and, in some cases, may become public information. MDT transmissions are subject to periodic review for appropriateness and conformance to this Rule by the Auditing and Review Division. All transmissions are also subject to constant monitoring by Supervisory and Operations Division personnel. Personnel found to be making personal or inappropriate transmissions using MDTs or two-way radios are subject to disciplinary action. Examples of prohibited transmissions are, but are not limited to:

- A. Unnecessary two-way radio conversations or MDT transmissions are prohibited; B. Transmissions on the two-way radio or MDT which are argumentative or involve the use of sarcasm, et cetera, are prohibited;
- C. Use of profane and obscene language is prohibited;
- D. Logging onto an MDT using someone else's access code number or password is prohibited;
- E. Identify yourself by using only your proper call sign; use of personal names during transmission is prohibited, except in an emergency; and
- F. Logging onto the two-way radio system with, or using, someone else's call sign is prohibited.

Sec. 3 Mobile Data Terminal Procedures: Police Officers assigned to response units equipped with Mobile Data Terminals shall:

- A. Sign on MDT and log on the air via the MDT;
- B. Receive calls for service via MDT;
- C. Acknowledge receipt of calls for service by transmitting appropriate MDT code; D. Inform dispatcher of arrival to assignment by transmitting appropriate MDT code; E. Clear assignment by transmitting the appropriate MDT code;
- F. Check vehicles, warrants and premise history information via MDT;

## Appendix N

- G. Communicate all self-initiated low priority on-sight incidents and motor vehicle stops to the dispatcher via MDT; and
- H. Log off the air via the mobile radio; logging off via the MDT is prohibited.

### EMERGENCY CALL PROCEDURES

Sec. 4 CRITERIA FOR ASSIGNING PRIORITY STATUS: This section provides Operations Division personnel with guidelines to use in evaluating the urgency of a call for service and assigning the appropriate police response.

Operations Division personnel shall adhere to the policy and procedures outlined herein regarding the assignment of priority to a call for service and police response. Dispatchers shall exercise prudent judgment and flexibility in evaluating and/or re-assigning the nature of a call when discretion is required due to exigent circumstances. Incidents entered into the CAD system will be automatically assigned priorities as listed below.

#### A. Priority One (Critical):

Calls for service in this category indicate that a police presence is needed at the scene of an incident. Immediate response to these calls is critical. Calls in this category shall be dispatched by two-way radio for the safety of responding officers and to alert other officers in the vicinity. Conditions that will define a call for service as a Priority One are:

1. Any apparent threat of life, any danger of serious physical injury, any major property damage, or any incident that may result in the same;
2. Any active felony or violent misdemeanor, or active incident that may result in either serious physical injury or major property damage or loss. Also considered as a Priority One call would be any felony or violent misdemeanor that recently occurred (within 15 minutes), and there is a probability that a suspect(s) may be apprehended;
3. Any serious injury or illness that may result in substantial personal harm if police assistance is delayed;
4. Any incident involving exigent or unique circumstances that demands an immediate police response (i.e., sniper, explosive device, gas leak); or
5. Any domestic violence incident.

#### B. Priority Two (Less Critical):

Calls for service in this category indicate that a police presence is needed at the scene, but unlike a Priority One call, an immediate response is not critical. Calls in this category shall be dispatched by two-way radio for officer safety reasons and to alert other officers in the vicinity. Conditions that would classify a call for service as a Priority Two call are:

1. Any recent or active crime or incident that does not represent a significant threat to life and property. These types of incidents would include a felony which has just occurred but without injury to the victim and the suspect(s) has fled the scene (longer than fifteen minutes);
2. Any in-progress incident that could be classified as a possible crime (e.g., suspicious person or vehicle, prowler, et cetera);

## Appendix N

3. Any property damage incident that represents a significant hazard to the free flow of traffic; or
4. Any incident that would require a prompt, but non-emergency response.

### C. Priority Three or Lower Priority Call (Delayed Response):

Calls for service in these categories indicate that some type of police response is needed but could be delayed for a period of time without adverse effect. Calls in this category shall be dispatched by voice for officer safety reasons and to alert other officers in the vicinity. Detailed information regarding calls in this category will be transmitted via the MDT. Callers should be notified of the potential delay at the time the call is received by the 9-1-1 Emergency Call Taker. Conditions that would classify a call for service as a Priority Three or lower priority call (priority 4-9) are:

1. Any non-active crime or incident that does not require an immediate investigation (i.e., a B&E that was not recently committed, but which is being reported at this time);
2. Any incident that involved non-emergency and/or non-criminal services; or
3. Any other incident that is no longer active, yet due to its nature, cannot be responded to by phone.

## Sec. 5 PROCEDURE FOR MANAGING CALLS:

A. Operations Dispatcher: The Operations Dispatcher shall deploy field units with the objective of achieving the Department's goal of keeping the same officer in the same neighborhood at least 60% of the time. While the Department is committed to providing a timely response to all high priority incidents (priority 1 and 2 calls), the dispatcher shall observe the Same Cop/Same Neighborhood philosophy when dispatching lower priority incidents. Strict emphasis shall be placed on keeping response units in their assigned sectors when assigning lower priority calls. The CAD call stacking and Differential Police Response (DPR) features shall be utilized to help accomplish this task.

Only low priority calls shall be stacked for sector units. Additionally, the dispatcher should work cooperatively with the Patrol Supervisor to ensure a fair distribution of the district's 9-1-1 workload.

Priority One Calls: Upon receiving a new incident or supplemented or modified life threatening information over the public address system from a 9-1-1 Emergency Call Taker concerning an incident assignment to a response unit, the Operations Dispatcher shall immediately notify the appropriate unit by two-way radio. Additionally, the Operations Dispatcher when dispatching these Priority One calls shall ensure an adequate response by assigning units in the following order:

1. The Rapid Response Unit whose patrol area encompasses the location of the incident;
2. The Rapid Response Unit whose patrol area is adjacent to the patrol area containing the location of the incident;
3. Any Rapid Response Unit whose close proximity to the incident would significantly enhance the police response;
4. A two-officer District wagon;
5. Two Neighborhood Service Units;

## Appendix N

6. Any two-officer District Detective Unit;
7. Two Mobile Operations (MOP) motorcycles whose close proximity to the incident would significantly enhance the police response; or
8. Any combination of the Patrol Supervisor and a service unit, foot beat, mounted, K-9 or motorcycle officer whose beat encompasses or is adjacent to the location of the incident.

NOTE: Response units always have the option of requesting back-up assistance at any time.

Priority Two Calls (Less Critical): Priority Two calls for service shall be assigned to response units in the following order:

1. The Neighborhood Beat Officer or Neighborhood Service Unit whose patrol area encompasses the incident location;
2. The closest available Neighborhood Service Unit whose proximity to the incident would significantly enhance the police response;
3. A District-wide Neighborhood Service Unit;
4. The Mounted Officer whose patrol area encompasses the incident location;
5. The K-9 Unit whose patrol area encompasses the incident location;
6. Any MOP cycle whose close proximity to the incident would significantly enhance the police response;
7. The Mounted Officer whose patrol area is adjacent to the incident location;
8. The K-9 Unit whose patrol area is adjacent to the incident location;
9. A District Detective Unit;
10. Any District response unit already assigned a Priority Three or lower priority call for service (priority 4-9);
11. The Patrol Supervisor whose supervisory area encompasses the incident location.

NOTE: At the discretion of the Operations Dispatcher, a Rapid Response Unit or District Wagon may be dispatched in place of one of the above units. In addition, responding officers have the discretion to request other appropriate or available units for assistance when necessary (e.g., B&E alarms, entering a building or dwelling, et cetera).

Priority Three or Lower Priority Calls (Delayed Response): Priority Three or lower priority calls for service shall be assigned to response units in the following order:

1. The Neighborhood Beat Officer or Neighborhood Service Unit whose patrol area encompasses the incident location;
2. The closest available Neighborhood Service Unit whose proximity to the incident would significantly enhance the police response;
3. A District-wide Neighborhood Service Unit;
4. The Mounted Officer whose patrol area encompasses the incident location;
5. The K-9 Unit whose patrol area encompasses the incident location;
6. Any MOP cycle whose close proximity to the incident would significantly enhance the police response;
7. The Mounted Officer whose patrol area is adjacent to the incident location;
8. The K-9 Unit whose patrol area is adjacent to the incident location;

## Appendix N

9. A District Detective Unit;
10. The Patrol Supervisor whose supervisory area encompasses the incident location.

NOTE: At the discretion of the Operations Dispatcher, a Rapid Response Unit or District Wagon may be dispatched in place of one of the above units. In addition, responding officers have the discretion to request other appropriate or available units for assistance when necessary (e.g., B&E alarms, entering a building or dwelling, et cetera).

Rapid Response Unit Re-assignment: When a Rapid Response Unit, upon investigating a reported Priority One call for service does not make an arrest and determines that the reported incident will require the completion of a lengthy incident report or was not a Priority One incident, the Rapid Response Unit shall notify the Operations Dispatcher of its findings and the Operations Dispatcher shall, after reviewing the incidents pending list, determine whether the Rapid Response Unit or a Neighborhood Service Unit will complete the assignment. If the Dispatcher determines that the Rapid Response Unit will handle the call for service, that Rapid Response Unit shall complete an incident report or miscel the call, whichever is appropriate.

The Dispatcher, upon deciding that a different unit will complete the assignment, will instruct the Rapid Response Unit to remain at the incident location until the arrival of the Neighborhood Service Unit or until it is assigned to another call for service. If a dispute develops with the reassignment, the Operations Dispatch Supervisor shall be notified to resolve the assignment.

In the event the Rapid Response Unit is assigned another call for service before the Neighborhood Service Unit has arrived, the Rapid Response Unit shall inform the caller or other responsible person, if known, that the neighborhood police officer is responding to complete the report and give further assistance if needed.

### B. Operations Division Supervisors:

The success of Call Management as outlined in this Rule depends largely on the Supervisors in the Operations Division. Therefore, to ensure compliance with Call Management objectives, the Operations Division Supervisors shall:

1. Acquire a complete and clear understanding of the Call Management program and its deployment strategy.
2. Ensure that projected unit assignment times for DPR incidents are passed on to callers.
3. Make periodic checks of dispatchers' work stations to ensure compliance with call stacking guidelines.
4. Make periodic checks of response units' status and direct dispatchers to remind units to clear their assignments as quickly as possible.
5. Ascertaining the status of the Patrol Supervisors on all channels.

## Appendix N

### 6. Make periodic checks on NIU call takers to ensure compliance with DPR call back procedures.

#### I. Operations Division Duty Supervisor:

The Operations Division Duty Supervisor shall ensure compliance with these procedures by:

- a. Ensuring adequate staffing of Dispatchers, Supervisors, 9-1-1 Emergency Call Takers, Telephone Operator, Stolen Car Unit, Towed M/V Unit and clerks. Assign people accordingly and ensure that all personnel are given lunch hours and breaks.
- b. Checking the computer for pending calls and investigating as to why units are on calls for over twenty (20) minutes. In addition, check as to why units are still logged on from a previous tour of duty.
- c. Monitoring broadcasts for log-ons, log-offs, and non-response.
- d. Notifying the appropriate units and/or individuals when required by Department procedures or whenever a high profile incident occurs.
- e. Monitoring for unprofessional transmissions, particularly Unit to Unit channels, e.g., Channel 7, 9, 10, etc..
- f. Distributing any Department Orders or forms to personnel as necessary.
- g. Checking the bilingual voice message when all lines are busy.
- h. Ensuring that pager messages are sent and properly logged.
  - i. Ensuring the sick line phone is staffed and that Districts/Divisions are notified of their sick officers. Ensuring that a written record is kept of all such calls.
- j. Checking the Horizon Board for the status of 9-1-1 Operators on duty.
- k. Being prepared for the tracing of telephone calls and for submitting the proper form if the trace is completed.
- l. Seeing that copies of incident reports (BPD Form 1.1) are directed to the appropriate units.
- m. Handling complaints from civilians and calls for Operations Dispatch Supervisors, as necessary.

#### II. Operations Division 9-1-1 Supervisor:

Operations Division 9-1-1 Supervisors shall ensure compliance with these procedures by:

- a. Inspecting the 9-1-1 Emergency Call Takers' work area, including 9-1-1 phones and voice boxes.
- b. Ensuring that trained personnel are assigned to all necessary positions.
- c. Monitoring personnel by telephone and computer to analyze their competency.
- d. Remaining available for any questions from 9-1-1 personnel pertaining to requests for assistance from the public.
- e. Providing cross-training (when available) to ensure personnel will be able to substitute for another position when needed.
- f. Ensuring that tours for visitors to Operations have a minimum effect on work areas.
- g. Keeping the Operations Duty Supervisor updated on all pertinent issues.

## Appendix N

### III. Operations Division Dispatch Supervisor:

Operations Dispatch Supervisors shall ensure compliance with these procedures by:

- a. Ensuring prompt log-on and log-off of units.
- b. Checking repeatedly the status of all units to ensure availability for calls.
- c. Ensuring prompt dispatch of high-priority calls.
- d. Monitoring motorized pursuits, terminating when appropriate; getting pursuit reports.
- e. Enforcing time and duration of Code 10's.
- f. Ensuring prompt clearing of alarm and service calls.
- g. Monitoring two-way radio transmissions for professional usage by field personnel. h. Assuming command of any serious incident requiring the opening and continued use of Channel One.
- i. Determining that all equipment is working properly.
- j. Reminding personnel that the Operations Dispatcher and/or Dispatch Supervisor will determine if a call will be dispatched, depending on the availability of all units. k. Keeping the Operations Duty Supervisor updated on all pertinent issues. l. Assist dispatchers in verifying units' status.

C. District Patrol Supervisor: The Patrol Supervisor shall review all Motor Vehicle Inspection Forms and ensure that any patrol vehicle containing a defective two-way radio or MDT is sent to the Telecommunications Management Unit (a/k/a Radio Shop) for repairs as soon as possible.

Regarding Call Management, the District Patrol Supervisor shall also be responsible for the following:

1. Ensuring that all patrol units clear their assignments in an expeditious manner.
2. Assisting the dispatcher in checking units' status and deployment.
3. Ensuring that officers change their system password via MDT when necessary.
4. Monitoring two-way radio and MDT calls to response units and by randomly responding to incidents within their Districts.
5. Monitoring response times and times spent on calls.
6. Responding personally to incidents in appropriate cases.
7. Determining the status and approximate locations of response units under their command, i.e., District wagons, walking, mounted, K-9, and MOP Units assigned to their District.

Additionally, while it is the dispatcher's responsibility to assign calls for service to the appropriate response units, the Patrol Supervisor shall monitor the number of low priority calls stacked for each sector unit. The purpose of monitoring stacked calls is to ensure that the Department honors projected unit assignment times and to prevent an unreasonable workload

## Appendix N

for any one patrol unit. This monitoring of stacked calls may be accomplished via the MDT installed in the Patrol Supervisor's vehicle.

Sec. 6 DISPATCHING A UNIT: The Operations Dispatcher, when dispatching a unit by two-way radio, shall announce "Operations to --," properly inserting the unit's call sign. Designations such as "Cars," "Wagons," "P.S.," "Unit," should not be used.

Example:

Dispatcher: Operations to Alpha 101  
or

Operations to Charlie 202  
or

Operations to Delta 674

During overlapping shifts, the Dispatcher shall utilize the shift designated

code: Dispatcher: Alpha 101A  
or

Charlie 202D  
or

Delta 674F

Sec. 7 GIVING AN ASSIGNMENT: Calls with a Priority of One or Two shall be dispatched by two way radio using as few words as possible, yet giving as much information as will be helpful to the officers. The Operations Dispatcher shall give the type of call followed by the location. The Operations Dispatcher shall include whether the incident is occurring inside or outside and any apartment number, if given. The Operations Dispatcher shall conclude the call by announcing the time.

Example:

Dispatcher: Operations to Delta 301

Unit: Delta 301

Dispatcher: 290 Comm. Ave., Apt. #10, family disturbance

Unit: Delta 301, acknowledged



## Appendix N

Dispatcher: 2200 hours

The following format shall be used in broadcasting Priority One or Priority Two calls for service:  
Example:

### STEP ACTION ANNOUNCEMENT

Step #1 Call the Unit Alpha 101

Step #2 Announce Incident Type Robbery in Progress

Step #3 Announce Detailed Location Bank of Boston

751 Washington Street

Calls with a Priority Three or lower priority will be dispatched by radio. Detailed information regarding calls in these categories will be transmitted via MDT.

Example:

Dispatcher: Operations to Delta 301

Unit: Delta 301

Dispatcher: 290 Comm. Ave., Apt. #10, B & E Report.

Unit: Delta 301 acknowledged.

When an assignment is dispatched by MDT, the unit will press the equipment's "en route" key to indicate that they are responding to the assigned call.

Sec. 8 UNIT ARRIVALS ON SCENE: All units will announce their on scene arrival. Units not equipped with an MDT shall make such announcement over the two-way radio. The announcement will give the unit's call sign, followed by the code "Adam Robert." The Operations Dispatcher will acknowledge by stating "Operations acknowledged" or by repeating the message, "Adam Robert" preceded by the unit's call sign.

Example:

Unit: C101 Adam Robert

Dispatcher: Operations acknowledged or C101 Adam Robert

MDT equipped units will announce their on scene arrival by simply pressing the "en route" key.

Sec. 9 ANSWERING FIELD UNITS: Operations Dispatchers should answer a unit by announcing the word, "Operations" followed by the calling unit's call sign.

Example:

## Appendix N

Field Unit: E102

Dispatcher: Operations E102

Field Unit: Seven Paul

Dispatcher: Operations acknowledge Seven Paul or E102 Seven Paul

Sec. 10 HOURLY TIME ANNOUNCEMENTS: Every hour, standard time announcement will be given individually by each Operations Dispatcher.

Example:

Dispatcher: This is the Boston Police Operations on Channel Two at 1400 hours.

Sec. 11 FIELD UNIT PROCEDURES: When communicating with the Operations Dispatcher, units should adhere to the following practices and/or recommendations:

### A. Radio Procedures

1. Plan your message.
2. Before transmitting, listen to make sure you will not interrupt a transmission currently in progress.
3. Depress the microphone button and pause before speaking.
4. Identify yourself by using only your proper call sign.
5. Place your mouth 1-3 inches from the microphone.
6. Speak normally and clearly, as in a telephone conversation.
7. Use an even, modulated tone of voice, avoiding any vocal display of emotion such as loss of temper, impatience or sullenness.
8. Release microphone button as soon as you have finished your message.
9. Give the Dispatcher adequate time to acknowledge your transmission.
10. If possible, avoid lengthy messages. If you have a lengthy message, transmit a portion of it, request an acknowledgment of the message so far, and then continue. If a call is properly covered by a miscel, then a miscel will suffice.

B. MDT Procedures: When using an MDT to miscel or clear a call, an officer shall add appropriate comments to the disposition:

Example: C D/14B, house in darkness, no answer at front door.

C D/RPT, victim will call later with additional information.

1. Acknowledge your calls by pressing the "en route" key.
2. Report your arrival on the scene by the code "Adam Robert" or by pressing the "on scene" key.
3. Clear your call promptly using the appropriate MDT commands.

## Appendix N

### Sec. 12 Vehicle or Field Stops:

A. Radio Procedures: When using the two-way radio for making car stops or stopping an individual, officers shall transmit the following information:

1. Location;
2. Registration number and vehicle description;
3. Number of occupants;
4. Description of individual(s); and
5. Activity of the vehicle or individual stopped.

B. Vehicle or Field Stops Using the MDT: When using the MDT for making a car stop or stopping an individual, officers should use the appropriate CAD type codes such as SS (Subject Stop) or TS (Traffic Stop), including registration number and vehicle/suspect description. For officer safety reasons, to alert the Dispatcher and nearby units of the location of a vehicle or individual stop, officers equipped with MDTs may use the two-way radio Field Stops procedure, if desired.

### Sec. 13 Radio Codes:

The primary purpose for using radio codes is to save time and avoid confusion and misunderstanding.

A. Use the proper code when a miscel or a service assignment code is called for. Unless requested by the Dispatcher, an officer should not give an explanation of his/her service response. The miscel will suffice. Avoid Unnecessary Conversation.

B. Use commonly accepted and/or standard abbreviations or names when transmitting information.

1. Utilize the standard phonetic alphabet as used in miscel codes;
2. Utilize crime information that accurately reflects the incident; and
3. Utilize proper designations.

Example: A&B DW: A cutting, stabbing, shooting

C. Think before you say anything using radio codes or any other radio transmission.

Sec. 14 CALL SIGN STRUCTURE: The call sign structure consists of five digits as

follows: DIGIT 1: Location and/or Organization

A (alfa) = District 1	B (bravo) =	M (mike) = Special Events
District 2	(BFS)	C (charlie) = District 3
L (lima) = District 18	(delta) = District 4	E (echo) =

## Appendix N

District 5 F (fox) = District 6 G (silver) = B.A.S.

(gold) = District 7 H (harry) = T (tango) = Special Operations

District 11 J (jake) = District 13 V (victor) = B.I.S.

K (kilo) = District 14 X (x-ray) = B.I.I.

N (nova) = Operations Y (yankee) = Administrative

R (romeo) = Paid Details S

(Note: Spoken over the air using only those phonetics in

parentheses.) DIGIT 2 Unit Type

1 (one) = Rapid Response

2 (two) = Patrol Wagon

3 (three) = Motorcycles

4 (four) = Neighborhood Service Units

5 (five) = K-9

6 (six) = Neighborhood Beat Officers

7 (seven) = Mounted Patrols

8 (eight) = Detectives

9 (nine) = Sergeants

A (alfa) = Lieutenants

B (bravo) = Captains

C (charlie) = Command Staff

D (delta) = Other

K (kilo) = Anti-Crime

(Note: Spoken over the air using only those phonetics in parentheses.)

DIGIT 3-4 Numbers

## Appendix N

01 (one) through 99 (ninety-nine)

DIGIT 5 Shift

A (ay) = 11:45 p.m. - 7:30 a.m.

D (dee) = 7:30 a.m. - 4:00 p.m.

F (eff) = 4:00 p.m. - 11:45 p.m.

NOTE: Digit 5 will be used by Operations only when there is a situation when two units with the same call sign are logged-on at the same time.

Exception: Officers who are off-duty and/or working a paid detail who do not have a call sign but who need to contact the Operations Division via radio shall identify themselves by utilizing the number engraved on their two-way portable radio unit (e.g., Portable radio #1234 will transmit as "Unit 1234 to Operations").

### Sec. 15 Officer in Trouble/Emergency Broadcast Procedures:

When an officer utilizes the "Emergency" button on their portable radio or MDT device to request immediate assistance, the Operations Dispatcher shall immediately take steps to ensure the officer's safety, using all necessary resources to determine whether or not the officer in question is in need of assistance or is experiencing radio difficulty.

Operations Dispatchers shall take note that when the "Emergency" button is depressed on an MDT, the message sent via MDT displays the unit's call sign, last assigned location and the name of the officer assigned to the unit. Units which are not currently assigned will still display their last known assignment, not their current location. The procedure for ensuring that officers receive needed assistance shall be the same regardless of whether or not they summon assistance via their portable radio or MDT.

If the officer in question is on assignment, patrol units shall be dispatched to the officer's last known location. Upon arrival, responding units shall immediately make an assessment of the situation and apprise the Operations Dispatcher as to whether or not additional help is needed.

If the officer requesting assistance is not on assignment or is not at the location assigned, the Operations Dispatcher shall request that all available units attempt to locate the officer and ensure whether or not the officer is in need of assistance. Upon locating the officer, responding units shall immediately notify the Operations Dispatcher that the officer has been located, render immediate assistance, if necessary, and apprise the Operations Dispatcher as to whether or not additional help is needed.

Anytime an officer realizes that they have accidentally pressed their "Emergency" button, either on their portable radio or MDT, they shall immediately inform the Operations Dispatcher so that responding units may be called off.

## Appendix N

### Sec. 16 NON-RESPONSE RADIO PROCEDURE

All Department field units, including Supervisors and Detectives, are required to log on by two way radio or by MDT, if assigned to a vehicle equipped with an MDT, with the Operations Dispatcher within fifteen (15) minutes of the start of the tour of duty whenever the unit is working. All field units will log off with the Operations Dispatcher when relieved at the end of the unit's tour of duty by the District/Division Supervisor.

When Logged on, all units are presumed to be on the air at all times and available to respond to call from the Operations Dispatcher. If a unit goes off the air for any reason (i.e., becomes unavailable for calls), the unit will request permission from the Operations Dispatcher, giving its location and the reason. If the reason is an authorized service assignment, the unit will use the proper service assignment code. The Operations Dispatcher or Operations Dispatch Supervisor may deny any request, at their discretion, if continued availability of the unit is essential. District Supervisory personnel still wishing to utilize such units shall contact the Operations Duty Supervisor, who shall have the final say on such utilization.

### Sec. 17 RADIO RESPONSE FAILURE NOTIFICATION

When any unit fails to log on or off with the Operations Dispatcher or, if any unit fails to respond to an Operations Dispatcher after being called two (2) consecutive times, the Operations Dispatch Supervisor will be notified who shall immediately notify the Patrol Supervisor via two-way radio of the unit in question. Immediate steps shall be taken to determine whether or not that unit needs assistance or is experiencing radio difficulty.

If the non-responding unit is listed as being off on an assignment, the Patrol Supervisor, or any other unit designated by the Operations Dispatcher, shall proceed to that location and check on the safety of the officer(s) assigned to that unit. If the unit in question is not on assignment or is not at the location they are assigned to, the Operations Dispatcher shall request that all available units attempt to locate the unit in question to ensure the unit does not require assistance. Once located, the unit shall contact the Operations Division as soon as possible. Once the unit has been located and the safety of the officer(s) has been assured, the Patrol Supervisor will conduct an investigation to determine the reason for the unit failing to respond. All of the unit's two-way radios will be tested. The Patrol Supervisor will record the results of the preliminary non-response investigation on the Supervisor's activity log prior to the completion of the tour of duty.

The Operations Dispatch Supervisor will record on a Radio Response Failure Notification Form, the name and call sign of the Patrol Supervisor notified, date, District/Division and unit call sign. A copy of the Radio Response Failure Notification Form shall be forwarded, via Department mail, to the District/Division Commander or Director to take corrective action, if deemed appropriate.

Within seven days, the completed Radio Response Failure Notification Form shall be forwarded, via the chain of command, to the Auditing and Review Division, where it shall be kept on file.

## Appendix N

### Sec. 18 ACCOUNTABILITY

The Operations Division Duty Supervisor shall be responsible for ensuring full compliance with this Rule by Operations Division personnel during the assigned shift. The Operations Division Commander shall be responsible for ensuring overall compliance of this Rule.

## **Rules and Procedures**

### **Rule 331**

**March 31, 2005**

#### **Rule 331 - DIGITAL IMAGES COLLECTION, TRANSFER, and ARCHIVE PROCEDURES (D.I.C.T.A.)**

Purpose: To standardize the procedures for the collection of digital images, and their transfer to an accessible, permanent storage system. Where applicable, its provisions are effective immediately, superseding all previously issued rules, regulations, procedures, orders, directives, and training bulletins on this subject.

This standardization establishes the procedures for the use of digital photography, its duplication onto compact discs, and its storage within the ID Unit. At present, the mandatory provisions of this rule apply only to digital photographs captured to record evidence determined to be relevant to a documented incident. They do not apply to images captured for intelligence, surveillance, or tactical survey purposes, or to digital video images.

#### **Section 1. Digital Images General Considerations:**

Advancements in modern technology have created the opportunity for law enforcement to collect evidence more easily, in a more uniform manner, and to use that information more effectively for investigative and courtroom presentation purposes. It has also allowed law enforcement to manage this information more efficiently to expedite its storage and retrieval. One area where these advancements can have an immediate impact is in the way the Department captures and stores photographic images. Digital imaging has built-in advantages over film-based photography in these aspects of evidence management as well as in several other areas including cost, access, and ease of duplication. Digital cameras also allow the investigator or photographer to instantly confirm that the image he/she seeks to preserve has been properly captured.

Technology has also made it possible to enhance, alter, or manipulate digital images to aid investigative efforts. Because of the possibility that digital images may be accidentally modified, or intentionally altered for unethical purposes, it is imperative to develop procedures that protect, to the greatest degree possible, the integrity of the evidence that is collected and stored, and to allow for the authentication of the original digital image, and establish a system to monitor and document the dissemination of digital image evidence.

#### **Page Two**

#### **Section 2. Definitions:**



For purposes of this rule only, the following definitions apply:

Digital Images Collection, Transfer, and Archive Procedures (D.I.C.T.A.): A permanent system within the Identification and Photography Unit (ID Unit) of the Bureau of Professional Standards and Development, which will allow for the transfer, storage, and retrieval of digital images collected for evidentiary purposes. This system shall operate under the direction of the Commander of the ID Unit.

Digital images: An electronic photograph taken with a digital camera, that must be available in standard image format for further storage.

Digital camera: A camera that records images in digital form for storage on a memory card.

Memory card: A removable module used for storing digital images in digital cameras.

Compact disc (CD): A magnetic storage medium on which digital images are stored.

CD burner: A memory card reader that enables digital images to be copied to a CD.

Gray scale placard: A placard that includes a ruler, color scale, and space for information relative to a documented incident.

Modification: Any enhancement, alteration, or manipulation of the elements of a digital image from its original form, beyond traditional and accepted techniques commonly employed to achieve an accurate recording of an event or object.

Primary investigator: That individual designated as having primary responsibility for the investigation of an incident with the authority to make decisions relative to the conduct of the investigation.

### Section 3. Identification Unit Responsibilities:

D.I.C.T.A. Procedures Manual: The Commander of the ID Unit shall develop and establish specific, detailed procedures and protocols to implement this rule to ensure its smooth and effective functioning. Those procedures and protocols shall be incorporated into a D.I.C.T.A. Procedures Manual that shall be updated as needed and available for inspection and reference by police officers, prosecutors, defense attorneys, and judges.

D.I.C.T.A. Procedures Specialist: The Commander of the ID Unit shall designate an individual(s) as the D.I.C.T.A. Specialist(s) whose duties shall include the following:

- Become familiar with all aspects of the D.I.C.T.A. procedures including this rule and the D.I.C.T.A. Procedures Manual;
- Explain, as needed, the procedures and technical aspects, including testifying in court as a subject matter expert;

### Page Three

- Recommend appropriate modifications or upgrades to the procedures as dictated by the needs of the Department, future changes in technology, and developments in the statutory and case law governing the admissibility of digital image evidence;
- Act as liaison with all investigative units to ensure the continuous operation and proper functioning of the D.I.C.T.A. procedures; to document and report problems or irregularities; to assess training needs; to evaluate equipment suitability and performance; and to monitor compliance with the provisions of this rule.

Equipment: The Commander of the ID Unit shall establish the technical specifications for all digital cameras and other digital equipment to be used by investigators or ID Unit staff, and shall approve the models to be used or issued by the Department. This information shall be included in the D.I.C.T.A. Procedures Manual. He/she shall also ensure that all equipment is serviced and/or calibrated properly.

Training: The Commander of the ID Unit shall develop appropriate standards for the training of investigators and ID Unit staff in digital photography and the D.I.C.T.A. procedures, and shall assist the Bureau of Professional Development in establishing training curriculums and materials to implement the provisions of this rule. This information shall be included in the D.I.C.T.A. Procedures Manual.

Storage: All CD's forwarded to the ID Unit for archiving will be logged in according to established ID Unit procedures. Upon receipt of the CD, the digital information will be reviewed to ensure consistency. When digital information is confirmed, the ID Unit will electronically notify the investigator by e-mail that the CD was received, reviewed, and is in the ID Unit archives. Investigators and Investigator Supervisors will be immediately notified of any discrepancy regarding the digital information forwarded for archiving.

### Section 4. Photographer/Investigator Responsibilities:

Equipment: In the collection of photographic images having evidentiary value, investigators and ID Unit staff shall only use digital cameras, and only those issued by the Department and approved by the Commander of the ID Unit. No other medium is permitted unless exigent circumstances dictate otherwise.

However, in incidents where the Homicide Unit or Firearm Discharge Investigation Team has taken jurisdiction, film photography may also be utilized concurrently with digital photography at the discretion of a supervisor.

Collection: In routine investigative efforts, individual investigators/units shall utilize Department issued digital cameras to capture images of locations or objects having evidentiary value. At the discretion of the investigator's supervisor, the ID Unit may be requested to photograph major incidents, or those that may require more sophisticated equipment, or greater expertise or skill by the photographer.

#### Page Four

All photographers shall utilize a BPD "gray scale placard" to designate the beginning and end of the digital images created in documenting evidence in an incident. No image(s) created between the designated beginning and end of the image sequence, including tests and accidental images, shall be removed or erased. All images are electronically assigned numbers automatically and must be accounted for to ensure the integrity of the collection process.

Transfer: After the collection is completed, the primary investigator/photographer is responsible for transferring the digital images by:

1. Removing the memory card from the digital camera;
2. Placing the memory card in a CD burner (located in each district, unit, and the ID Unit) to create two (2) optical storage discs (CD):
  - a. one (1) for the investigative case file;
  - b. one (1) to be delivered by an investigator or officer to the Latent Print evidence in-take window for permanent archiving;
    - i. Using felt tip pen only, fill in the information required on the face of the CD which will include the CC#, type of incident, photographer, date/time, and number of images.
    - ii. Enter the information into the evidence management system.
    - iii. Seal the disc in its carrying case with the EMS bar-coded sticker (placing sticker in such a way as to be readable by equipment).
3. Re-formatting the memory card for subsequent use.

All digital images captured as evidence in an incident must be immediately copied from the memory card to the CDs. No other transfer, copying, or printing of the original images, as captured on the digital camera memory card, is permitted prior to copying images onto the CDs.

Retrieval: Copies of digital images for a prosecutor to use in court or to comply with discovery obligations may be obtained by the primary investigator or his/her supervisor by submitting a request to the ID Unit/Photo Room. "Read only" CDs and/or prints will be created and either mailed to the requesting officer or made available to be picked up at the Photo Lab at One Schroeder Plaza.

#### Section 5. Investigator's Supervisor Responsibilities:

The supervisor of the primary investigator has the discretion to decide whether the ID Unit should assume responsibility for photographing an incident.

Only the supervisor of the primary investigator may approve requests for release of digital images, in any form, for other than court presentation or to comply with discovery obligations.

Only the supervisor of the primary investigator may request any modifications in any digital image(s).

#### Page Five

#### Section 6. Forensic Group Units:

Digital images created by units within the BIS Forensic Group, whether in the field, or in a controlled environment such as a laboratory or studio, may be stored in the ID Unit archives (under the appropriate CC#) with the approval of the respective unit commander.

#### Section 7. Modifications:

Photographers and investigators should be prepared to authenticate that the images they introduce as evidence in court are fair and accurate representations of scenes, events, or objects, as previously viewed by them. Thus, any modifications in any digital image is strictly prohibited without the documented permission of the primary investigator's supervisor.

All modifications to any digital image must be documented on a Department form created for that purpose, and maintained in the investigative case file.

Any CD or print reflecting any modifications to any digital image shall be clearly labeled as such on the CD or print.

If the modified image is to be delivered or transferred to a court or other tribunal, a prosecutor, or a defense attorney, then a copy of the form documenting the modifications must be attached to it, as well as a copy of the original image.

Kathleen M. O'Toole  
Police Commissioner

Notes:

- Amended by SO 07-016, issued April 2, 2007, update the organization names to reflect the new BPD organizational structures. Section 3.

## Rules and Procedures

### RULE 332

August 6, 2010

#### RULE 332 - SUSPECT INTERROGATIONS - DOCUMENTATION

**Purpose:** To standardize the procedures for the documentation of suspects' interviews, especially those occurring in police facilities.

**Sec. 1 General Considerations:** The Boston Police Department seeks to ensure that the information it elicits in criminal investigations is accurate and complete. To further this goal, all members of the Department are encouraged to document statements made by victims, witnesses, and suspects. That documentation may take several forms depending on the circumstances in which it is obtained.

The Supreme Judicial Court has indicated its preference for the electronic recording of suspects' interviews if the prosecution seeks to introduce a defendant's confession or statement at trial. Failure to do so will require a judge to instruct the jury to weigh the statement made by the defendant with great caution and care, as well as to scrutinize the circumstances in which it was obtained for evidence that the statement was not voluntary. (*Commonwealth v. DiGiambattista*, 442 Mass. 423, (2004))

In order to balance the Supreme Judicial Court's preference for electronic recording of a suspect's interview with the operational needs of the department to gather and document information from suspects involved in all types and levels of crimes, and in a variety of situations, locations, and settings, it is appropriate to provide guidance to officers while maintaining sufficient flexibility to ensure that the Department continues to carry out its mission efficiently and effectively.

This Rule does not apply to interviews of individuals who are victims or witnesses but is strictly limited to interviews of persons who are, or who are likely to become, defendants in a criminal matter.

Officers are reminded that Mass. General Law Chapter 272 section 99 does not allow the recording of any individual without that person's knowledge except in very narrow circumstances with a court's permission.

**Sec. 2 Definitions:** For purposes of this special order only, the following definitions shall apply:

Electronically record: Create a permanent record by means of audio or video recording (audiotape, videotape, digital recording, or any other electronic means).

Suspect: A person who, based upon any level of suspicion, is believed to be involved in a crime.

Interview: A conversation with a suspect where it is expected that the suspect may provide incriminating information that the interrogator intends to submit into evidence in a criminal proceeding against that suspect.

Police facility: Any building utilized by a law enforcement agency for any purpose, that is under the control of the police administration, and in which the public does not have unfettered access. This may include police stations, substations, garages, offices, and other buildings, regardless of whether such building normally holds persons who have been arrested. It does not include any building in which a reasonable person would believe that he or she is free to move about without the permission of a police officer or other law enforcement agent.

**Sec. 3 Policy:** The preferred method of documenting statements made during the interview of a suspect in a police facility is to electronically record the interview. This preference shall apply regardless of whether the interview is custodial or consensual.

The decision whether to electronically record an interview of a suspect outside of a police facility should be made by the interrogator, preferably in consultation with his supervisor when feasible, and the investigator shall consider such factors such as practicability, location, permission of the suspect, and severity of the crime.

**Sec. 4 Procedure:** If the decision is made to offer a suspect the opportunity to have his/her interview electronically recorded, the interrogator shall ensure that appropriate Department forms have been completed and maintained in the case file. These forms may include but are not limited to the following:

- [Miranda warning and waiver form](#)  
(BPD Form 0078-BFS-0413)
- [Waiver of Prompt Arraignment form](#)  
(BPD Form 0003-BIS-0105)
- [Electronic Recording of Interview Refusal form](#)  
(BPD Form 0001-BIS-1204)

Interrogators shall endeavor to electronically record the original administration of all warnings and waivers.

In situations where the interview is not recorded because the suspect refuses to be electronically recorded, the interrogator must have the suspect fill out the Electronic Recording of Interview Refusal form before the interview commences. This form must also be completed by the suspect if, during the interview, (s)he decides (s)he no longer wants to be electronically recorded. If possible, the interrogator shall electronically record all warnings and waivers, along with any refusal.

In situations where the interview is not recorded from the beginning, but the suspect later elects to have the interview electronically recorded, the interrogator shall note “on tape” the time that the initial interview began and the time the suspect elected to be recorded. If the interview is

custodial, every effort shall be made to review or repeat the administration of appropriate warnings and waivers. If the initial interview was not recorded due to the suspect’s election not to be recorded, the interrogator shall review this fact “on tape”, as well as the fact that no threats, promises, inducement, or rewards were offered to the suspect prior to taping. Notes of

## Appendix P

all "off tape" statements by a suspect shall be taken and preserved in the original case file, even if duplicative of information contained in a subsequent recorded statement. If an interview is not recorded for any reason other than the refusal of the subject, such as failure of equipment, the reason(s) why the interview was not recorded must be documented in a written report. Any failure of the recording equipment, wherever situated, must be immediately reported to the Commander of the unit conducting the investigation.

**Sec. 5 Storage:** The lead investigator assigned to the case shall ensure that all electronic recordings of police interviews shall be preserved, at least until the final disposition of the criminal matter for which they were obtained. Digitally recorded audio and video police interviews shall be preserved on the server in accordance with the guidelines for the device. The investigator shall download a copy of the original digital recording file to a compact disc (CD) from the server in accordance with the guidelines for the device. This CD will now be labeled the "original" disc.

The original recording shall be labeled as such and authenticated by the interrogator with the following information:

- § Date and time recording is initiated and concluded
- § Name of person being interviewed
- § Name of all person(s) present during the interview
- § Location of interview
- § Incident report number (CC#)
- § The nature of all interruptions

All audio and video tapes and original CD's of digitally recorded interviews shall be bar-coded, logged into the BPD Evidence Management System, and stored with the case file, or in a district or unit filing system designed to accommodate electronic tapes. All video recordings of homicide interviews shall be stored in the case file in the Homicide Unit.

**Sec. 6 Duplication:** Duplicates of recordings shall be so labeled and shall include information required by Section 5. The name of a party to whom a duplicate is issued shall be noted in the case file.

**Sec. 7 Transcription:** After consultation with the Assistant District Attorney prosecuting a case, a Unit Commander may request the transcription of a recording if deemed necessary to the successful prosecution of the case. The name of a party to whom a transcript is issued shall be noted in the case file.

Note: See Special Order 04-48 issued November 8, 2004 – Documentation of Interviews of Suspects. SO 04-48 has been incorporated in its entirety into Rule 332

Edward F. Davis  
Police Commissioner





**Police Commissioner's Special Order**

Number: SO 21-54

Date: November 3, 2021

Post/Mention: Indefinite

**SUBJECT: RULE 334 – SEARCH WARRANT APPLICATION AND EXECUTION AMENDED**

Rule 334, Search Warrant Application and Execution, is hereby amended superseding all previous rules, special orders, memos and directives on this subject and is effective immediately.

Please note two new forms associated with this rule: Boston Police Search Warrant Service Checklist (Form 0155-BIS-0721) and The Search Warrant Operational Plan (Form 0156-BIS-0721).

Commanding Officers shall ensure that this order and the attached Rule are posted on Department bulletin boards.

Gregory P. Long  
Superintendent In Chief

**SEARCH WARRANT APPLICATION AND EXECUTION**

**PURPOSE:**

To ensure that the application for and execution of search warrants meet constitutional requirements and properly safeguard the rights and safety of all parties.

**Sec. 1 GENERAL CONSIDERATIONS:**

The Fourth Amendment of the Constitution of the United States and Article XIV of the Declaration of Rights of the Commonwealth of Massachusetts protect persons from unreasonable search and seizure. Except in a certain, well-defined circumstance, a warrant is required to conduct any search and/or seizure. In addition, individuals who are subject to a legal search and seizure have a right to expect that their other rights, their health and their safety will be properly safeguarded.

**Sec. 2 SEARCH WARRANT APPLICATION PROCEDURES:**

**Sec 2.1 Affiant Responsibilities:** A police officer or detective conducting an investigation who has probable cause to believe that a crime has been committed and that evidence of that crime is concealed at a specific location, may apply for a search warrant as the affiant. Per SO 18-007, in order to ensure officer safety prior to any officer or investigator, participating in any drug, organized crime, or violent crime investigation, it is required that they utilize the New England High Intensity Drug Trafficking Area (HIDTA) Investigative Support Center (ISC) and obtain a deconfliction number.

No affiant shall apply for a search warrant to any court without first seeking and obtaining the approval of his/her immediate supervisor. If at any time during the preparation of a search warrant application the affiant's immediate supervisor becomes unavailable, the affiant will immediately notify the detective unit commander who will assign a supervisor to assist the affiant.

The procedures for such application are:

- A. Review the Boston Police Search Warrant Service Checklist (Form 0155-BIS-0721) Note that not all of the items on the checklist will apply to or be necessary for every warrant. After completing a review of Boston Police Warrant Service Checklist, the affiant shall initial the form and submit it to his/her immediate supervisor when he/she submits the affidavit for approval.
- B. Complete an Initial Search Warrant Packet. Initial Search Warrant Packet shall be defined as application, search warrant, affidavit, and Boston Police Warrant Service Checklist, in accordance with the provisions of M.G.L. c.276, s. 1-7 or applicable statute and include all relevant information that the checklist indicates is both applicable and necessary. For all warrants relying upon the use of a confidential informant, the affiant shall attempt to gain additional corroboration or substantiation of information that is supplied by said informant and include such information in the affidavit if the affiant believes it is necessary.

- C. Affiant shall submit the completed Initial Search Warrant Packet to his/her supervisor for review and approval. If disapproved by the affiant's supervisor, the affiant shall conduct an additional investigation or obtain additional corroboration prior to resubmitting the Initial Search Warrant Packet to his/her supervisor for another review.
- D. Once the supervisor has approved and initialed the affidavit, have the application, affidavit, and warrant form reviewed by an Assistant District Attorney (ADA) prior to submitting it to the court through a clerk magistrate, assistant clerk magistrate or judge;
- E. If approved by the supervisor and if no changes are made following the review for probable cause and legal sufficiency by the ADA, the affiant shall submit the completed application, affidavit, and warrant form to the court.
- F. If the application, affidavit, and warrant are approved by the affiant's supervisor but not approved by the ADA then the following shall occur:
  - i. If changes are suggested by the ADA, the affiant shall review the suggested changes with his/her supervisor. If Supervisor and affiant are in concurrence, the affiant shall make the appropriate changes. Should changes be made, the affiant shall re-submit to the ADA for approval. If approved by the ADA, affiant shall submit to the court through a clerk magistrate, assistant clerk magistrate or judge; or
  - ii. If the affiant's supervisor determines that probable cause has been established and the ADA will not approve of the search warrant, the affiant's supervisor may submit the search warrant through the chain of command to his/her Bureau Chief. The Bureau Chief may direct further investigation and shall consult with a designee from the Suffolk County District Attorney's Office. After consultation with the SCDAO, the Bureau Chief has the authority make the final determination to apply for the search warrant.
- G. Affiants shall comply with the provisions of MGL Chapter 276, Section 2D:
  - (a) A warrant that does not require a law enforcement officer to knock and announce their presence and purpose before forcibly entering a residence shall not be issued except by a judge and only if the affidavit supporting the request for the warrant:
    - i. Established probable cause that if the law enforcement officer announces their presence their life or the lives of others will be endangered: and
    - ii. Includes attestation that the law enforcement officer filling the affidavit has no reason to believe that minor children or adults over the age of 65 are in the home, unless there is credible risk of imminent harm to the minor child or adult over the age of 65 in the home.
  - (b) A police officer executing a search warrant shall knock and announce their presence and purpose before forcibly entering a residence unless authorized by a warrant to enter pursuant to subsection (a).
  - (c) An officer shall not dispense with the requirements of subsection (a) and (b) except to prevent a credible risk of imminent harm as defined MGL Chapter 6E, Section 1, as serious bodily injury or death that is likely to be caused by a person with the present ability, opportunity and apparent intent to immediately cause serious physical injury or death and is a risk that, based on the information available at the time, must be instantly confronted and addressed to prevent serious bodily injury or death; provided, however, that imminent harm shall not include fear of future serious bodily injury or death.
- H. **High-Risk Warrant Approval Procedure:** A high risk warrant includes but is not limited to a "No Knock" warrant, "Nighttime" warrant and/or any search warrant entry that will be executed by the BPD SWAT Team. The approval and submission procedure for all high-risk warrants is as follows.

1. Affiant submits the search warrant application to his/her supervisor for approval. If approved;
2. The search warrant application shall be submitted to ADA for approval. If approved by the ADA;
3. The search warrant application shall be submitted through the affiant's chain of command for approval by the Bureau Chief or designee. If approved by Bureau Chief or designee;
4. Affiant shall submit the search warrant application to the court for authorization.
  - a. No Knock warrants shall only be authorized by a judge.
  - b. For nighttime search warrants and search warrants executed by the BPD SWAT the affiant should initially seek to have the warrant authorized by a judge. If authorization by a judge is not feasible, the affiant shall seek authorization from a clerk or clerk-magistrate.

In the event of exigent circumstances, the BIS chain of command may be bypassed and the search warrant submitted directly to the BIS bureau chief or designee.

Approval for such warrants will be based on circumstances identified in the Boston Police Warrant Service Checklist, including but not limited to a history of violence, persons known or suspected to be in the location, environmental factors of the location and/or the presence of firearms is reasonably suspected. Citizen and officer safety shall be given the utmost consideration in the approval and execution process.

Search Warrants for evidence in locations already secured by the Boston Police Department will not be considered "high-risk" and do not apply in this section.

**Sec 2.2 Supervisor Responsibilities:** The immediate supervisor of the affiant is responsible for reviewing and approving the content of all Initial Search Warrant Packets.

- A. To ensure that the review process is thorough and complete and that the affidavit contains all relevant information, the supervisor shall refer to the Boston Police Search Warrant Service Checklist appearing on BPD Form 0155-BIS-0721 when evaluating the information contained in affidavits submitted for review. It should be noted that not all items in the checklist will apply to every warrant and that some items may not be necessary.
- B. The supervisor shall ensure that affidavits meet the following criteria:
  - I. Establish that probable cause exists to believe that a crime has been committed and that the place to be searched and items to be seized are located in the place specified in the affidavit;
  - II. Include enough information to allow an individual, not previously connected to the investigation, to properly identify the place or premises to be searched and the item(s) to be seized. Specific entry location documentation or evidence shall be included.
  - III. Include information that establishes both the basis of knowledge and the veracity (credibility or reliability) of an informant/source of information, as determined by Rule 333, for all warrants relying on the use of such informant, or include additional substantiation or corroboration to make up for any deficiencies in establishing the informant's basis of knowledge or veracity. The affiant shall ensure the informant is not disqualified per Rule 333, Sec. 4.

- C. Supervisors shall ensure that the Initial Search Warrant Packet seeking "No Knock" warrants, "Nighttime" warrants, "Anticipatory" warrants and warrants to search "All Persons Present" are adequately and properly supported.
- D. Affidavits that a supervisor deems insufficient shall be returned to the affiant who shall be instructed to seek additional investigation and/or corroboration prior to resubmitting the affidavit for another review.
- E. If an affiant has had an affidavit returned for insufficiency by his/her supervisor and is not successful in attempts to obtain additional corroboration, the affidavit may be resubmitted, through the supervisor, to be considered for approval by the Detective Supervisor Commander. Affiant must inform Detective Supervisor Commander that this affidavit has been previously submitted and denied. In such cases, only the Detective Supervisor Commander may approve such affidavit.
- F. The supervisor shall instruct the affiant to contact an ADA to review the application, affidavit, and warrant form for approval prior to submitting the affidavit to the court.
- G. The supervisor shall instruct the affiant to submit the application for the search warrant to the court, if no changes are made following review by the ADA. Should changes be necessary, see section 2.1.F for appropriate procedure.
- H. Upon being informed by the affiant that a search warrant has been granted, the supervisor shall notify the Detective Unit Commander (if unavailable, an on-duty Bureau Chief or designee), who shall ensure that a detective superior officer is present and in charge of the search.
- I. The supervisor assigned to the search warrant shall submit the Search Warrant Operational Plan (Form 0156-BIS-0721) and Boston Police Warrant Service Checklist, to his immediate supervisor detailing the names of the officers assigned to the search team, their specific duties/responsibilities and all pertinent information regarding the date, time, location of the search, the name(s) and criminal histories of the target(s) and special considerations which may arise pertaining to other persons who may be present during the warrant execution and other potential hazards such as animals.

**Sec 2.4 Special Operations Division Commanders Responsibilities:** The Commanding Officer of the Special Operations Division or designee is responsible for establishing, maintaining and updating procedures utilized by the Boston Police SWAT Team; the Commander will also ensure that no person shall be assigned to the SWAT Team without first being trained in such procedures.

### **Sec. 3 SEARCH WARRANT EXECUTION PROCEDURES:** **Execution Considerations**

#### **Sec. 3.1 Execution Considerations**

- A. The primary responsibility of all members of the department involved in the execution of search warrants is the preservation of life and the safety of all individuals involved.
- B. Every search warrant executed by the Department will comply with the method of execution, every search warrant executed will comply with all applicable sections of Rule 334 and include all the required documents of the Search Warrant Packet. Every supervisor responsible for the execution of a search warrant will ensure their personnel are in compliance with this rule, all City Ordinances and laws of the Commonwealth, to include MGL Chapter 276, Section 2D.
- C. All search warrants shall be executed by a minimum of one supervisor and six officers, with the exception of administrative and evidentiary warrants (see Section 4) and high-risk warrants, see Section 2.1 H.

- D. The affiant and affiant's supervisors shall conduct an initial review based on factors identified in the Search Warrant Service Checklist, to determine the appropriate resources to execute the entry.

Factors to be considered include:

- A. physical description of the target location (including details of primary entry and additional points of entry); and
  - B. information concerning the person(s) occupying the premises and
  - C. their propensity for violence and
  - D. presence of firearms and
  - E. any other safety concerns.
  - F. Citizen and officer safety shall be given the utmost consideration in the approval and execution process.
- E. The supervisor in charge of the entry/search shall prepare a Search Warrant Operational Plan and determine how entry is to be made. The decision to utilize the Boston Police SWAT Team should be guided by the totality of information gathered by the affiant, to include the Boston Police Warrant Service Checklist.
- F. The Boston Police SWAT Team shall be utilized if:
- 1. The target or occupants of the residence being entered have a recent and/or relevant history of firearms on their record;
  - 2. The investigation reveals information that would make the affiant reasonably suspect a firearm may present a risk to the search team and occupants of the residence;
  - 3. The Boston Police SWAT Team should be utilized whenever a supervisor reasonably suspects there could be a threat to the safety of anyone involved in the entry and search of the location.
- G. If the supervisor determines the Boston Police SWAT Team should be utilized then the Bureau Chief shall be notified at least 48 hours in advance of the execution of the warrant. If 48 hours advance is not possible, notification will be as soon as practicable

All search warrant executions utilizing the SWAT Team will be considered "High Risk" and need to be authorized by affiant's Bureau Chief prior to execution (see 2.1, Sec. H).

### **Sec 3.2 Search Warrant Pre-search Briefing Requirements:**

The Search Warrant Operational Plan (Form 0156-BIS-0721) shall be completed prior to any search warrant briefing and search warrant execution.

The pre-search briefing shall be held by the supervisor in charge of the entry/search and the affiant shall be present. A District or Unit Supervisor of the affiant must attend the pre-search briefing.

At the pre-search briefing, the affiant's supervisor or supervisor in charge of the entry/search shall make a detailed presentation of all relevant information. The briefing should include the incident number, summary of the investigation and its objectives; a copy of the Search Warrant Operational Plan; a review of the physical description of the target location (including details of primary entry and additional points of entry); and information concerning the person(s) occupying the premises and their propensity for violence, presence of firearms and any other safety concerns.

Affiant's supervisor must ensure information is clearly articulated as to allow an individual not previously connected to the investigation to properly identify the place or premises to be searched and the item(s) to be seized.

The supervisor in charge of the search shall ensure that the Search Warrant Operational Plan details the roles, the call signs, the assignments and the responsibilities of each member of his or her team.

With the exception of evidentiary search warrants, the supervisor in charge of the search shall ensure the presence of at least one (1) supervisor and six (6) officers at the search during the pre-search briefing. Unless necessary for the integrity of an investigation or surveillance needs, a uniformed officer shall accompany the search team during execution.

Personnel issued body worn cameras shall wear and activate their BWCs prior to entry and in compliance with Rule 405. Once the scene is secure, the supervisor in charge of entry may order officers to deactivate their cameras.

**Sec. 3.3 Search Warrant Day of Briefing:** On the day of any Search Warrant Execution, the supervisor in charge of the search shall ensure that the Search Warrant Operational Plan details the roles, the call signs, the assignments and the responsibilities of each member of the non-SWAT entry and search teams.

- No officer may participate in the entry unless they attend the pre-search briefing on the day of or 24 hours before, except in exigent circumstances and only after being cleared by the supervisor in charge of the search. If clearance has been granted, a verbal briefing for the officer prior to entry is required.
- Every member of the entry and search teams will be shown a copy of the Search Warrant Operational Plan at the pre-search briefing and/or briefed by the affiant on the operational plan.
- Except for those using subterfuge to gain entry, all personnel not in uniform shall wear Department approved outer most garment marked to clearly identify individuals as Boston Police officers.
- All personnel issued a BWC shall activate the BWC, unless attempting subterfuge to gain entry.
- All personnel participating in the entry shall wear Department issued body armor.
- Personnel shall not wear any mask or face cover, unless authorized by Supervisor on scene.

**Section 3.4 SWAT Team Search Warrant Pre-Search Briefing Requirements:** If the SWAT Team is authorized, a SWAT Team Briefing shall be held prior to execution. Members of this meeting shall include the SWAT Team, the affiant, the affiant's supervisor and/or the affiant's unit/district supervisor.

At the SWAT Team Briefing, the affiant's supervisor with the assistance of the affiant, shall make a detailed presentation of all relevant information. The briefing should include a summary of the investigation and its objectives; a copy of the Search Warrant Operational Plan; a review of the physical description of the target location (including details of primary entry and additional points of entry); and information concerning the person(s) occupying the premises and their propensity for violence and any other safety concerns.

The SWAT Team supervisor in charge of the entry shall ensure that the Search Warrant Operational Plan details the roles, the call signs, the assignments and the responsibilities of each member of the entry and search teams.

### **Sec 3.5 Search Warrant Entry Procedures:**

At entry, the affiant's supervisor shall then notify operations of a Code 11. Unless operational considerations or a need for secrecy mandate otherwise, the affiant's supervisor shall notify the Operations Duty Supervisor prior to the entry.

- A. The affiant or designee shall take all steps necessary to ensure the entry personnel are entering the proper premises to be searched. When the premise to be entered and searched is an individual unit in a multi-unit dwelling, the affiant shall point out to entry personnel the particular unit to be entered and searched.
- B. If the unit to be entered and searched does not include precise detailing necessary for the entry team, the affiant is responsible for confirmation for the location of entry. The affiant may wear body armor and must specifically identify the correct location to enter for SWAT personnel on scene. If multiple locations are being searched simultaneously, affiant's supervisor will designate personnel to confirm location of entry. Affiant supervisor will ensure designee has sufficient knowledge of target location prior to entry.
- C. Affiant, affiant designee, or any entry supervisor, may halt entry at any point prior to entry. The affiant supervisor and supervisor in charge of entry shall determine further course of action.
- D. Affiant supervisor and supervisor in charge of entry will coordinate communication during entry.
- E. Entry to the premises shall be made by the entry personnel or the Boston Police SWAT Team. Until such time as entry is made and the premises are declared secure, command and control of the premise rests with the supervisor of the entry personnel or, when utilized, the SWAT Team. Where the SWAT Team is not utilized, the supervisor in charge of the entry personnel and the supervisor in charge of the search may be the same person.
- F. Entry personnel are responsible for:
  - i. Containment of the area perimeter and target structure(s);
  - ii. Effecting entry to the target location;
  - iii. Gaining control of all persons inside the target location using that amount of force as is reasonably necessary;
  - iv. Conducting a protective sweep of the premises
  - v. Frisking individuals pursuant to the warrant or when reasonable suspicion is present at the target location for weapons and, if appropriate,
  - vi. Detaining all suspects at a central location; and
  - vii. Preventing the destruction of evidence.

When entry is made by force, damages should be kept to a minimum to facilitate securing the premises after the search is complete.

Once the premises have been declared secure, the supervisor in charge of the entry personnel shall relinquish command and control of the premises and turn that responsibility over to the supervisor in charge of the search, if applicable.



### **Sec. 3.6 Search Procedures:**

- A. Once the premises have been declared secure and prior to initiating the search, the supervisor in charge of the search or designee shall photograph or video the premise, specifically noting any pre-existing damages or damages caused during the entry.
- B. Upon initiating the search, the supervisor in charge of the search will ensure that all search personnel continue with their pre-assigned duties (i.e., perimeter security; prisoner control; evidence officer; search teams etc.) unless reassigned.
- C. Perimeter security personnel are responsible for:
  - i. Ensuring that no unauthorized persons escape from or enter the premises while the search is being conducted;
  - ii. Recovering any evidence thrown from the premises; and
  - iii. Remaining on their posts until ordered otherwise by the supervisor in charge of the search, or unless exigent circumstance arise; and
  - iv. Remaining outside the premises until ordered to enter by the supervisor in charge of the search, or in the case of an emergency.
- D. Prisoner control personnel are responsible for:
  - i. Ensuring that all persons being detained but not placed under arrest are held in a central location, using that amount of force or restraint reasonably necessary;
  - ii. Ensuring that all persons have been frisked for weapons, if appropriate, and that persons being placed under arrest have been properly searched;
  - iii. Documenting all persons found inside the premises; and
  - iv. Ensuring that all persons placed under arrest are transported to designated District for booking;
  - v. Supervisor in charge will ensure a member of the primary execution team remains with all persons placed under arrest throughout booking at the district, when feasible.
- E. Search team personnel are responsible for:
  - i. Searching all persons present inside the target location, when permitted by the warrant;
  - ii. Conducting a complete and thorough search of all areas specified by the warrant and assigned to them by search team supervisor;
  - iii. Notifying the evidence officer when any weapons, money, evidence or contraband is found; and
  - iv. After the evidence officer has noted its location, bagging and marking the weapons, money, evidence and contraband for identification and delivering same to the evidence officer for safekeeping.
- F. Evidence officers are responsible for:
  - i. Noting the names of the officers that are assigned to search individual rooms;
  - ii. Noting, sketching, and/or photographing the interior of the premise and location of any evidence found and the names of the officers who found it; and
  - iii. Taking custody of any weapons, money, evidence and contraband for safekeeping in accordance with existing Department procedures and the following rules and/or orders:

- a. Weapons – Rule 311, Ballistics Procedures and Special Order 91-11, Fingerprint Examination of Firearms;
- b. Money – Rule 309A, Handling and Disposition of Seized Money

The duties of other personnel with special assignments, such as pre-raid and post-raid surveillance personnel, will vary and will be defined within the Search Warrant Operational Plan.

G. The supervisor in charge of the search is responsible for:

- i. Ensuring that all personnel carry out their assigned duties;
- ii. Counting all found money not seized as evidence in the presence of at least one other officer and the person claiming ownership at the search location, when feasible. The supervisor in charge of the search shall obtain a receipt from the person to whom the money is given. Supervisor shall record the time and amount of money given to the person claiming ownership
- iii. Whenever it is not possible to count seized money at the search location, the supervisor in charge shall ensure the affiant's incident report includes an explanation as to why. The money shall then be secured, transported directly to a BPD facility by two (2) sworn officers, and counted as soon as practicable.
- iv. Ensuring that all weapons, money, evidence and contraband has been accounted for, properly marked for identification, transported to the respective District or Unit and handled in accordance with applicable Department procedures;
- v. Ensuring that all prisoners are transported to the designated District station for prisoner processing;
- vi. Ensuring post-search photos or video images are taken;
- vii. Ensuring that the premises are properly secured, if left vacant after the search has been completed.
- viii. Ensuring a copy of the search warrant is left at the premise.

**Sec. 3.7 Wrong Premises Entry:** In the event that the supervisor determines that the wrong premises have been entered, the search shall immediately terminate.

The affiant's supervisor shall ensure the safety of all affected occupants and immediately notify Operations and EMS, as necessary. Affiant's supervisor shall ensure notification to the legal owners and/or occupants of the premise is made.

Operations Duty Supervisor shall then make notifications to:

- 1. Affiant's District / Unit Commander
- 2. District/Unit Commander of search warrant location
- 3. Affiant's Bureau Chief or designee
- 4. BFS Bureau Chief
- 5. Internal Affairs

Affiant's supervisor will make effort will also ensure an incident report, subsequent Form 26, and photos of all damage to the wrong premises (with consent of occupant) are made and retained.

In all such cases, the supervisor shall submit copies of all written reports and photos on the entire operation to the affiant's Bureau Chief or designee.

**Sec. 3.8 Post Search Procedures:**

A. The supervisor in charge of the search shall be responsible for:

- i. Ensuring that all necessary reports and documentation are completed and that such reports are thorough and accurate;
- ii. Ensuring that all evidence that is seized are recorded on the return of the search warrant.
- iii. Ensuring all evidence that is seized is recorded on the affiant's incident report, unless restricted by court order or at the direction of the affiant's supervisor.
- iv. Ensuring that the completed search warrant is returned to the court within seven (7) days of issuance;
- v. Ensuring that all controlled substances seized are secured in the proper safe or storage area until transported to the Evidence Management Division.
- vi. Ensuring that all firearms seized are properly stored until they are transported to the Ballistics Unit in accordance with the provisions of Rule 311;
- vii. Ensuring that a Seized Money Forms are completed. BPD Form 2292B shall be completed for all drug money seized or BPD Form 2292A shall completed for all other money seized;
- viii. Ensuring all money is properly secured until transported to the custody of the Financial Evidence Officer in accordance with the provisions of Rule 309A, Handling and Disposition of Seized Money;
- ix. Ensuring that all other evidence is handled in accordance with applicable Department procedures;
- x. A post-search debriefing session with the members of the search team for the purpose of enhancing the efficiency of future operations shall be held by the on-scene supervisor;
- xi. Maintaining a complete file of all documents associated with the search warrant and execution; and
- xii. When mandated by the law, direct the completion of forms related to child abuse or neglect and/or elder abuse or neglect.

The supervisor in charge of the Boston Police SWAT Team, if utilized, shall be responsible for submitting an after-action report, through channels, to the Bureau Chief of Field Services or designee.

To the maximum extent possible the above policies and procedures shall be adhered to with respect to the execution of all searches, with or without a warrant.

**Sec. 4 EVIDENTIARY SEARCH WARRANTS:** At the discretion of the supervisor in charge of the search, search warrants that are being executed for the sole purpose of gathering evidence or fruits of a crime, where there is no anticipated possibility of a confrontation, may be conducted with one detective supervisor and at least one other sworn officer. Evidentiary Search Warrants, including but not limited to motor vehicles, technology, cellphones, do not require a HIDTA Conflict Check or Search Warrant Checklist. Evidentiary Search Warrants do require a Search Warrant Operational Plan only as applicable.

**Sec. 5 OUTSIDE AGENCIES:** Outside agencies seeking the assistance of the Department in the execution of their search warrants shall be directed to contact the appropriate District Detective Supervisor or Specialized Unit Supervisor who shall determine the appropriate unit to provide the necessary assistance and the level of assistance to be provided. The appropriate District Detective Supervisor or Specialized Unit Supervisor must notify their Bureau Chief or designee.

Any BPD personnel participating in outside agency search warrants must comply with the BPD Rules and Procedures.

The Boston Police SWAT Team may be utilized to assist outside agencies only with the permission of Chief, Bureau of Field Services or designee.

**Sec. 6 SEARCHES CONDUCTED OUTSIDE THE CITY OF BOSTON:** Boston officers attempting to serve a search warrant outside the City of Boston shall notify their Bureau Chief or designee through their chain of command prior to the execution of the search warrant. Officers shall contact the local police department wherein the search target is located and seek their assistance in serving the warrant. If there is a conflict between the policies and procedures mandated by this rule and the policies and procedures of the local police department, the affiant's Bureau Chief or designee shall be notified of the conflict prior to execution. Regardless of any conflict, exceptions to Rules 303 and 304 are prohibited and these rules will be adhered to by all members of the Boston Police Department in the event necessary during a search warrant execution.

#### **Sec 7. FINAL SEARCH WARRANT PACKET:**

Once a search warrant is executed, a copy of a Final Search Warrant packets shall be scanned and sent electronically to the Bureau of Investigative Services and to the Unit or District Commander where the search warrant is executed within two weeks.

Scanned Final Search Warrant Packet will be saved on the BIS server with the file name that reflects "Address\_Subject Name\_Date\_Incident Number"

Final Search Warrant Packets will include:

- Incident Number
- The Search Warrant Operational Plan
- Boston Police Search Warrant Service Checklist
- Supervisor Search Warrant Checklist
- Search Warrant Return

ADDENDUM A: Boston Police Search Warrant Service Checklist (Form 0155-BIS-0721)

ADDENDUM B: The Search Warrant Operational Plan (Form 0156-BIS-0721)

Gregory P. Long  
Superintendent In Chief



# BOSTON POLICE DEPARTMENT

## Warrant Service Checklist

This checklist is not to be used rigidly. All affiants and/or affiant supervisors are to use this as a gauge and to add their experience and training when identifying any factors that may impact the service of search warrants at a residence or commercial location.

### SUSPECT FACTORS

Any "yes" answers require further explanation in the notes section below.

Has a BOP/III been run on the suspect?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
Known to use or has propensity for violence:	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
• Homicide	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
• Armed Robbery	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
• Assault	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
• Resisting Arrest	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
• Assault on Police Officer	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
• Other:	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
Is suspect on probation or parole?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
Is suspect a substance (drug/alcohol) abuser?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
• If yes, what types?			
Is the suspect aware that there is a high likelihood of lengthy incarceration if he/she is arrested?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
Is the suspect wanted?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
Does the suspect have a history of mental illness?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
• If yes, describe the condition?			
• From where was the information obtained?			
Is suspect suicidal?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
• Performed a MA Suicide Check (Q5) on CJIS?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
Does the suspect have military/police background?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
• If yes, describe branch of service/department, length of service, specialties, etc.			
Have specific threats of violence been made against police officers?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
Has specific threats of violence been made against others?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown

Has the suspect been the target of a search warrant in the past?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
Is the suspect currently/historically associated with an organization which is known or suspected of violent criminal behavior?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
<ul style="list-style-type: none"> <li>• If yes, what group or organization?</li> </ul>			
<ul style="list-style-type: none"> <li>• Can the organization be classified as:</li> </ul>			
· Paramilitary	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
· Terrorist	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
· Religious Extremist	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
· Gang	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
· Other:	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown

Provide further explanation/details regarding any/all affirmative answers.

**NOTES:**

---

## OFFENSE FACTORS

Is the offense a felony?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
<ul style="list-style-type: none"> <li>• If yes, list the offense:</li> </ul>			
Is the offense a violent felony?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
Was a weapon used in the commission of the offense?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
Were victims injured during the commission of the offense?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
Was/were an officer(s) injured, due to an assault, during the commission of the offense?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown

Provide further explanation/details regarding any/all affirmative answers.

**NOTES:**

---

# WEAPON ASSESSMENT

Does the suspect have prior gun charges? ☐ Yes ☐ No ☐ Unknown

- If yes, what year(s)?

Does the suspect have prior gun convictions? ☐ Yes ☐ No ☐ Unknown

- If yes, what year(s)?

Is suspect known or believed to possess a weapon? ☐ Yes ☐ No ☐ Unknown

- If yes, what type(s)?

Is the location of possible weapons known? ☐ Yes ☐ No ☐ Unknown

- Where?

Has an LTC check on the location and all persons known to be present been completed? ☐ Yes ☐ No ☐ Unknown

*Provide further explanation/details if necessary.*

## NOTES:

---

# SITE ASSESSMENT

Photographs of the target location? ☐ Yes ☐ No ☐ Unknown

Photographs of the front and rear target location doors? ☐ Yes ☐ No ☐ Unknown

Photographs of the front and rear main doors of a multi unit building? ☐ Yes ☐ No ☐ Unknown

What types of doors are on the target location (wood/metal, number types of locks)?

What types of doors are on the main entrances if it's a multi unit building (wood/metal, number types of locks)?

Floor plan to the target location if known? ☐ Yes ☐ No ☐ Unknown

Does the target locations have access to the roof? ☐ Yes ☐ No ☐ Unknown

Does the target locations have access to the basement? ☐ Yes ☐ No ☐ Unknown

Does the target locations have access to a crawlspace? ☐ Yes ☐ No ☐ Unknown

Has the target location been the target of prior search warrants or incidents (photos, sketches etc.) ☐ Yes ☐ No ☐ Unknown

What is the past criminal history for the target location?

Are there geographic barriers/hazards or other considerations? ☐ Yes ☐ No ☐ Unknown

- If yes, describe: (May include upstairs apartments or rooms, terrain features, etc.)

Is the site fortified?

☐ Yes ☐ No ☐ Unknown

- If yes, describe: (May include barricaded doors/windows, burglar bars, etc.)

Does the site have counter surveillance personnel or monitoring devices (CCTV/alarms)?

☐ Yes ☐ No ☐ Unknown

- If yes, describe:

Are counter surveillance personnel armed and present?

☐ Yes ☐ No ☐ Unknown

Do we know of neighboring relatives or friends of the target close by?

☐ Yes ☐ No ☐ Unknown

- If yes, where?

Are additional adults likely to be present?

☐ Yes ☐ No ☐ Unknown

- If yes, how many?

Do we know the criminal history of other people present?

☐ Yes ☐ No ☐ Unknown

Do we know the criminal history connected to the target location?

☐ Yes ☐ No ☐ Unknown

Are additional adults likely to be present who present a threat or are likely to be hostile to police?

☐ Yes ☐ No ☐ Unknown

Dogs/pets present that are likely to be vicious or require additional personnel or equipment to safely contain?

☐ Yes ☐ No ☐ Unknown

Children/Elderly/Disabled person(s) on site?

☐ Yes ☐ No ☐ Unknown

Do we know the medical history of people present?

☐ Yes ☐ No ☐ Unknown

Chemicals/Lab on site? If yes, has Commander of Drug Control Unit been notified?

☐ Yes ☐ No ☐ Unknown

Provide further explanation/details regarding any/all affirmative answers.

## NOTES:



---

## WARRANT PARTICULARS

Are all of the necessary details to support a no knock, nighttime entrance and/or all persons present request included in the affidavit?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
Has a DA approved the affidavit?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
Has a Detective Supervisor approved the affidavit?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
Has the warrant been signed by a clerk/justice?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
Does the warrant authorize:	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
• No Knock Entrance	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
• If yes: BIS COMMAND APPROVAL (Signature and Date)			
• Nighttime Entrance	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
• All Person Present	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown

---

## DECONFLICTION

Has HIDTA been notified: (978.451.3900)	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Deconfliction #:	Expiration:	

*Provide further explanation/details regarding any/all affirmative answers.*

**NOTES:**

---

## ASSESSMENT CHANGES AT TIME OF EXECUTION

Assessment Changes at time of execution	<input type="checkbox"/> Yes	<input type="checkbox"/> No
---	------------------------------	-----------------------------

*Provide further explanation/details regarding any/all affirmative answers.*

**NOTES:**

Affiant Signature: \_\_\_\_\_ ID #: \_\_\_\_\_

Supervisor Signature: \_\_\_\_\_ ID #: \_\_\_\_\_

SWAT REQUESTED?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
-----------------	------------------------------	-----------------------------



# BOSTON POLICE DEPARTMENT

## Search Warrant Operational Plan

Operation Name: \_\_\_\_\_ Date: \_\_\_\_\_ Time: \_\_\_\_\_

Target Location: \_\_\_\_\_

Affiant Name/Assignment: \_\_\_\_\_ Contact # \_\_\_\_\_

Warrant Execution Supervisor: \_\_\_\_\_ Contact # \_\_\_\_\_

CC#: \_\_\_\_\_ HIDTA #: \_\_\_\_\_ BPD District: \_\_\_\_\_

Prosecutor: \_\_\_\_\_ Contact #: \_\_\_\_\_ ☐ ADA ☐ AAG ☐ AUSA

Search Warrant Issuing Court: \_\_\_\_\_ Warrant #: \_\_\_\_\_

Type of Warrant:

☐ Knock & Announce

☐ Day

☐ No Knock

☐ Night (10 p.m. – 6 a.m.)

Briefing Location: \_\_\_\_\_ Briefing Time: \_\_\_\_\_

Staging/Command Post Commander: \_\_\_\_\_ Contact # \_\_\_\_\_

Controlled Delivery of:

☐ Weapons ☐ Cocaine ☐ Heroin ☐ Marijuana ☐ Pills (type) \_\_\_\_\_

☐ Other: \_\_\_\_\_

Types Of Premises:

☐ Residential Single

☐ Residential Multi Unit

☐ Other: \_\_\_\_\_

☐ Commercial Retail

☐ Commercial Warehouse/Storage

☐ Commercial Office

☐ Institutional

☐ Vehicle

☐ Social Club

Additional Description: \_\_\_\_\_

# TARGET LOCATION

Photos Attached (printed 8" x 10"; affiant must label offender/address on each photo)

Target Address \_\_\_\_\_

Children Present:	<input type="checkbox"/> Yes <input type="checkbox"/> No	Elderly Present:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Medical/Disabled Handicap:	<input type="checkbox"/> Yes <input type="checkbox"/> No	Vehicle Traffic Difficulties:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Animals:	<input type="checkbox"/> Yes <input type="checkbox"/> No	High Crime Area:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Foot Traffic:	<input type="checkbox"/> Yes <input type="checkbox"/> No	Drugs Present at Location:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Approach Difficulties:	<input type="checkbox"/> Yes <input type="checkbox"/> No	Close Proximity to School:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Firearms/Weapons present at location:	<input type="checkbox"/> Yes <input type="checkbox"/> No	Counter Surveillance:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Chemical Bio Hazard:	<input type="checkbox"/> Yes <input type="checkbox"/> No	Physical Fortification :	<input type="checkbox"/> Yes <input type="checkbox"/> No
Video Surveillance:	<input type="checkbox"/> Yes <input type="checkbox"/> No	Prior Search Warrants Executed:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Photo of Target:	<input type="checkbox"/> Yes <input type="checkbox"/> No	Criminal History of Address:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Criminal History of all Persons Present:	<input type="checkbox"/> Yes <input type="checkbox"/> No	Abutting Address Concerns:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Photo(s) of Location:	<input type="checkbox"/> Yes <input type="checkbox"/> No	Video of Property:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Geographic Barrier:	<input type="checkbox"/> Yes <input type="checkbox"/> No	Floor plan, if possible:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Access to Roof:	<input type="checkbox"/> Yes <input type="checkbox"/> No	Access to Crawlspace:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Access to Basement :	<input type="checkbox"/> Yes <input type="checkbox"/> No	Type of Door:	

Additional Information \_\_\_\_\_

## CASE BACKGROUND

## CASE OBJECTIVE

# OFFENDER/SUSPECT INFORMATION

Photos Attached (printed 8x10; must label offender/address on each photo)

Suspect Name: \_\_\_\_\_

Suspect Address: \_\_\_\_\_ Cell Phone: \_\_\_\_\_

Age:	DOB:
Height:	Weight:
Eyes:	Hair:

Scars	<input type="checkbox"/> Yes <input type="checkbox"/> No	Tattoos	<input type="checkbox"/> Yes <input type="checkbox"/> No
Facial Hair	<input type="checkbox"/> Yes <input type="checkbox"/> No	Beard	<input type="checkbox"/> Yes <input type="checkbox"/> No
Mustache	<input type="checkbox"/> Yes <input type="checkbox"/> No	BOP	<input type="checkbox"/> Yes <input type="checkbox"/> No
History of Violence	<input type="checkbox"/> Yes <input type="checkbox"/> No	History of Violence toward LE	<input type="checkbox"/> Yes <input type="checkbox"/> No
Felony Arrest	<input type="checkbox"/> Yes <input type="checkbox"/> No	Felony Convictions	<input type="checkbox"/> Yes <input type="checkbox"/> No
Suspect known to have firearm	<input type="checkbox"/> Yes <input type="checkbox"/> No	Suspect Wanted	<input type="checkbox"/> Yes <input type="checkbox"/> No
Suspect on Parole	<input type="checkbox"/> Yes <input type="checkbox"/> No	Suspect on Probation:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Suspect known to have mental health issue:	<input type="checkbox"/> Yes <input type="checkbox"/> No	Q5:	<input type="checkbox"/> Yes <input type="checkbox"/> No

Additional Description: \_\_\_\_\_


## OFFENDER/SUSPECT VEHICLE(S)

Vehicle Make	Vehicle Model	Vehicle Color(S)	Vehicle Registration

**ADDITIONAL PERSON(S) PRESENT**

Name: \_\_\_\_\_

Address: \_\_\_\_\_ Cell Phone: \_\_\_\_\_

**ADDITIONAL OFFENDER / SUSPECT?**

Age:	DOB:
Height:	Weight:
Eyes:	Hair:

Scars	<input type="checkbox"/> Yes <input type="checkbox"/> No	Tattoos	<input type="checkbox"/> Yes <input type="checkbox"/> No
Facial Hair	<input type="checkbox"/> Yes <input type="checkbox"/> No	Beard	<input type="checkbox"/> Yes <input type="checkbox"/> No
Mustache	<input type="checkbox"/> Yes <input type="checkbox"/> No	BOP	<input type="checkbox"/> Yes <input type="checkbox"/> No
History of Violence	<input type="checkbox"/> Yes <input type="checkbox"/> No	History of Violence toward LE	<input type="checkbox"/> Yes <input type="checkbox"/> No
Felony Arrest	<input type="checkbox"/> Yes <input type="checkbox"/> No	Felony Convictions	<input type="checkbox"/> Yes <input type="checkbox"/> No
Suspect known to have firearm	<input type="checkbox"/> Yes <input type="checkbox"/> No	Suspect Wanted	<input type="checkbox"/> Yes <input type="checkbox"/> No
Suspect on Parole	<input type="checkbox"/> Yes <input type="checkbox"/> No	Suspect on Probation:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Suspect known to have mental health issue:	<input type="checkbox"/> Yes <input type="checkbox"/> No	Q5:	<input type="checkbox"/> Yes <input type="checkbox"/> No

Additional Description: \_\_\_\_\_

---

---

**ADDITIONAL PERSON(S) PRESENT**

Name: \_\_\_\_\_

Address: \_\_\_\_\_ Cell Phone: \_\_\_\_\_

**ADDITIONAL OFFENDER / SUSPECT?**

Age:	DOB:
Height:	Weight:
Eyes:	Hair:

Scars	<input type="checkbox"/> Yes <input type="checkbox"/> No	Tattoos	<input type="checkbox"/> Yes <input type="checkbox"/> No
Facial Hair	<input type="checkbox"/> Yes <input type="checkbox"/> No	Beard	<input type="checkbox"/> Yes <input type="checkbox"/> No
Mustache	<input type="checkbox"/> Yes <input type="checkbox"/> No	BOP	<input type="checkbox"/> Yes <input type="checkbox"/> No
History of Violence	<input type="checkbox"/> Yes <input type="checkbox"/> No	History of Violence toward LE	<input type="checkbox"/> Yes <input type="checkbox"/> No
Felony Arrest	<input type="checkbox"/> Yes <input type="checkbox"/> No	Felony Convictions	<input type="checkbox"/> Yes <input type="checkbox"/> No
Suspect known to have firearm	<input type="checkbox"/> Yes <input type="checkbox"/> No	Suspect Wanted	<input type="checkbox"/> Yes <input type="checkbox"/> No
Suspect on Parole	<input type="checkbox"/> Yes <input type="checkbox"/> No	Suspect on Probation:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Suspect known to have mental health issue:	<input type="checkbox"/> Yes <input type="checkbox"/> No	Q5:	<input type="checkbox"/> Yes <input type="checkbox"/> No

Additional Description: \_\_\_\_\_

---

---

**ADDITIONAL PERSON(S) PRESENT**

Name: \_\_\_\_\_

Address: \_\_\_\_\_ Cell Phone: \_\_\_\_\_

**ADDITIONAL OFFENDER / SUSPECT?**

Age:	DOB:
Height:	Weight:
Eyes:	Hair:

Scars	<input type="checkbox"/> Yes <input type="checkbox"/> No	Tattoos	<input type="checkbox"/> Yes <input type="checkbox"/> No
Facial Hair	<input type="checkbox"/> Yes <input type="checkbox"/> No	Beard	<input type="checkbox"/> Yes <input type="checkbox"/> No
Mustache	<input type="checkbox"/> Yes <input type="checkbox"/> No	BOP	<input type="checkbox"/> Yes <input type="checkbox"/> No
History of Violence	<input type="checkbox"/> Yes <input type="checkbox"/> No	History of Violence toward LE	<input type="checkbox"/> Yes <input type="checkbox"/> No
Felony Arrest	<input type="checkbox"/> Yes <input type="checkbox"/> No	Felony Convictions	<input type="checkbox"/> Yes <input type="checkbox"/> No
Suspect known to have firearm	<input type="checkbox"/> Yes <input type="checkbox"/> No	Suspect Wanted	<input type="checkbox"/> Yes <input type="checkbox"/> No
Suspect on Parole	<input type="checkbox"/> Yes <input type="checkbox"/> No	Suspect on Probation:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Suspect known to have mental health issue:	<input type="checkbox"/> Yes <input type="checkbox"/> No	Q5:	<input type="checkbox"/> Yes <input type="checkbox"/> No

Additional Description: \_\_\_\_\_

---

---

# ADDITIONAL INFORMATION

Units Assisting:

☐ BPD SWAT

☐ Tactical Car

☐ EOD/Ballistics K-9

☐ Patrol/Narcotics K-9

☐ Bomb Squad

☐ Hazmat

☐ EMS

☐ Animal Control

Other: \_\_\_\_\_

Outside Agencies:

☐ State Police

☐ FBI

☐ DEA

☐ ICE

☐ Postal Service

☐ ATF

☐ HUD

☐ Secret Service

☐ USMS

☐ Other/Local Department: \_\_\_\_\_

Prisoner Processing Location(s): \_\_\_\_\_

Debriefing Instructions: \_\_\_\_\_

Code 99 Instructions, if applicable: \_\_\_\_\_

Pre-Execution Surveillance by: \_\_\_\_\_

Call Sign: \_\_\_\_\_ Contact #: \_\_\_\_\_

## PERSONNEL & ASSIGNMENTS

No.	Name	Agency	Call Sign	Entry Assignment	Search Assignment	Other



## PERSONNEL & ASSIGNMENTS

[illegible]



**Police Commissioner's Special Order**

Number: SO 21-27

Date: June 8, 2021

Post/Mention: Indefinite

**SUBJECT: RULE 335, GANG ASSESSMENT DATABASE**

Rule 335, Gang Assessment Database, is hereby amended superseding all previous rules, special orders, memos and directives on this subject and is effective immediately.

Changes to this Rule include:

- Clarification of the purpose of the Gang Assessment Database in preventing and reducing violence and victimization in the City of Boston;
- Clarification of the role of the Boston Regional Intelligence Center (BRIC) in management of the Gang Assessment Database;
- Clarification and amendment of criteria for access, submission, verification, dissemination, and review;
- Removal of the "inactive" status, thereby ensuring that those individuals will be reviewed for purge or re-categorized to more accurately reflect their participation in gang activity;
- Clarification that Field Interaction/Observation/Encounter ("FIOE") Reports shall not be used as the sole criteria for verification;
- Addition of an annual public reporting requirement regarding number of individuals added to and purged from the Database.
- Addition of a Juvenile section with the intention of connecting juveniles to services and providing a pathway out of the Gang Assessment Database.

The BRIC shall have a reasonable amount of time from the date of adoption of this rule to ensure the Gang Assessment Database is in full compliance.

Commanding Officers shall ensure that this order and the attached Rule are posted on Department bulletin boards.

Gregory P. Long  
Superintendent In Chief

**RULE 335: GANG ASSESSMENT DATABASE****General Considerations:**

In 1993, the Boston Police Department created a coordinated, multi-agency enforcement unit to address the youth violence problem affecting the City of Boston. The Youth Violence Strike Force, as it was named, has since evolved to incorporate prevention, intervention, and enforcement strategies. Furthermore, in 2005 the Boston Police Department created the Boston Regional Intelligence Center (BRIC), which formalized the Department's responsibilities for information sharing, analysis, threat assessment and risk management. Amongst several strategic responsibilities, the BRIC works closely with the Youth Violence Strike Force to analyze data and information pertaining to criminal activities that often result in cycles of retaliatory violence perpetrated against rival gangs and individuals, and their perceived neighborhoods and/or territories, presenting a substantial risk to communities within the City and Region. The following Rule delineates the responsibilities of the Youth Violence Strike Force as well as the process for gang associate verification, analysis and entry into the Gang Assessment Database by designated personnel from the Boston Regional Intelligence Center.

**Section 1. Youth Violence Strike Force:**

Established in 1993 in response to the increased use of violence amongst youth in the City of Boston.

The mission of the Boston Police Department's Youth Violence Strike Force (YVSF) is to proactively reduce gun violence, particularly concentrating on individuals affiliated with gangs or violent criminal behavior. YVSF utilizes traditional policing strategies, incorporating prevention, intervention and enforcement efforts, as well as intelligence-led policing strategies to inform decision-making at every level. Patrol officers and detectives collect information and focus on sources of firearm and gang violence through the identification of individuals, groups, and locations. YVSF works collaboratively with community partners and other stakeholders to garner information on illegal firearms and related violence. Officers aim to prevent ongoing conflicts among street gangs through direct interaction with individuals and groups. Officers not only respond to but anticipate retaliatory violence between groups, and make every effort to deter further violence. Through community-based partnerships, suitable individuals with whom the YVSF makes contact are referred to social services and offered a variety of opportunities.

**Section 2. Boston Regional Intelligence Center**

Boston Police Department's Bureau of Intelligence and Analysis (BIA) provides management and oversight of the Boston Regional Intelligence Center (BRIC). The mission of the BRIC is to serve as the central point for the collection, synthesis, analysis, and dissemination of strategic and tactical intelligence to law enforcement, intelligence, first responder, and private sector partners; and to assist the federal government as a partner for national security.

Furthermore, in 2005, the Boston Police Department created the Boston Regional Intelligence Center (BRIC), which formalized the Department's strategic responsibilities for information sharing, analysis, and risk management. Amongst a number of strategic responsibilities, the BRIC works closely with the Youth Violence Strike Force to gather and analyze data and information pertaining to criminal activity that often result in cycles of retaliatory violence perpetrated against rival gangs and groups, and presents a substantial risk to the City and Region.

### **Section 3. Purpose of the Gang Assessment Database**

The purpose for the existence of the Gang Assessment Database is to:

1. Provide law enforcement a consistent citywide framework for identifying individuals and groups that associate as a "gang" and thus are likely to engage in or perpetrate criminal activity for the furtherance of the criminal organization, which may include targeted and/or retaliatory violence; and
2. Assist in the investigation of gang related criminal activity in the City of Boston.

The database is only used for valid law enforcement purposes, including enhanced officer awareness, suspect identification, witness and victim identification, resource deployment, investigative support, and to aid in the prosecution of gang related crimes. Through community-based partnerships, suitable individuals in the database with whom the YVSF makes contact are referred to social services and offered a variety of opportunities.

### **Section 4. Definitions:**

**Sec. 4.1 Gang:** A gang is an ongoing organization, association, or group of three (3) or more persons, whether formal or informal, which meets both of the following criteria:

1. Has a common name or common identifying signs or colors or symbols or frequent a specific area or location and may claim it as their territory and
2. Has associates who, individually or collectively, engage in or have engaged in criminal activity which may include incidents of targeted violence perpetrated against rival gang associates.

**Sec. 4.2 Gang Associate:** Any person, whether juvenile or adult, that has been verified using the Point-Based Verification System defined by this Rule and has obtained at least ten (10) points.

**Sec. 4.3 Gang Assessment Database:** Electronic database maintained by the BRIC that includes Gang Associates and Gangs in accordance with this rule.

**Sec. 4.4 Active Status:** An individual who has met the point criteria to be considered a Gang Associate and is reasonably suspected of participating in gang related criminal activity within the past five years. When an individual no longer meets the criteria for active status, they will be purged from the system.

**Sec. 4.5 Deceased Status:** An individual who is no longer living, but met the criteria to be a Gang Associate. Individuals with this status will be reviewed in accordance with this rule and the record may be retained if the circumstances of the death may result in the potential for retaliatory violence or criminal activity.

**Sec. 4.6. Long Term Incarceration Status:** An individual who has been verified as a Gang Associate in accordance with this Rule, who is currently incarcerated, serving a sentence of 2 or more years.

**Sec. 4.8 Primary Affiliation:** The group with which an individual is associated. In cases where an individual associates with more than 1 group, the primary affiliation should be considered the group in which Law Enforcement can most clearly articulate the individual having the strongest ties. This affiliation will have at least 10 points under the verification criteria. All individuals in the database shall have a primary affiliation.

**Sec. 4.9 Secondary Affiliation:** A secondary group that an individual could be verified as being associated with by at least 6 points. This is in addition to their Primary Affiliation.

**Sec. 4.10 Profile Page / Face Sheet:** A summary detailing a Gang Associate's key identifiers and any items used to verify an individual as a Gang Associate.

**Sec. 4.11 Authorized User:** All sworn Boston Police Officers and other individuals designated by the Commander of the BIA or his/her designee, in collaboration with the Commander of the Youth Violence Strike Force or his/her designee, shall be granted access to the Gang Assessment Database in accordance with this rule.

**Sec 4.12 Juvenile-** An individual who has not attained the age of 18.

## **Section 5. Gang Associate Verification:**

The Department uses a ***“Point-Based Verification System”*** to determine when an individual will be considered a Gang Associate. An individual that does not have a minimum of ten (10) points using the Verification System will not be included in the Gang Assessment Database. The BRIC will maintain copies of supporting documentation for all criteria used to verify an individual. The BRIC will analyze the validity of the supporting documentation for each individual criteria used to verify an associate and maintain the discretion to decline to use the information towards any criterion. The BRIC will maintain the discretion to decline to enter individuals into the database who meet the 10 point criteria but are determined to not be engaged in gang-related criminal activity.

The following list of items or activities may result in an individual's verification for entry into the Gang Assessment Database:

- Contact with Known Gang Associate (FIO) (2 points per interaction)
  - FIOs shall not be used as the sole verification criteria for any individual.
- Court and Investigative Documents (9 points)
- Documented Association (Police Incident Report) (4 points per interaction)
- Group Related Photograph (2 points)
- Information Developed During Investigation and/or Surveillance (5 points)

- Information from Anonymous Informant or Tipster (1 point)
- Information from Reliable, Confidential Informant (5 points)
- Known Group Tattoo or Marking (8 points)
- Membership Documents (9 points)
- Named in Documents as a Associate / Member(8 points)
- Participation in Publications (8 points)
- Possession of Documents (8 points if not in custody or incarcerated; 3 points if in custody or incarcerated)
- Possession of Gang Publications (2 points)
- Prior Validation by a Law Enforcement Agency (9 points)
  - The Law Enforcement Agencies validation process must be at least as rigorous as that used by the Boston Police Department.
- Published News Accounts (1 point)
- Self Admission (8 points)
- Use and or Possession of Group Paraphernalia or Identifiers (4 points)
- Victim/Target Affiliated with Associate of Rival Group (8 points if not in custody or incarcerated; 3 points if in custody or incarcerated)

A blank verification form is attached to this rule as Appendix A.

#### **Section 6. Access:**

The Department will provide access to the Gang Assessment Database to all personnel defined as authorized users in Section 4.11. All authorized users must complete a User Agreement before gaining access. Authorized users must have a legitimate law enforcement purpose for accessing the Gang Assessment Database. The Boston Regional Intelligence Center (BRIC) will serve as the administrator of the database and ensure that users have adequate access.

Authorized Users will have the following access permissions:

- **READ** all Gang Assessment Database entries within the system
- **SEARCH** all Gang Assessment Database entries within the system

#### **Section 7. Submission to the Gang Assessment Database:**

Authorized Users will be able to submit an individual for consideration for admission into the Gang Assessment Database. All submissions for verification shall include documentation to support the individual's entry into the Gang Assessment Database using the Point-Based Verification System. Submissions can be made to the Commander of the BRIC or his/her designee or the Commander of the Youth Violence Strike Force or his/her designee. All submissions for verification will be manually reviewed by a BRIC analyst and supervisor to determine compliance with this rule prior to entry into the database. If the individual is verified as a gang associate, the supporting documentation shall be maintained by the BRIC in the Gang Assessment Database. No individual will be considered for addition to the Gang Assessment Database on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations.

## **Section 8. Dissemination of Gang Assessment Database Information:**

All data contained in the Gang Assessment Database is considered Law Enforcement Sensitive. Authorized Users may access the Gang Assessment Database when there is a legitimate law enforcement purpose for doing so, such as an ongoing investigation or in support of a prosecution. All court ordered, defense requested, or public record requested production of information contained in the Gang Assessment Database should be directed to the Boston Police Department's Office of the Legal Advisor.

Specific Authorized Users within the BRIC, selected by the Commander of the BIA or his/her designee will have access to print Gang Associate profile pages / face sheets for legitimate law enforcement purposes. All printing from the database shall be logged and the reason and recipient noted.

## **Section 9. Review of Gang Assessment Database Entries:**

The Commander of the BIA or his/her designee, in collaboration with the Commander of the Youth Violence Strike Force or his/her designee, shall be responsible for ensuring that files are maintained in accordance with the goals and objectives set forth in this Rule. To that end, entries in the Gang Assessment Database shall be reviewed at least once every five years to determine if the individual remains active based on the definitions provided above. When an individual no longer meets the criteria for Active Status, they will be purged from the system.

BRIC will report by January 31st of each year to the Police Commissioner on the total number of individuals added to and purged from the database in the previous calendar year. These totals will then be released to the public.

## **Section 10. Juveniles:**

The BPD/BRIC is committed to identifying juveniles in the Gang Assessment Database in order to connect them with services. The BPD/BRIC has partnered with Boston's Safe and Successful Youth Initiative ("SSYI") to provide services as a pathway out of gang involvement. The BRIC will notify SSYI of all juveniles in the Gang Assessment Database to facilitate connecting the juvenile with appropriate services. Provided, however, that SSYI will not be notified if doing so would compromise an ongoing investigation.

The BRIC will consider the input of SSYI program personnel when determining if a juvenile meets the criteria for exclusion / removal from the Gang Assessment Database.

It is the ultimate goal of the Boston Police Department to eventually purge all juveniles from the gang database and stop the cycle of violence in the City of Boston.

Gregory P. Long  
Superintendent In Chief



**Police Commissioner's Special Order**

Number: SO 21-38

Date: 9/8/21

Post/Mention: Indefinite

**SUBJECT: RULE 405, BODY WORN CAMERA POLICY**

Rule 405, Body Worn Camera Policy, is hereby amended and reissued superseding all previous rules, special orders, memos and directives on this subject.

See Section 8.4, Officer Notification.

Gregory P. Long  
Superintendent In Chief



**Boston Police Department**

**Rules & Procedures**

**Rule 405**

**September 8, 2021**

**BODY WORN CAMERA POLICY**

**Sec. 1 GENERAL CONSIDERATIONS:**

The purpose of this policy is to establish guidelines for the proper use, management, storage, and retrieval of video and audio data recorded by Body Worn Cameras (BWCs). BWCs are effective law enforcement tools that reinforce the public's perception of police professionalism and preserve factual representations of officer-civilian interactions. BWCs may be useful in documenting crime and accident scenes or other events that include the confiscation and documentation of incidental evidence or contraband. The equipment will enhance the Department's ability to document and review statements and events during the course of an incident, preserve video and audio information and evidence for investigative and prosecutorial purposes. BWC recordings, however, provide limited perspective of encounters and incidents and must be considered with all other available evidence, such as witnesses' statements, officer interviews, forensic analysis and documentary evidence. Additionally, studies have shown that BWCs are a contributing factor in reducing complaints against police officers, increasing police accountability, and enhancing public trust.

It is the policy of the Department to respect the legitimate privacy interests of all persons in Boston, while ensuring professionalism in its workforce. Officers shall only use BWCs within the context of existing and applicable federal, state, and local laws, regulations, and Department rules and policies. The Department prohibits recording civilians based solely upon the civilian's political or religious beliefs or upon the exercise of the civilian's constitutional rights, including but not limited to freedom of speech, religious expression, and lawful petition and assembly. BWC footage shall not be reviewed to identify the presence of individual participants at such events who are not engaged in unlawful conduct. BWCs will not include technological enhancements including, but not limited to, facial recognition or night-vision capabilities.

When performing any patrol function as determined by the Police Commissioner or his/her designee, officers assigned BWCs must wear and activate BWCs according to Department policy.

**Sec. 2 PROCEDURES:**

Sec. 2.1 Training: Prior to being issued a BWC, officers shall successfully complete BPD Academy training related to this policy as well as the activation, use, categorization, and uploading of data. All department personnel who may supervise officers wearing BWCs or will require access to review videos shall also attend Department approved training.

Sec. 2.2 Camera Activation and Incidents of Use: Officers will activate the BWC only in conjunction with official law enforcement duties, where such use is appropriate to the proper performance of duties, and where the recordings are consistent with this policy and the law. As in

all law enforcement and investigative activities, the safety of officers and members of the public are the highest priority. If an immediate threat to the officer's life or safety makes BWC activation dangerous, then the officer shall activate the BWC at the first reasonable opportunity to do so. Once activated, the officer shall not deactivate the BWC until the encounter has fully concluded and/or the officer leaves the scene (see Section 2.8, BWC Deactivation). Officers shall record all contact with civilians in the following occurrences unless the decision to stop recording is made pursuant to Section 2.6 and 2.7:

1. Vehicle Stops;
2. Investigative person stops: consensual, or articulable reasonable suspicion stops pursuant to Rule 323 (FIOE Report), or stops supported by probable cause;
3. All dispatched calls for service involving contact with civilians;
4. Initial responses by patrol officers, including on-site detentions, investigations pursuant to an arrest, arrests, and initial suspect interviews on-scene;
5. Transport of prisoners;
6. Pat frisks and searches of persons incident to arrest (if not already activated);
7. Incidents of Emergency Driving;
8. Incidents of Pursuit Driving;
9. When an officer reasonably believes a crowd control incident may result in unlawful activity;
10. Any contact that becomes adversarial, including a Use of Force incident, when the officer has not already activated the BWC; or
11. Any other civilian contact or official duty that the officer reasonably believes should be recorded to enhance policing transparency, increase public trust and police-community relations, or preserve factual representations of officer-civilian interactions, provided that recording is consistent with Sections 2.3, 2.4, 2.5, 2.6, 2.7, 4.1 and 4.2 of this policy.

If an officer fails to activate the BWC, fails to record the entire contact, or interrupts the recording, the officer shall document in the incident report that a recording failure occurred. If an officer fails to activate the BWC, fails to record the entire contact, or interrupts the recording, and does not create an incident report, the officer shall submit BWC Special Notification Form to his/her Duty Supervisor to document that a recording failure occurred by the end of the shift or as soon as practical. The Duty Supervisor shall submit the officer's Form through his/her chain of command to his/her Bureau Chief.

**Sec. 2.3 Recording within a Residence:** Upon entering a private residence without a warrant or in non exigent circumstances, the officer shall notify occupants they are being recorded. When determining whether or not to record, the officer shall be guided by the safety of all person(s) present, and weigh the discretionary factors referenced in Section 2.4 with the fact that a home is a uniquely private location. Per SO 019-015, if the officer deactivates the BWC recording per occupant request, that officer should notify the Operations Division by radio that the incident is no longer being recorded by occupant request and call off on a Code 29, if possible. Officers recording in a residence shall be mindful not to record beyond what is necessary to the civilian contact, and shall not use the BWC with exploratory intent to create an inventory of items in the residence.

If an officer uses his/her discretion to turn off the BWC, the officer shall document this action in the incident report. If the officer does not create an incident report, the officer shall submit a

BWC Special Notification Form to his/her Duty Supervisor to document that he/she decided to stop recording by the end of the shift or as soon as practical. The Duty Supervisor shall submit the officer's Form to his/her District or Unit Commanding Officer. The District or Unit Commander or his/her designee shall provide a copy of the form to his/her Bureau Chief.

Sec. 2.4 Recording in Areas Where There May be a Reasonable Expectation of Privacy: Officers should be mindful of locations where recording may be considered insensitive or inappropriate. Such locations may include locker rooms, places of worship, religious ceremonies, certain locations in hospitals or clinics, law offices, and day care facilities. At such locations, at the officer's discretion and based on the circumstances, the officer may turn off the BWC. The officer may also consider diverting the BWC away from any subjects and recording only audio, if appropriate. When exercising discretion in such situations, the officer should generally base his/her decision to stop recording, divert the BWC, or record only audio on the following BWC Discretionary Recording Considerations. The officer must be able to articulate the reason for his/her decision to exercise discretion.

BWC Discretionary Recording Considerations include, but are not limited to: the sensitive or private nature of the activities or circumstances observed; the presence of individuals who are not the subject of the officer-civilian interaction; the presence of people who appear to be minors; any request by a civilian to stop recording; and the extent to which absence of BWC recording will affect the investigation.

If an officer uses his/her discretion to turn off the BWC, the officer shall document this action in the incident report. If the officer does not create an incident report, the officer shall submit a BWC Special Notification Form to his/her Duty Supervisor to document that he/she decided to stop recording by the end of the shift or as soon as practical. The Duty Supervisor shall submit the officer's Form to his/her District or Unit Commanding Officer. The District or Unit Commander or his/her designee shall provide a copy of the form to his/her Bureau Chief.

Sec. 2.5 Notice of Recording: The officer shall make a reasonable effort to inform civilians that the officer is recording them unless an immediate threat to the officer's life or safety or the life or safety of any other person makes BWC notification dangerous. Officers shall notify civilians with language such as "I am advising you that I am recording our interaction with my Body Worn Camera." Officers shall not record civilians surreptitiously.

Sec. 2.6 Consent to Record: Officers do not have to obtain consent to record. If a civilian requests the officer stop recording, the officer(s) has no obligation to stop recording if the officer is recording an occurrence identified in Section 2.2. When evaluating whether to stop recording, officers should weigh the BWC Discretionary Recording Considerations identified in Section 2.4. Officers should record the request to turn the BWC off and the officer's response to that request, if possible

If an officer deactivates a BWC in response to a civilian request, the officer shall also indicate the request in an incident report. If an officer deactivates a BWC in response to a civilian request and does not create an incident report, the officer shall fill out a BWC Special Notification Form and submit it to his or her Duty Supervisor indicating that a civilian requested the officer turn the

BWC off by the end of the shift or as soon as practical. The Duty Supervisor shall submit the officer's Form to his/her District or Unit Commanding Officer. The District or Unit Commander or his/her designee shall provide a copy of the form to his/her Bureau Chief.

Sec. 2.7 Recording of Victims / Witnesses: If an officer's BWC would capture a visual or audio recording of a victim or witness who is giving his/her first account of a crime, the officer may record the encounter but should weigh the BWC Discretionary Recording Considerations specified in Section 2.4 in determining whether to activate or discontinue audio and/or video recording. If the officer decides to activate and/or continue audio and/or video recording, the officer shall make the notification specified in Section 2.5. If the victim is in any way unsure of the need for the recording or is uncomfortable with the thought of being recorded, the officer shall inform the civilian that the civilian may request to have the BWC turned off. If the camera is already activated, the officer should record the request to turn the BWC off and the officer's response, if possible.

Sec. 2.8 BWC Deactivation: To the extent possible, prior to deactivating a BWC, the officer shall state the reason for doing so. Generally, once the officer activates the BWC, the officer will continue recording until the event has concluded. Below are some non-exhaustive examples of when deactivation may be permissible:

1. The officer has concluded the interaction;
2. All persons stopped have been released or left the scene or an arrestee has arrived at the booking area or secure court facility. If a transporting officer has a BWC, that officer shall continue recording until the transporting officer enters the booking area or secure court facility;
3. The event is sensitive, the officer has weighed the BWC Discretionary Recording Considerations specified in Section 2.4, and has decided to deactivate the BWC;
4. The incident has concluded prior to the arrival of the officer;
5. A supervisor orders the officer to turn the camera off.

Sec. 2.8.1 Suspicious Device Protocol: First initial responding officers and/or first officers on scene of a suspicious object shall **power off** their BWC when in the immediate proximity of the suspicious object. All other responding officers shall ensure they are at least 300 feet from the object prior to activating their BWCs. When dispatching any calls for suspicious objects, the Operations Division should remind first responding officers to **power off** their BWCs prior to approaching the scene of the device.

#### Sec. 2.9 Special Operations Division Activation Factors

1. **Motorcycles:** Mobile Operations Patrol (MOP) Officers shall wear body-worn cameras and activate when interacting with the public during patrol activities. MOP units are not required to activate their cameras during escorts, unless an interaction with the public may warrant possible interaction recording.
2. **K-9:** K-9 Officers will wear body-worn cameras daily and will activate when performing patrol functions as described in Rule 405. If they are utilized for specific incidents involving EOU they will consult with and follow the protocol of EOU personnel.

3. **Tactical Cars:** Officers assigned to a Tactical Car will wear BWC and activate once they activate emergency driving or expect to interact with the public. Officers should avoid capturing lock codes to the extent feasible when accessing gun safes.
4. **Explosive Ordnance Unit (“Bomb Squad”):** Bomb Squad Officers shall adhere to Special Order 19-036 and not wear their body-worn cameras when approaching possible suspicious objects. Otherwise, cameras are to be worn daily and activated when interacting with the public. Bomb tech will exercise their best judgment and due caution when deciding when to have BWCs on during EOU related duties.
5. **Dive Team:** Officers will use BWC in the regular assignments as directed but not during dive operations.
6. **Crisis Negotiator:** Crisis negotiators will follow training and protocols to determine whether the BWC is to be activated. Remote negotiations (by phone, loud speaker etc.) do not require BWC activations.
7. **Snipers:** Officers are not expected to activate body-worn cameras during sniper deployment if the BWC would interfere with operations.
8. **SWAT Team - Code 99 / Search Warrants:** Briefings, tactical discussions or communications regarding officer placement or safety are not to be recorded. SWAT Officers will activate their cameras on approach to an entry point, or at the direction of SWAT Team Supervisors.
9. **Hazmat:** Will wear body-worn cameras daily and activate per Rule 405 when performing day to day patrol duties unless electrical or signal interference is a concern.
10. **Harbor Patrol Unit:** Will wear body-worn cameras daily and activate per Rule 405 when performing day to day patrol duties.
11. **Commercial Vehicle Enforcement Unit (CVEU):** Will wear body-worn cameras daily and activate per Rule 405 when performing day to day patrol duties.
12. **Sensitive Nature / Redactions:** Concerns regarding tactics and internal communications shall be redacted for public dissemination when legally permissible.

### Sec. 3 CAMERA DEPLOYMENT:

#### Sec. 3.1 Officer Responsibility:

BWC equipment is the responsibility of every officer issued the equipment. Officers must know the location of each of their assigned cameras at all times. Officers must use the equipment with reasonable care to ensure proper functioning. Officers shall inform their Duty Supervisors as soon as possible of equipment malfunctions or loss of a BWC so that the officer can procure a replacement BWC. An officer who loses or misplaces a BWC shall complete any necessary protocols required by the Department for lost equipment (per Rule 322).

Police officers shall use only BWCs issued by this Department. The BWC equipment and all data, images, video recordings, audio recordings, and metadata captured, recorded, or otherwise produced by the equipment is the sole property of the Boston Police Department and shall not be released without the authorization of the Commissioner or his/her designee.

1. At the beginning of each shift, the officer will:
  - a. Ensure that one of his/her BWCs has a fully charged battery and is functioning properly;
  - b. Power on his/her fully charged and functioning assigned BWC;
  - c. Confirm that his/her BWC is properly paired, via Bluetooth, to his/her assigned Department-issued mobile device. If officers are unable to pair their Department

issued mobile device to their BWC, officers can still record video using the BWC. Pairing instructions are attached to this Special Order **and** available on the BPD Intranet. If officers cannot pair their Department-issued mobile device to their BWC, they must complete the appropriate online BWC Special Notification form and must log in to evidence.com on a Department computer to tag their videos once the video is uploaded to evidence.com; and

- d. Notify a Duty Supervisor whenever there is a malfunction or damage to the BWC, and fill out the appropriate online BWC Special Notification Form.
2. During each shift, the officer shall:
- a. Affix their BWC properly upon their uniform in a manner consistent with training;
  - b. Position and adjust the BWC to record events;
  - c. Position and adjust the BWC microphone to ensure that it is unobstructed;
  - d. Activate the BWC and record as outlined in Section 2 above;
  - e. Document the existence of a BWC recording in all of the appropriate documents, i.e. Incident Report, Citation, FIO, Administrative Reports;
  - f. Notify investigative or specialized unit personnel, including the Crime Scene Entry Scribe, of the existence of BWC recording; and
  - g. Document in the incident report the circumstances and reasons if he/she fails to activate the BWC, fails to record the entire contact, interrupts the recording, or the BWC malfunctions. If the officer does not create an incident report, the officer shall submit an online BWC Special Notification Form to document the circumstances and reasons.
3. Prior to end of shift: docking/uploading requirements:
- a. When officers end a shift in their assigned district/unit: At the end of the officer's shift, each officer shall place the BWC used during that shift in a docking station assigned to the officer by the Boston Police Department. The docking station will charge the BWC's battery and transfer video data to the storage system. Officers shall ensure all required references to BWCs in appropriate Department documentation are included, such as incident reports or Form 26 reports at the end of their shift.
- At the end of his/her shift each officer shall retrieve his/her other assigned BWC from the docking station prior to leaving the district/unit. Each officer shall ensure their other assigned BWC is secure, fully charged, has adequate storage available, and is accessible to the officer for use prior to his/her next patrol function.
- b. When the officer ends a detail (in or outside of his/her assigned district) or ends shift at a location outside of his/her assigned district/unit: The officer must dock the BWC used during his/her detail or shift at their assigned district/unit to upload video the next time the officer reports to his/her assigned district, but no later than two days after taking the video. Each officer shall ensure their other assigned BWC is secure, fully charged, has adequate storage available, and is accessible to the officer for use prior to his/her next patrol function.

- c. If an officer becomes aware that the uploading process is not occurring or becomes aware of any other malfunction of the system, the officer shall notify their Duty Supervisor immediately, and fill out the appropriate online BWC Special Notification Form.
- d. A District/Unit Commander may order, due to investigative needs, an officer to upload their videos via evidence.com at any time.

Sec. 3.2 Labeling and Categorization of BWC Recordings: Proper categorization of recorded data is critical. The retention time for recorded data typically depends on the category of the event captured in the video. Accurate categorization and accurate descriptions also help officers, supervisors, prosecutors, and other authorized personnel to readily identify and access the data they need for investigations or court proceedings.

Section 3.2.1 Categorization: At the conclusion of the call or prior to the end of their shift, officers shall assign uploaded data into the appropriate BWC Mobile Device Application categories in accordance with the nature of police activity. Categorization options are in order of the seriousness of offense and should be labeled to reflect the most serious nature of police activity. These categories include but are not limited to:

1. Death Investigation
2. Code 303- Lethal/Less Lethal
3. Sexual Assault/Abused Person
4. Use of Force
5. Arrest
6. Felony - No Arrest
7. Misdemeanor - No Arrest
8. Investigate Person
9. Investigate Premise
10. Significant Event - Public Safety
11. Traffic Stop
12. Encounter/FIO
13. Sick Assist
14. No Report - Dispatch/On Site
15. Test/Training
16. Accidental Recording

The Department may develop other categories, as needed.

If an officer is assisting other officers on a call, the assisting officer shall use the category, and I or P# of the original incident.

Sec. 3.2.2 BWC Mobile Device Application: Officers assigned BWCs shall comply with the use of the Department authorized BWC Mobile Device Application for all BWC requirements. Employees shall follow the training and procedures provided by the Boston Police Academy and the Video Evidence Unit.

When installed, the BWC Mobile Device Application and/or BWC Device Application's location services will be set to off and officers should not turn it on.

Section 3.2.3 Title Description: Officers shall enter the nature and location of each call in the title field in the BWC Mobile Device Application. Officers shall properly title all footage at the conclusion of the call or prior to the end of their shift.

Sec. 3.2.4 ID Description: Officers shall assign the BWC Mobile Device Application "ID" field as the "I number" or "P number" assigned to each video recorded.

Sec. 3.3 Request to Redact: Officers wearing BWCs should be aware that their BWCs may unintentionally capture private/security information such as door codes, phone codes, and computer codes. If the officer knows that his/her BWC captured sensitive information or material, the officer shall inform his/her Duty Supervisor and request redaction of the video prior to distribution to any outside parties. The officer shall document in the BWC Special Notification Form to his/her Duty Supervisor the nature of the information captured and the request for redaction. The Duty Supervisor shall submit the officer's Form to his/her District or Unit Commanding Officer. The District or Unit Commanders or his/her designee shall provide a copy of the form to his/her Bureau Chief and an additional copy to Video Evidence Unit to maintain the record. The Commander of the BWC Unit will authorize redaction when he/she determines it is necessary.

#### **Sec.4. RECORDING RESTRICTIONS:**

Sec. 4.1 Improper Recording: Officers shall not use BWCs to record in violation of this Policy or any rule or procedure of the Boston Police Department, including:

1. During breaks, lunch periods, or time periods when an officer is not responding to a call, or when not in service;
2. Any personal conversation of or between other department employees without the recorded employee's knowledge;
3. Non-work related personal activity, especially in places where a reasonable expectation of privacy exists, such as locker rooms, dressing rooms, or restrooms;
4. Investigative briefings;
5. Encounters with undercover officers or confidential informants; or
6. Departmental meetings, workgroups, in-service training, or assignments of an operational or administrative nature.

Using BWCs for training purposes is not a violation of this restriction.

If an officer inadvertently records as listed above, the officer shall follow the request to redact/delete procedures described in Section 3.3.

Sec. 4.2 Improper Use of BWC Footage:

1. Officers shall use BWC data, images, video recordings, audio recordings, or metadata only for legitimate law enforcement reasons. They shall not use data, images, video



recordings, audio recordings, or metadata for personal reasons, or non-law enforcement reasons.

2. Department personnel shall not use BWC data, images, video recordings, audio recordings, or metadata to ridicule or embarrass any employee or person depicted on the recording.
3. Department personnel shall not disseminate BWC data, images, video recordings, audio recordings, or metadata unless the Police Commissioner or his/her designee approve the dissemination and the Department personnel disseminates the BWC data, images, video recordings, audio recordings, or metadata in the course of his/her official duties.
4. Department personnel shall not copy or otherwise reproduce any BWC recording/footage (including using an iPhone, iPad, or other electronic or other device).
5. Bureau Chiefs, supervisors and Internal Affairs shall not randomly review BWC recording/footage for disciplinary purposes

## **Sec. 5 SUPERVISOR RESPONSIBILITIES:**

Sec. 5.1 Duty Supervisors: All Duty Supervisors assigned to oversee officers utilizing Department-issued BWCs shall:

1. Ensure officers are utilizing their BWC consistent with this directive.
2. Ensure BWCs and related equipment are kept in a secure location within the district or unit.
3. Notify the Video Evidence Unit if an officer utilizes a BWC that is not assigned to him or her, so the Unit may reassign the recordings of audio and video to the officer who created the recordings.
4. Contact the Video Evidence Unit whenever any officer is unable to use the BWC or upload digitally recorded data due to technical problems.
5. Request replacement BWC equipment from the Video Evidence Unit when an officer indicates the equipment is lost or malfunctioning via the Special Notification Form. Once procured by Video Evidence Unit ensure new equipment is received by requesting officer.
6. Ensure that officers include all required references to BWCs in appropriate Department documentation, such as incident reports or Form 26 reports.

Duty Supervisors may review BWC data, images, video recordings, audio recordings, or metadata, consistent with this Policy, to approve any reports

Sec. 5.2 District or Unit Commanding Officers or Designees:

Commanding officers or his/her designee will review BWC activity logs and reports to ensure officers remain in compliance with Department policy and training.

## **Sec. 6 INTERNAL ACCESS/REVIEW:**

Sec.6.1 Officer Access to Their Own Footage (Not Related to Officer Involved Death, Officer Involved Shooting, or Other Use of Deadly Force): Officers may review their own BWC

recording when they are:

1. Involved in an incident, for the purposes of completing an investigation and preparing official reports. To help ensure accuracy and consistency, officers should review the BWC recording prior to preparing reports;
2. Preparing for court. Officers should advise the prosecuting attorney that they reviewed the BWC recording; and
3. Providing a statement pursuant to an internal investigation or other critical incidents.

If an officer requests access to footage be made available for a time frame longer than the retention schedule allows, a request to extend retention schedule via the BWC Special Notification Form must be sent to the Video Evidence Unit. The footage will be available according to Schedule II in Section 9.2.

If an officer needs a physical copy of their footage, a request shall be made via the online BWC Special Notification Form and sent to the Video Evidence Unit. Physical copies of the video shall be subject to M.G.L. Ch. 66, Sec. 10 and in accordance with all applicable state laws and regulations.

Sec. 6.2 Officer Access to Footage Following an Officer Involved Death, Officer Involved Shooting, or Other Use of Deadly Force (Rule 205 and/or Rule 303 Investigations): Following an officer involved death, officer involved shooting or other use of deadly force, officers and supervisors at the scene shall not view any video before the Homicide Unit or Firearm Discharge Investigation Team (“FDIT”) views the footage and uploads it into the system.

The on-scene incident commander shall be permitted to view BWC video and relay necessary information if exigent circumstances exist and it is necessary to view the video to (1) identify suspect information or (2) gather pertinent information that is necessary to protect life or safety prior to Homicide Unit or FDIT arrival.

At a time determined by the supervisor in charge of the investigation, officers who: (1) were involved in the incident, (2) discharged their weapon, and/or (3) witnessed the incident may view their own video before giving a statement. At the officer’s request, the officer’s attorney may be present when the officer views the video.

BWC video footage is a tool that may aid officers in providing an accurate and complete account of the incident. BWC footage should not replace an officer’s memories of the incident and the officer should base his/her statement on his/her memories, not solely on the video.

Sec 6.3 Collecting and Securing BWC Footage Following an Officer Involved Death, Officer Involved Shooting, or Other Use of Deadly Force (Rule 205 and/or Rule 303 Investigations): In accordance with Rule 205 and Rule 303, the Patrol Supervisor shall respond immediately to a death investigation or reported use of deadly force within his/her District.

The Patrol Supervisor, as soon as circumstances allow, shall collect all BWC equipment, including department-issued mobile devices, which belong to the officers who: (1) were involved

in the incident, (2) discharged their weapon, and/or (3) witnessed during the time of the officer involved death, officer involved shooting or other use of deadly force, and store the equipment in a secure compartment of his/her vehicle until the Homicide Unit or FDIT personnel arrives on scene. Once on scene, the Homicide Unit or FDIT personnel shall secure any remaining BWC equipment from involved officers and witness officers, as well as equipment already secured by the Patrol Supervisors, at the earliest opportunity. The Homicide Unit or FDIT personnel will transport the cameras to the involved officer's assigned district or the Homicide Unit for upload into the system. The BWC equipment will be returned to the officer as soon as possible following the event.

Once uploaded, the Video Evidence Unit shall restrict video access from all users except for the BIS Bureau Chief, Homicide Unit and/or FDIT investigators assigned to the case. The BIS Bureau Chief may approve access to other users, as necessary.

Sec. 6.4 Officer Access to Footage: Officers who need to review video or audio footage from another officer shall make a request via the online Special Notification Form to the Video Evidence Unit describing why they need to review the footage.

The Commander of the Video Evidence Unit shall approve or deny the request. With approval, the Video Evidence Unit will provide access to the video and audio footage to the requesting officer. If providing another officer's video or audio, the Video Evidence Unit shall notify the District or Unit Commander of the officer whose BWC footage is requested that the BWC footage is being shared.

Sec. 6.5 Supervisor Access to Footage: Any supervisor within the recording officer's chain of command, and any Bureau Chief, may review the footage consistent with Section 4.2. A supervisor outside of the chain of command shall only be allowed to review footage with the permission of the Video Evidence Unit Commander.

Sec. 6.6 Audit and Review Access to Footage: Audit and Review shall conduct periodic checks to ensure Department personnel are using BWCs according to Department policy.

## **Sec. 7 SUPERIOR DETECTIVE AND DETECTIVE RESPONSIBILITIES:**

Superior detectives must ensure that detectives adhere to the duties and responsibilities as follows in this Section:

Detectives will not use the BWC system or evidence.com until they have successfully completed the required training.

The Department will give detectives access to all BWC footage related to their assigned cases.

When assigned a case for investigation, the assigned detectives will:

1. Determine the identity of all involved officers.
2. Search evidence.com for any associated BWC media, using applicable search parameters to verify that they have located all relevant files.

The assigned Detective will review all BWC footage within a reasonable time. However, if the Detective determines that the BWC footage is not relevant to the investigation or the investigation is closed, the Detective may, with the approval of their supervisor, choose not to review the BWC footage. The supervisor's approval shall be noted in the case management file.

Detectives should be aware that additional BWC footage may be updated at a later time or date.

Should a detective consider material too sensitive to be accessible for other members of the Department, the detective shall notify his/her supervisor of the sensitive material. The detective's supervisor shall review the video and, if deemed appropriate, send a request via the BWC Special Notification Forms to the Video Evidence Unit to make the data unavailable for a given amount of time.

## **Sec. 8 EXTERNAL ACCESS:**

Sec. 8.1 Prosecutorial / Law Enforcement Access: Federal, state, and local prosecutors shall make requests for BWC footage directly to the Video Evidence Unit. In accordance with current practice, should an officer receive a subpoena for BWC footage, the officer shall direct the subpoena to their supervisor with a Form 26. The officer shall indicate in their Form 26 that a request for video has been made. The officer shall also direct a copy of the subpoena and Form 26 as soon as practicable to the Video Evidence Unit for response.

Officers are not permitted to provide video to any external partners and shall forward any requests made without a subpoena directly to the Video Evidence Unit.

Upon receipt of the request, Video Evidence Unit ("VEU") shall determine if the case has been assigned to a detective. If so, the VEU will notify the assigned Detective and/or Detective Supervisor of the request. The Detective or Detective Supervisor will then be responsible for providing all responsive and related case video directly to the federal, state, or local prosecutor. If no detective is assigned to the case, VEU shall identify all relevant BWC footage and provide it directly to the federal, state, or local prosecutor.

Sec. 8.2 Public Information Requests: Video Evidence Unit shall respond to public information requests submitted under M.G.L. Ch. 66, sec. 10 in accordance with all applicable state laws and regulations.

Sec. 8.3 Other External Information Requests: The Department may receive requests for BWC footage not covered by sections 8.1 and 8.2. For example, civil discovery requests are appropriately submitted to the assigned attorney in the Office of the Legal Advisor, and requests for information submitted by a collective bargaining representative under M.G.L. c. 150E are appropriately submitted to Office of Labor Relations. Should an officer receive a civil case subpoena or court order, he or she shall forward the request directly to the Office of the Legal Advisor.

If these offices receive other external requests for BWC footage, they shall request necessary and

responsive footage from the Video Evidence Unit via the online BWC Special Notification Form.

The Video Evidence Unit shall maintain a log of the request, and assist the requesting office to collect and process the requested footage. The Video Evidence Unit shall provide the requested footage to the requesting office, and complete redactions if required by the requesting office. The requesting office will be responsible for the review, approval, and release of footage to the appropriate person(s) as consistent with applicable law and agreements.

Sec. 8.4 Officer Notification: The Video Evidence Unit will notify officers of requests for BWC footage made under Section 8.2 (Public Information Requests) and Section 8.3 (Other External Information Requests) where the officer has not received a subpoena or request for BWC footage directly, unless prohibited by legal or investigative restrictions.

Sec. 8.5 Detective Notification: When releasing BWC footage to the public that has been designated as part of an investigation via the BWC Platform, the assigned detective shall be notified, unless prohibited by legal or investigative restrictions.

## **Sec. 9 RETENTION:**

Sec. 9.1 Camera Storage: BWC recordings and data are kept in a cloud-based storage platform managed by Video Evidence Unit.

Sec. 9.2 Video Footage Retention: The Department will retain BWC footage based on categorization, but may retain the footage longer on a case-by-case basis as determined by the Police Commissioner or his/her designee. The footage retention schedule for cloud-based footage access is as follows:

a. Schedule I- Indefinite Retention:

- Death Investigation
- Code 303- Lethal/Less Lethal
- Sexual Assault / Abused Person

b. Schedule II- 7 Year Retention:

- Use of Force
- Arrest
- Felony - No Arrest

c. Schedule III- 3 Year Retention:

- Misdemeanor - No Arrest
- Investigate Person
- Investigate Premise

d. Schedule IV- 180 Day Retention:

- Significant Event - Public Safety
- Traffic Stop
- Encounter/FIO

- Sick Assist
- No Report - Dispatch / On Site
- Test/Training
- Accidental Recording

Gregory P. Long  
Superintendent In Chief



**Boston Police Department**

**Rules & Procedures**

**Rule 406**

**June 3, 2019**

## **Mobile Device Policy**

**1. Purpose and Scope:** The purpose of this policy is to define standards, procedures and restrictions for the use of Department-issued smartphones and mobile devices. This policy applies to all employees, including contractors, who are issued a mobile device for Boston Police Department (BPD) business. Employees are not required to utilize their mobile devices while off-duty, unless functioning in an on-call capacity.

Prior to receiving a Department-issued mobile device, employees must review the regulations set forth herein and complete any training required by the Department.

**2. Roles and Responsibilities:** The Department will determine who shall receive a Department issued mobile device for use in the performance of his/her duties based on Department need and availability of devices.

All employees are expected to exercise the same discretion using the mobile device as they are expected for the use of desk phones and computers.

Employees issued a mobile device do not have an expectation of privacy in anything viewed, created, stored, sent, or received on a Department-issued mobile device. All information on these devices may be subject to public records law and its regulations. Employees are reminded that all mobile devices and content on the device remain the property of the Department.

**Sec. 2.1 Lost or Stolen Property:** If the Department-issued mobile device or related equipment is damaged in the course of business, officers must bring the equipment to the Telecommunications Division for repair/replacement. Employees must immediately report lost or stolen equipment to the employee's supervisor and the Telecommunications Division so that the service can be cancelled on the device. Employees are expected to protect Department issued equipment from loss, damage or theft.

**Sec. 2.2 Returning of Equipment:** Upon resignation or termination of employment, or at any time upon request by the Department, the employee must produce the equipment for return or inspection. Employees who are unable to present the equipment in good working condition due to negligence or misuse within the time period requested may be required to provide the cost of a replacement.

## Appendix T

**3. Smartphone/Mobile Device Conduct:** Users of Department-issued mobile devices must abide by all standards of professional behavior and conduct.

Department-issued mobile devices cannot be used to discriminate in any way based upon an individual's race, color, national origin, religion, disability, age, citizenship status, creed, ancestry, military status, sex, sexual orientation, gender identity, genetic information or membership in any other class protected under federal or state law.

Some additional examples of conduct in violation of these standards include, but are not limited to:

- a. communication of information that disparages, threatens, or harasses others; b. knowing receipt or communication of sexually explicit material, propositions or suggestive remarks; or
- c. knowing receipt or communication of aggressive material including violence, abuse, obscenities or material that promotes illegal acts.

Subsections a) through c) shall not apply to material received or sent related to an investigation or as needed in the course of an individual's official duties.

**4. Personal Use of Department-Issued Mobile Devices:** The Department allows limited, reasonable, personal use of Department-issued mobile devices with the knowledge that all use of Department-issued mobile devices may be monitored and subject to Department policy and public records laws. In addition to the standards of conduct set out above in Section 3, personal use of Department-issued mobile devices must not incur a cost to the Department, disrupt the workplace, interfere with work responsibilities, or cause embarrassment to the Department. The personal use of any social media applications shall conform to Rule 102 (The Conduct and General Rights and Responsibilities of Department Personnel), and if used by an employee in the course of their job duties, shall also conform to Section 5.1 below.

Employees using a Department-issued mobile device for personal use do not have an expectation of privacy in anything viewed, created, stored, sent, or received on a Department-issued mobile device. All information on these devices may be subject to public records law and its regulations. Employees are reminded that all mobile devices and content remain the property of the Department.

**5. Mobile Device Applications:** Upon receipt of a Department-issued cell phone, employees may download additional applications that serve a business-related purpose.

While on duty, employees will be responsible for the information provided through Department installed applications, as it pertains to their assignment and job description. Should any Department-installed application experience any issues or become non-functioning, it is the responsibility of the employee to notify his/her supervisor for maintenance. Supervisors shall notify the Unit responsible for the application about related issues, as soon as possible.



## Appendix T

All employees must ensure that system software and Department-installed applications are current and updated. Users will be notified of available updates directly on the device and must follow instructions for downloading and updating the device. Users should contact the Telecommunications Division for assistance, as necessary.

**Section 5.1 Department-Sanctioned Social Media Uses:** The Department permits use of social media applications for work use only as it pertains to job responsibilities. The use of any social media applications shall conform to Rule 102 (The Conduct and General Rights and Responsibilities of Department Personnel). Investigatory uses are not outlined in this rule.

- a. Community Outreach: Employees authorized to do so as part of their job function may use social media for community outreach and engagement, provide crime prevention tips, offer online-reporting opportunities, share crime maps and data, respond to citizen inquiries, and to promote Department events.
- b. Notifications: Employees authorized to do so as part of their job function may use social media to make time-sensitive notifications including but not limited to road closures, special events, weather emergencies, missing or endangered persons, and public safety emergencies.
- c. Hiring and Recruitment: Employees authorized to do so as part of their job function may use social media to recruit potential employees and/or volunteers, as well as assist in the hiring process.

**6. Text Messages/Emails:** Employees are reminded that all work product, including text messages, must be preserved in accordance with existing Department policy or legal requirements. In the event that text messages and/or emails are sent and/or received relative to an investigation or official duties, employees are prohibited from deleting the substance of communication from the mobile device prior to preserving the communication in another manner.

**7. Camera/Video Capabilities:** Department-issued mobile devices may have camera and video capabilities. Employees should be aware that any photographs and/or video taken with a Department-issued mobile device may be subject to discovery obligations and public records laws that require the production of these materials.

Methods of capturing and preserving photographs and/or video evidence on Department-issued mobile devices shall be in accordance with Rule 331 of the Department's Rules and Procedures.

Officers are required to use existing procedures for video, photographic, and/or digital evidence unless authorized by a Commanding Officer. Any deviation from existing procedures shall be documented in a Form 26 and provided to the appropriate Bureau. Employees must preserve any such photographs and/or video evidence prior to deleting them from the device.

**8. Terms of Acceptance:** Employees who receive a Department-issued smartphone or mobile computing device will abide by the following conditions:

## Appendix T

- The Department reserves the right to remotely configure the device. This includes remotely setting services and installing/uninstalling applications. These may include location-based services and applications running on the phone or device, such as “Find My Phone” so that a lost or stolen device can be located.
- Employees must maintain a cloud-based account on the device utilizing their Department email address as the user ID. The retention of all account information and passwords is the sole responsibility of the employee.
- Should an employee’s Department-issued mobile device become lost or stolen; an immediate attempt will be made, by the employee, to locate the device using a cloud based account. The employee must be in possession of the cloud-based account password to complete this process. If the device cannot be located as a result of failure to follow this process, the replacement cost of the device may be the responsibility of the employee.
- Employees who require the use of their Department-issued mobile device outside of the coverage area for work-related purposes are required to contact the Telecommunications Division in writing at least one week prior to travel to request a change to global coverage, if feasible. The Telecommunications Division will respond with approval or denial of the request.
- Employees, not previously authorized to do so, who use a Department-issued mobile device outside of the existing coverage area are responsible for any data, voice roaming or other charges incurred as a result. Employees shall check with Telecommunications to identify out of coverage areas prior to travel outside of the country.
- Employees who receive a Department-issued smartphone or mobile device acknowledge that the content of all text messages (SMS and other types of messages) and phone logs associated with the cellular access account supplied by the Department are and remain the property of the Boston Police Department.
- Phones are to be used to increase efficiency in the performance of job duties.



**Police Commissioner's Special Order**

Number: SO 21- 32

Date: July 15, 2021

Post/Mention: Indefinite

**SUBJECT: RULE 407, UNMANNED AIRCRAFT SYSTEMS POLICY**

Effective immediately, Rule 407 – Unmanned Aircraft Systems Policy is hereby issued superseding all previous rules, special orders, memos and directives on this subject.

A handwritten signature in black ink that reads "Gregory P. Long". The signature is fluid and cursive, with the first letters of each word being capitalized and prominent.

Gregory P. Long  
Superintendent In Chief

## **UNMANNED AIRCRAFT SYSTEMS POLICY**

### **Sec. 1 Purpose:**

The purpose of this policy is to establish guidelines and procedures which inform members of the Department of the circumstances under which a Department Unmanned Aircraft System may be deployed by the Boston Police Department.

### **Sec. 2 Definitions:**

*Unmanned Aircraft System (UAS):* A UAS consists of four parts:

- 1) The Unmanned Aerial Vehicle (UAV)
- 2) A ground control station
- 3) Command and control links
- 4) Crew members (PIC and VO)

*Unmanned Aerial Vehicle (UAV):* an aircraft that is operated without a physical human presence within or on the aircraft which, depending on how it is utilized, is capable of capturing and documenting photographs and video of the affected area or providing an aerial perspective of the area and is guided by remote control under the supervision of the assigned operating officer.

*Small Unmanned Aircraft (UA):* a UA weighing less than 55 pounds, including everything that is onboard or otherwise attached to the aircraft, and can be flown without the possibility of direct human intervention from within or on the aircraft.

*Remote Pilot-in-Command (Remote PIC):* A person who holds a remote pilot certificate with a UAS rating and has final authority and responsibility for the operation and safety of a UAS operation conducted under 14 CFR 107.

*Visual Observer (VO):* A person acting as a flight crew member who assists the small UA remote PIC to see and avoid other air traffic or objects in flight or on the ground.

*Boston Police Department UAS Manager:* A Department member designated by the Police Commissioner to oversee implementation, management, training, documentation, deployments and adherence to current FAA regulations for all UAS owned, maintained, or deployed by the Department. The UAS Manager shall create unit specific SOPs and ensure the safe operation of

all Department Unmanned Aerial Systems. The UAS manager shall be assigned to the Homeland Security Unit of the Bureau of Field Services and report directly to the Unit Commander.

### **Sec. 3 Policy:**

This policy is to establish how designated Boston Police employees will operate (UAS) within the National Airspace System (NAS) within the Boston Police Department. This policy will put processes in place for the deployment and activation of UAS.

Under the direction of the Boston Police Department UAS Manager, develop unit-specific Standard Operating Procedures (SOP's). The Boston Police Department UAS Manager shall be responsible for creating, maintaining and ensuring up-to-date policies, procedures, reports, logs etcetera, as required.

#### **Boston Police UAS Deployments Shall:**

- a) Comply with the United States Constitution
- b) Comply with the Massachusetts Declaration of Rights
- c) Comply with all applicable laws and ordinances
- d) Comply with all Boston Police Department Policies, Procedures, Rules, unit-specific SOP's, and Special Orders
- e) Be approved by the UAS Manager or designee
- f) Ensure that a proper Notice to Airmen (NOTAM) is in place

### **Sec. 4 Prohibited Use:**

Boston Police Department UAS shall not be used for the following:

- a) To conduct personal business of any type
- b) To intimidate, harass, or discriminate against any individual or group
- c) To target a person based solely on individual characteristics, such as, but not limited to race, ethnicity, national origin, religion, disability, gender or sexual orientation
- d) UAS shall not be equipped with weapons of any kind
- e) UAS shall not include facial recognition technology
- f) The use of any UAS by the Boston Police Department is strictly prohibited unless authorized by the UAS manager or designee. Any officer that intentionally uses the UAS without proper authorization or in deviation of the standards set forth in this policy may be subject to disciplinary action.

### **Sec. 5 Privacy Concerns:**

A UAS shall not be intentionally used for viewing, recording or transmitting images and/or video in a criminal investigation at any location or property where a person has a reasonable expectation of privacy unless:

- a) A warrant or court order has been approved for the search of the property

- b) Exigent circumstances exist, including: search and rescue deployments, tactical deployments, crash scenes, fire scenes, hazardous material scenes, and natural disasters
- c) Consent is given by the owner or person responsible for the property is obtained

#### **Sec. 6 Deployment Protocols:**

Consistent with this policy, applicable laws and unit specific SOPs, Department authorized UAS may be deployed including but not limited to, the following:

- a) Search & Rescue deployments
- b) Photographic and video deployments
- c) Motor vehicle crash investigations/crash scene mapping
- d) Criminal investigation & crime scene mapping
- e) Tactical response deployments
- f) Providing an aerial visual perspective to assist officers in providing direction for crowd management, traffic incident management, special circumstances, and temporary perimeter security
- g) Fire services support
- h) Aerial Police Response deployment
- i) Other special events/incidents as assigned by the Commissioner, Superintendent-in-Chief, and/or the Boston Police UAS Manager or designee, consistent with and as permitted by law

#### **Sec. 7 Boston Police Unmanned Aircraft System Manager Responsibilities:**

The Department UAS Manager or designee shall:

- a) Ensure that annual statistics are saved for all UAS deployments
- b) Ensure that all BPD UAS information required to be retained by all applicable laws and ordinances is provided to the Office of the Police Commissioner on an annual basis
- c) Ensure that flight and training records are properly maintained by the appropriate Unit Commander responsible for the use of the unit-specific UAS and forwarded to the Unmanned Aircraft System Manager
- d) Ensure that all unit-specific remote pilots hold a Remote Pilot Certificate with a UAS rating issued by the FAA under 14 CFR 107
- e) Ensure that all Department UAS are registered with the FAA as required by 14 CFR 107
- f) Ensure that all training and licensing is compliant with current FAA regulatory requirements
- g) Ensure that Boston Police Rule 331 collection and storage protocols are in place, and properly performed
- h) Ensure that, for each deployment, a notice to airmen (NOTAM) protocols are in place

- i) Ensure that acquisition protocols are properly utilized

## **Sec. 8 Operational Protocols:**

All Department requests for UAS deployments shall be directed to the Boston Police Department Operations Division. Upon receiving a request for an UAS deployment the Operations Division shall immediately notify and relay all pertinent information to the UAS Manager or designee of the UAS request.

The UAS Manager, the appropriate Unit Commander or the Remote PIC may decline, cancel, or terminate any UAS request due to:

- a) Safety, weather, visibility
- b) Type of request is beyond the UAS or crew member's capability
- c) Availability
- d) Mechanical maintenance of the UAS
- e) Determination that use of the UAS is not the appropriate resource after operational risk assessment or resource assessment is completed
- f) Determination that the use of the UAS is in violation of this policy or Massachusetts General Laws
- g) All UAS deployments will be flown in compliance with all current FAA Regulations including but not limited to 14 CFR 107. The Remote PIC has final authority and responsibility for the operation conducted under 14 CFR 107

## **Sec. 9 Training:**

Boston Police Department employees selected to be Remote PIC's shall:

- a) Be properly trained and licensed as required by 14 CFR 107
- b) Satisfy and maintain all the conditions of the Certificate of Authorization (COA) issued by the FAA if applicable
- c) Have a working knowledge of the airspace intended for deployment and air traffic control communications requirements
- d) Have the ability to obtain and interpret weather information

Boston Police Department employees selected to be Visual Observers shall:

- a) Be properly trained according to standards set by the UAS Manager or designee that comply with FAA current regulatory requirements if any
- b) Satisfy and maintain all the conditions of the COA issued by the FAA if applicable

**Sec. 10 External Release of UAV Video Recordings and Photography:**

- a) UAVs must be operated at such an altitude, speed, and with a planned flight pattern that will ensure that inadvertent video recordings or photos of private spaces of third parties are avoided or minimized
- b) Should any video or still images captured during UAV use contain any personally identifiable information, the Department shall handle as it handles all personally identifiable information collected in the course of any investigation per local, state, and federal statutes
- c) All UAV recordings related to an ongoing criminal investigation or in support of a prosecution may be provided by the commanding officer of the appropriate unit to the applicable law enforcement entity. Should a unit officer receive a subpoena for UAV footage, the officer shall direct the subpoena as soon as practicable to the commander of their unit, with a copy to the Office of the Legal Advisor. UAV recordings may be requested by the public pursuant to a public records request (M.G.L. c. 66 §10). If an officer or commander receives a request for UAV recording from the Media, the request shall be directed to the Office of Media Relations. All other requests for UAV recordings, including victim or witness requests, shall be directed to the Office of the Legal Advisor
- d) UAV footage is the sole property of the City of Boston and shall be retained per the Massachusetts Statewide Retention Schedule



Gregory P. Long  
Superintendent In Chief



Number: SO 16-031

Date: 10/19/2016

Post/Mention: Indefinite

SUBJECT: AUTOMATED LICENSE PLATE RECOGNITION SYSTEM

Section 1. Purpose

The purpose of this Special Order is to establish a policy and procedures to ensure the proper use of Automated License Plate Recognition (“ALPR”) systems by employees of the Boston Police Department.

Section 2. Policy

The ALPR system is a computer-based system that utilizes special cameras to capture license plate information. The ALPR system captures an infrared image of a license plate and converts it to a text file using Optical Character Recognition (“OCR”) technology. The text is compared to various Vehicle of Interest (“VOI”) lists generated by various law enforcement agencies, including the National Crime Information Center (“NCIC”), the Massachusetts Department of Criminal Justice Information Services (“CJIS”) and the Boston Police Department and generates an alert when there is a hit. The ALPR system will identify a license plate and/or a motor vehicle, but will not identify the person operating the motor vehicle. The Department may, as a separate step and for legitimate law enforcement purposes as set forth in this Special Order, undertake to identify the owner of a vehicle in the event the ALPR system generates an alert, such as by running the license plate number through the database of the Massachusetts Registry of Motor Vehicles (“RMV”) or CJIS.

It shall be the policy of the Boston Police Department that all members abide by the policy and procedures set forth in this Special Order when using ALPRs to scan, detect, and identify vehicles or persons of interest, thereby increasing the efficiency and effectiveness of its public safety efforts in a manner that safeguards the privacy concerns of law-abiding citizens.

The ALPR system shall be restricted to legitimate law enforcement uses for the purpose of furthering legitimate law enforcement goals and enhancing public safety. Such uses and goals include, but are not limited to, providing information to officers that will assist in on-going criminal investigations, crime prevention, crime detection, the apprehension of wanted persons, ensuring the safety of vulnerable individuals through the recovery of missing and endangered persons, and improving the quality of life in our community through the identification and removal of stolen motor vehicles.

The Department shall utilize VOI lists that further the above-specified goals of the ALPR system where there is a legitimate and specific law enforcement reason for identifying a vehicle or a person reasonably believed to be associated with that vehicle.

Section 3. Definitions

Section 3.1. Alert: An electronic, visual and /or auditory notice or alarm that is triggered when

the ALPR system receives a potential hit on a license plate.

Section 3.2. Alert data: Information captured by an ALPR relating to a license plate that may match the license plate on a VOI list.

Section 3.3. ALPR data: Scanned files, alert data, and any other documents or other data generated by or through utilization of the ALPR system.

Section 3.4. ALPR system: The ALPR camera and all associated equipment and databases.

Section 3.5. Hit: A read potentially matched to a license plate that has previously been registered on an agency's vehicle plates VOI list, such as those associated with vehicles that have been stolen, vehicles associated with Amber Alerts, vehicles wanted for specific crimes, vehicles associated with, or that may assist with the identification of, suspects involved in criminal activity.

Section 3.6. Read: Digital images of license plates and associated metadata (e.g., date, time, and geographic coordinates associated with the vehicle image capture) that are captured by the ALPR system.

Section 3.7. Scan file: Data obtained by an ALPR of license plates that were read by the device, including potential images of the plate and vehicle on which it was displayed, and information regarding the location of the Department vehicle or fixed location at the time of the ALPR read.

## Section 4. Management of the ALPR System

Section 4.1. Overall System Management. The Technology Services Division ("TSD") shall have responsibility for maintaining the ALPR database, including but not limited to, inventory, service and maintenance of the system. TSD shall ensure that the ALPR system is maintained in conformity with this Special Order and other Department policies, procedures, rules and regulations.

Section 4.2. Equipment Inspection. Designated, trained personnel shall check equipment on a regular basis to ensure functionality and camera alignment. Any equipment that falls outside expected functionality shall be corrected or removed from service until deficiencies have been corrected.

Section 4.3. Damaged or Malfunctioning Equipment. Damage or other malfunctions to the equipment will be reported to the Duty Supervisor or the Commanding Officer of the Auto Theft Unit, as appropriate.

## Section 5. ALPR Operations

Section 5.1 Installation and Functioning. The ALPR cameras will be mounted on Department vehicles and at fixed locations. Scanned data files collected by the ALPR camera will, on an ongoing basis, be automatically uploaded from the ALPR in the vehicle or the fixed location to the Department's ALPR server. The ALPR system will not have sound recording capability.

Section 5.2. Mobile Unit Assignment. The Commissioner or his/her designee may assign, at his or her discretion, officers to the police motor vehicles equipped with the ALPR for use in investigations, in response to a major crime or incident, or for any other legitimate law enforcement purpose.

Section 5.3. VOI Lists. Designation of VOI lists to be utilized by the ALPR system shall be made by the Commissioner or his/her designee. VOI lists shall be obtained or compiled from sources as may be consistent with the purposes of the ALPR system set forth in this Special Order, and shall be regularly uploaded so the lists remain current. Sources for the lists may include, but are not limited to:

1. Automated NCIC and CJIS databases, including the stolen car list;
2. Amber Alerts; and
3. Department-generated VOI list(s) or manual entries of license plates.

Section 5.4. Manual Plate Entry Process.

Section 5.4.1. Manual Plate Entry of Plate Numbers to VOI List. The Operations Division Supervisor shall have the responsibility for manual entry of plate numbers to the VOI list. All requests for entry of plate numbers to the VOI list shall be made in writing (paper or electronic) to the Operations Division Supervisor by a sworn officer of the rank of Sergeant or above. Whenever a license plate number is manually entered into the ALPR system, the employee requesting the manual plate entry shall document the reason for doing so.

Section 5.4.2. Manual Plate Entry Notification. The Operations Division shall notify TSD of manual entry of plate numbers. The Operations Division shall notify TSD of the name of the officer who made the request, as well as the date and time of the request.

Section 5.4.3. Manual Plate Removal. TSD shall send a list of plate numbers on the manual entry list to the appropriate Bureau Chief monthly for confirmation that the plates should remain on the manual entry list.

Section 5.5. Notification of VOI List Alerts/Hits at Fixed Locations. Notification of alerts or hits to the ALPR system from fixed locations shall be routed as follows:

1. Manual Entry Plates. Notification of an alert or hit to a license plate number that has been entered manually into the VOI list shall be automatically sent to the Operations Division for immediate verification and follow up action, as necessary. Notification shall also be routed electronically to the officer who requested the manual plate entry.
2. Amber Alerts. Notification of an alert or hit to a license plate number related to an Amber Alert shall be automatically sent to the Operations Division for immediate verification and follow up action, as necessary.
3. Stolen Vehicles. Notification of an alert or hit to a license plate number that is related to a stolen vehicle shall be automatically sent to the Commander of the Auto Theft Unit and to the Operations Division for immediate verification and follow up action, as necessary.
4. Other Automated NCIC/CJIS databases. Notification of an alert or hit to a license plate

number that is related to an automated NCIC/CJIS database shall be automatically sent to the Operations Division for immediate verification and follow up action, as necessary.

Section 5.6. Login/Log-Out Procedure. To ensure proper operation and facilitate oversight of the ALPR system, officers assigned to a vehicle with ALPR shall login to the ALPR system at the beginning of a tour of duty and shall log-out of the ALPR system at the end of a tour of duty.

Section 6. Authorized Usage of ALPR. Only Department employees trained in its use and this Special Order may operate the ALPR system or access or use stored ALPR data. Each authorized Department employee shall be issued an individual log-in ID and be required to utilize alphanumeric passwords consisting of a combination of upper and lower case letters, numbers, and symbols.

Section 6.1. Permitted Uses. Authorized Department employees may only access the ALPR system and / or use, release or disseminate ALPR data for legitimate law enforcement purposes.

Section 6.2. Prohibited Uses. The following uses of the ALPR system are specifically prohibited:

1. Invasion of Privacy. Except when done pursuant to a court order, it is a violation of this Special Order to utilize the ALPR to record license plates except those of vehicles that are exposed to public view (*e.g.*, vehicles on a public road or street, or that are on private property but whose license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a business establishment).
2. Harassment / Intimidation. It is a violation of this Special Order to use the ALPR system, associated data or VOI lists to harass and/or intimidate any individual or group.
3. Use Based on a Protected Characteristic. It is a violation of this Special Order to use the ALPR system, associated data or VOI lists solely because of a person's race, gender, ethnicity, sexual orientation, disability or other classification protected by law.
4. Personal Use. It is a violation of this Special Order to use the ALPR system, associated data or VOI lists for any personal purpose.
5. First Amendment Rights. It is a violation of this Special Order to use the ALPR system, associated data or VOI lists for the purpose of infringing upon any individual's or group's First Amendment rights.

Section 6.3. Disciplinary Action for Prohibited Use. Any employee who engages in an impermissible use of the ALPR system, associated data or VOI lists may be subject to disciplinary action up to and including termination.

Section 7. Police Action as a Result of ALPR Alert or Hit When Operating a Mobile Unit.

Section 7.1. Hit / Alert Verification. VOI lists utilized by the Department's ALPR system may be updated by agency sources more frequently than the Department may be uploading them,

and the Department's ALPR system will not have access to real time data. Further, there may be errors in the ALPR's read of a license plate. Therefore, an alert alone shall not be a basis for police action (other than following the VOI). Prior to initiation of a stop of a vehicle or other intervention based on an alert received by an officer operating ALPR in a police vehicle, an officer shall do the following before proceeding:

1. Verify the current status on VOI list. Officers must receive confirmation, from an Operations Division dispatcher or the Mobile Data Terminal, that the license plate is still reported stolen, wanted, or otherwise of interest.
2. Visually verify the license plate number and vehicle type. Officers shall visually verify that the license plate on the vehicle of interest matches identically with the image of the license plate number captured (read) by the ALPR, including both the alphanumeric characters of the license plate and the state of issue.
3. Notify the Operations Division. Officers shall notify the Operations Division of an Alert or Hit.

Section 7.2. Vehicle Stops based on ALPR. All stops of motor vehicles must be constitutionally valid and otherwise comply with the Department's Rules and Procedures. Depending on the reason associated with the license plate's placement on a VOI, there may not be sufficient justification for stopping the vehicle based on the hit alone; therefore to assist with implementation of these obligations and in furtherance of the purposes of the ALPR system, the following requirements apply to traffic stops:

1. Completed Verification of the Alert or Hit. An officer must have complied with Section 7.1 above prior to proceeding with a motor vehicle stop.
2. Non-encounter alerts. In the event that an alert is designated as a non-encounter alert, the officer shall follow any instructions included in the alert.
3. Persons of Interest. With regard to cases in which an alert may indicate a person of interest, such as a wanted person, officers are reminded that in some cases, the driver or occupant of the vehicle may not be the person with whom the license plate is associated. Therefore, officers must develop a reasonable belief that the operator or occupant is the person of interest included in a VOI list prior to initiating a stop.
4. Independent reason for traffic stops. An officer may stop a vehicle where he/she has an independent reason for doing so, such as an unrelated traffic violation.
5. Appropriate police action. Nothing in this Special Order shall restrict or prohibit an officer from taking appropriate police action based on facts or reasons obtained independently from ALPR operation.

Section 8. Security and Confidentiality of ALPR. ALPR data shall be kept in a secure data storage system with access restricted to authorized persons only. The ALPR system, associated data and VOI lists will be considered confidential information to the extent permitted by law.

Section 9. Retention. Scanned data will be retained for a period of thirty (30) days. Data required for investigatory purposes, evidentiary purposes, by court order, or by law will be retained as appropriate.

Section 10. Reporting Successful Uses. All successful uses of the ALPR shall be documented and forwarded to the employee's Commanding Officer. The Commanding Officer will compile statistics of these successful uses and provide monthly updates on such uses to the Commanding Officer's Bureau Chief.

Section 11. Usage Audit. The Audit and Review Unit will be responsible for conducting, reviewing and retaining audits of the ALPR system usage. Audits shall be completed on a periodic basis and shall determine the Department's adherence to this Special Order and the procedures it establishes, as well as the maintenance and completeness of records contemplated by this Special Order. At the completion of this audit, a full report on the outcome shall be forwarded to the Commissioner. Audits shall include, but not be limited to, a review of the following:

1. Records of ALPR operators and their ALPR usage, including vehicles of interest added to a VOI list by individual officers.
2. A listing of access to the police Department's server, in order to verify security of that data and compliance with this Special Order. All written requests for scanned file access will be retained for comparison against the audit record.
3. Records of reproduction of scan files pursuant to Section 12 below.

## Section 12. Reports and Requests for ALPR Data

Section 12.1. Reports. TSD shall produce ALPR usage reports on a regular basis and/or upon request to the Bureau of Investigative Services, the Bureau of Field Services, the Bureau of Intelligence and Analysis, or the Police Commissioner or his designee.

Section 12.2 Internal Requests for ALPR Data. Sworn Department personnel of the rank of Sergeant and higher are authorized to make a request to TSD for a copy of scan files. Whenever an internal request for scan files is made, the employee making the request shall document the reason for the request. Requests may be made only for legitimate law enforcement purposes, as part of normal procedures for investigations and the handling of evidence or in furtherance of the purposes for the ALPR system stated in this Special Order. TSD shall be responsible for making reproductions of scan files. TSD shall document all requests for copies of scan files.

### Section 12.3. External Requests for ALPR Data.

Section 12.3.1. Mutual Aid Requests. The Operations Division Duty Supervisor may approve a mutual aid request for use of the ALPR for purposes consistent with this Special Order, as may be appropriate under the circumstances and as resources permit. Operations Division Duty Supervisors are encouraged to provide mutual aid to other communities when they become aware of a serious incident, as to which serious incident

they reasonably believe the ALPR may be useful. Examples of serious incidents include homicides, shootings, kidnappings, sexual assaults or AMBER alerts, or other serious or violent felonies as to which suspect vehicle information is available.

Section 12.3.2. Court Orders / Requests from Prosecutors / Subpoenas. All ALPR data requests submitted in connection with open investigations shall be processed through the employee assigned to the investigation to TSD. Requests not associated with an open investigation shall be forwarded to the Office of the Legal Advisor for handling.

Section 12.3.3. Requests from Media. All ALPR records requests for ALPR data from the media shall be forwarded to the Office of Media Relations for handling.

Section 12.3.4. Other Public Records Requests. All non-media public records requests for ALPR data shall be forwarded to the Office of the Legal Advisor for handling.

William B. Evans Police Commissioner



## **Police Commissioner's Special Order**

Number: SO 21-25

Date: May 25, 2021

Post/Mention: Indefinite

### **SUBJECT: DIVERSITY, EQUITY AND INCLUSION (DEI) POLICY**

As part of the Boston Police Department's ongoing commitment to police reform and the recommendations of Mayor Walsh's Task Force on Police Reform the BPD created a Diversity, Equity and Inclusion (DEI) policy for the Department. This policy has been reviewed by an internal BPD DEI committee as well as the Mayor's Office of Equity.

#### **Commitment to Diversity, Equity and Inclusion**

The Boston Police Department is committed to fostering, cultivating and preserving a culture of diversity, equity and inclusion throughout the department.

Boston Police Department employees -- sworn and civilian -- are our most valuable asset. The men and women of the Boston Police Department are dedicated public servants who work hard every day to serve the community. We are confident in their abilities to identify and work to address barriers to diversity, equity and inclusion. The Boston Police Department is guided by community policing, community engagement, and procedural justice; with the communities we serve as well as our community of employees.

We understand that trust is built by working closely with the community and treating people with dignity and respect. The Boston Police Department prioritizes diversity, equity and inclusion in recruitment, hiring, promotion, opportunities for career advancement (i.e. assignments, professional development and trainings), and retention within the confines of the law, Civil Service and collective bargaining obligations.

#### **Definitions**

**Diversity** -- all aspects of human difference, social identities, and social group differences, including but not limited to race, ethnicity, gender identity, sexual orientation, socio-economic status, language, culture, national origin, religion/spirituality, age, (dis)ability, military/veteran status, political perspective, and associational preferences.



**Equity** -- fair and just practices and policies that ensure all community members can thrive. Equity is different than equality in that equality implies treating everyone as if their experiences are exactly the same. Being equitable means acknowledging and addressing structural inequalities — historic and current — that advantage some and disadvantage others.

**Implicit bias**<sup>1</sup> – refers to the attitudes or stereotypes that affect our understanding, actions, and decisions in an unconscious manner.

- Impacts well-intentioned people outside of conscious awareness.
- The discriminatory behavior is not based on animus and is not deliberate.

**Inclusion** -- a community where all members are and feel respected, have a sense of belonging, and are able to participate and achieve to their potential.

**Procedural Justice**<sup>2</sup> – the procedures used by law enforcement officers where community members are treated with respect, dignity, and fairness. The four elements of procedural justice are:

- *Respect* – treat people with dignity
- *Trustworthiness* – convey worthy intentions, professional competence, and good character
- *Voice* – allow a person to share his/ her/ their point of view
- *Neutrality* – make bias free decisions

### **Importance of Diversity in Building Trust with the Community**

Diversity within law enforcement agencies – including but not limited to race, ethnicity, sex, gender identity, sexual orientation, socio-economic status, language, culture, national origin, religion/spirituality, age, (dis)ability, military/veteran status, political perspective, background and experience -- is critical to building trust with the communities they serve. Research has found that:

*“... when members of the public believe their law enforcement organizations represent them, understand them, and respond to them – when communities perceive authorities as fair, legitimate and accountable – it deepens trust in law enforcement, instills public confidence in government, and supports the integrity of democracy. This trust is essential to defusing tension, to solving crimes, and to creating a system in which residents view law enforcement as fair and just. Victims and witnesses of crime may not approach or engage with law enforcement if they do not perceive such authorities to be responsive to their experiences and concerns. This trust – and the cooperation it facilitates – also enables officers to more effectively and safely perform their jobs.”<sup>3</sup>*

---

<sup>1</sup> This definition is taught at the Boston Police Academy to recruits in the Fair and Impartial Policing curriculum.

<sup>2</sup> This definition is taught at the Boston Police Academy to recruits in the Fair and Impartial Policing curriculum.

<sup>3</sup> Advancing Diversity in Law Enforcement, U.S. Department of Justice and U.S. Equal Employment Opportunity Commission. October 2016. Pg. ii

The Boston Police Department is committed to strengthening relationships and building trust with the community. The BPD's model of community policing and engagement has been recognized nationally. This model includes extensive outreach; innovative programs, events and activities; and connecting those in need with services, supports and opportunities.

The Boston Police Department understands that a key element of building trust is by having a department that not only reflects, but represents the community. BPD has taken significant steps to increase diversity within the sworn police force by 1) reinstating the Cadet Program in 2015, 2) hiring a fulltime Diversity Recruitment Officer/ Promotional Exam Administrator in 2017, and consistently requesting language preference lists from the Civil Service Commission. Affinity groups also play an important role in recruitment.

### **Importance of Diversity, Equity and Inclusion within the Department**

The Boston Police Department embraces and encourage employees' differences in lived experience, race, ethnicity, sex, gender identity, sexual orientation, socio-economic status, language, culture, national origin, religion/spirituality, age, (dis)ability, military/veteran status, political perspective, and other characteristics that make our employees unique and able to connect with the diverse communities we serve.

Affinity groups such as: Benevolent Asian Jade Society of New England, Cabo Verde Police Association, Emerald Society of the Boston Police, Gay Officers Action League (GOAL) of New England, Latino Law Enforcement Group of Boston (LLEGO), Massachusetts Association of Italian American Police Officers, Massachusetts Association of Minority Law Enforcement Officers (MAMLEO), Massachusetts Association of Women in Law Enforcement (MAWLE), and Women in Blue are critical to the advancement of diversity, equity and inclusion within the Department through advocacy and mentoring.

All employees of the Boston Police Department have a responsibility to treat others with fairness, dignity and respect at all times – whether that is engaging with the public or with fellow employees. (See Rule 113 Public Integrity Policy, Rule 113A Bias Free Policing, Rule 113B Transgender Policy, and Rule 114 Sexual Harassment, Discrimination, Harassment, and Retaliation Policy and Complaint Procedure.)

### **Training**

The Boston Police Department is committed to ensuring that our police officers receive training in fair and impartial policing. This includes procedural justice and implicit bias. Officers also receive training in the constitutionality and proper documentation of police interactions in order to reduce the effects of implicit bias and more effectively serve the diverse communities they represent.

**Accountability**

Employees who believe they have been subjected to any kind of discrimination or have witnessed discrimination by other BPD employees should report the incident pursuant to Rule 114 Sexual Harassment, Discrimination, Harassment, and Retaliation Policy and Complaint Procedure. Any employee found to have exhibited any inappropriate conduct or behavior against others may be subject to disciplinary action per Rule 109 Discipline Procedure.

Gregory P. Long  
Superintendent In Chief



## Police Commissioner's Special Order

Number:	SO 21-46
Date:	10/1/21
Post/Mention:	Indefinite

### **SUBJECT: OUTSIDE AGENCY NOTIFICATION**

When an outside law enforcement agency conducts an operation or investigation in the City of Boston that may impact public safety or the safety of Department personnel or the personnel of the outside agency, that law enforcement agency should contact the duty supervisor of the district of occurrence or appropriate unit supervisor to advise of their intended presence and activity, i.e. arrest warrant or search warrant and location. The Department recognizes that not all activity within the City of Boston by an outside agency will require notification.

When a member of the Department receives notification from an outside agency that the agency intends to conduct an investigation or operation the Department member shall forward the caller to the duty supervisor or unit supervisor. The supervisor shall obtain pertinent information, keeping in mind the need for operational integrity and officer safety. The supervisor shall notify the Operations Division supervisor, district duty supervisor and appropriate unit supervisor. In accordance with Department rules and regulations, including Rule 334 Search Warrant Application and Execution, appropriate Department resources shall be deployed to assist with the operation or investigation as needed. If a member of the Boston Police Department is a liaison with an outside agency that is conducting an investigation or operation in the City of Boston, that Department member should follow this protocol.

During the duration of the outside agency's operation or investigation, the Operations Division supervisor, dispatcher, district duty supervisor and unit supervisor shall monitor the respective BPD channel for communications relating to the operation/investigation, i.e., 911 calls of public concern or awareness of the operation, need for additional resources and the termination of the investigation/operation.

The supervisor shall consult with the outside agency regarding the completion of a 1.1 to document the incident. If a 1.1 will not compromise the integrity of the investigation or officer safety, the duty supervisor or unit supervisor shall ensure that a 1.1 incident report titled (Assist Outside Agency) is completed. However, whenever a person is taken into custody, force is deployed or property is damaged by another agency or BPD personnel, a 1.1 shall be completed.

Gregory P. Long  
Superintendent In Chief



**Police Commissioner's Special Order**

Number: SO 22- 8

Date: April 22, 2022

Post/Mention: Indefinite

**SUBJECT: BOSTON POLICE DEPARTMENT VIDEO MANAGEMENT SYSTEMS  
POLICY**

BPD video management systems are covered by the City of Boston Surveillance Ordinance, and as such will be included in the Boston Police Department's surveillance policy to be presented to the Boston City Council later this year.

The Boston Police Department's video management systems are also governed by the Metro Boston Homeland Security Region's Critical Infrastructure Monitoring System (CIMS) Closed Circuit Television (CCTV) Policy.

The Video Management Systems Policy ensures that comprehensive protections are in place regarding video management systems access, usage, and retention,

This special order is hereby issued superseding all previous rules, special orders, memos and directives on this subject and is effective immediately.

Commanding Officers shall ensure that this order and policy are posted on Department bulletin boards.

Gregory P. Long  
Superintendent In Chief

## **BOSTON POLICE DEPARTMENT VIDEO MANAGEMENT SYSTEMS POLICY**

### **Introduction**

The Boston Police Department is dedicated to ensuring public safety in our neighborhoods while balancing civil rights and privacy protections. Video management systems are a tremendous tool for the department in criminal investigations, at large scale events, to protect critical infrastructure and other official law enforcement purposes.

The Boston Police Department's video management systems are governed by the Metro Boston Homeland Security Region's Critical Infrastructure Monitoring System (CIMS) Closed Circuit Television (CCTV) Policy. The BPD VMS Systems Policy is consistent with, and builds on the MBHSR policy.

This policy defines procedures that limit access and use of video management systems as well as provide important privacy and civil rights protections for individuals while in the City of Boston.

### **Definitions**

**CCTV.** Closed circuit television

**Video Management System (VMS).** The software and hardware that provides access and system administration of CCTV video cameras under the management of the Boston Police Department.

**MBHSR.** Metro Boston Homeland Security Region, which consists of Boston, Brookline, Cambridge, Chelsea, Everett, Quincy, Revere, Somerville, and Winthrop.

**CIMS.** Critical Infrastructure Monitoring System.

**System Administrator.** Person(s) allowed to grant and oversee access to the CIMS/VMS network. The Commander of the BPD Video Evidence Unit and the Director of BPD Telecommunications are designated system administrators.

### **Urban Area Security Initiative (UASI):**

In July 2003, the U.S. Department of Homeland Security (DHS), under the Office of Domestic Preparedness, designated Boston and the surrounding cities and towns a high-risk urban area, qualifying it for regional grant funding under the Urban Areas Security Region (UASI) program. Through the UASI program, DHS has since provided annual funding to build and sustain regional capabilities to prevent, protect, respond, and recover from acts of terrorism. The Boston UASI Region, or Metro Boston Homeland Security Region (MBHSR), includes Boston, Brookline, Cambridge, Chelsea, Everett, Quincy, Revere, Somerville and Winthrop. The MBHSR has utilized UASI grant funding to augment the purchase of infrastructure and sustainment services for the CIMS/VMS.

### **CIMS/VMS Administration.**

The Police Commissioner or his/her designee will designate the number of System Administrators allowed to grant and oversee access to the CIMS/VMS network. Those designated System Administrators have the ability to create groups and assign permissions based upon job function or

## Appendix Y

assignment.

Permissions are determined by the System Administrator and include the capabilities to view, rewind, download, or restrict camera footage. System Administrators are designated based upon their subject matter expertise to the MBHSR CIMS program and do not hold operational functions that would create a conflict of interest.

A requesting jurisdiction within the MBHSR will have the ability to view images/video produced by the CIMS/VMS cameras only after the BPD has authorized and granted such access. The Police Commissioner or their designee shall have exclusive authority to authorize other jurisdictions within the MBHSR access to footage recorded by the CIMS/VMS cameras. Access will only include live viewing and/or review viewing (rewinding). It will not include the ability to download or record. Please see the **Video Retention and Preservation** section for the process to request downloaded video footage from the Video Evidence Unit.

### **VMS Camera System**

Boston and the other jurisdictions in the MBHSR each have and maintain their own camera systems. The VMS Camera System that operates across the region is maintained by a service vendor for the interoperable communication and technology between agencies in MBHRS. It is the policy and practice of the Boston Police Department to provide access to VMS camera systems in Boston to other MBHSR jurisdictions on a case-by-case basis and pursuant to this policy. There are a limited number of outside agencies who have ongoing access to view or review view (rewind) a subset of cameras on the VMS camera system for public safety purposes. See **Appendix A** for a list of these agencies and the number of cameras they each have access to.

### **Access Protocol**

#### **Boston Police Department Personnel**

All BPD personnel who require or request access to view the live feed of the VMS Camera System are approved through the BPD Bureau of Administration and Technology (BAT). The BAT/Video Evidence Unit (VEU) will create user groups that will administratively allow access to certain cameras within the VMS system for department employees that have been granted permission to use the system. All activity is recorded each time an employee logs into the system. All user activity is logged and maintained by the department.

#### **Outside Jurisdictions**

Any request for live feed access made by an outside jurisdiction is reviewed for approval through the BPD Bureau of Administration and Technology. If granted, the BPD Telecommunications system administrator will make the necessary steps to activate the connection. If approved, access is granted for a specific time period and only for cameras relevant to the request. This approval and access process will be documented and maintained by the Bureau of Administration and Technology.

### **System Maintenance**

The overall maintenance, purchasing, and installation of the VMS Camera System is administered by the BPD Telecommunications Unit. After the data is recorded it is under the administration of the BPD Video Evidence Unit. The Video Evidence Unit will assist department employees who

## Appendix Y

apply for access to the VMS system.

### **VMS Use**

The BPD VMS camera system is used for official law enforcement purposes only. Anyone who engages in an impermissible use of the MBHSR CIMS or BPD VMS Camera System may be subject to criminal prosecution, civil liability, and/or administrative sanctions up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and Department policies.

Violations of this policy occur when an individual utilizes the MBHSR CIMS network for purposes including but not limited to;

- **Invasion of Privacy.** Except pursuant to a court order, it is a violation of this Policy to observe, or record footage of, locations except those that are in public view from a vantage point that is accessible to the general public and where there is no reasonable expectation of privacy. Areas in which there is a reasonable expectation of privacy include the interior of private premises such as a home.
- **Harassment / Intimidation.** It is a violation of this Policy to use the MBHSR CIMS or BPD VMS to harass and/or intimidate any individual or group.
- **Use / Observation Based on a Protected Characteristic.** It is a violation of this Policy to use the MBHSR CIMS or BPD VMS to observe individuals solely because of their race, gender, ethnicity, sexual orientation, disability or other classification protected by law.
- **Personal Use.** It is a violation of this Policy to use the MBHSR CIMS or BPD VMS for any personal purpose.
- **First Amendment Rights.** It is a violation of this Policy to use the MBHSR CIMS or BPD VMS for the purpose of infringing upon First Amendment rights.

### **Video Retention and Preservation**

VMS video shall only be downloaded and copied by members of the Video Evidence Unit. BPD requests for archived VMS video shall only be accepted via an internal request link that can be found on the BPD intranet. That request will be logged and processed once it is received. The Video Evidence Unit is the keeper of records for all requests made via the Department website as well as subpoenas.

Recorded video is retained for 30 days unless a request has been made to preserve the footage from a BPD employee, an outside law enforcement agency, or from internal personnel fulfilling a Public Records Request or subpoena.



**APPENDIX A**

Outside Agencies with ongoing access to BPD VMS cameras:

- United States Coast Guard -- 21 cameras (VIEW ONLY)
- Brookline Police Department -- 8 cameras (VIEW ONLY)

2021



## Boston Regional Intelligence Center *Privacy, Civil Rights, and Civil Liberties Protection Policy*

The Intelligence Reform and Terrorism Prevention Act of 2004, as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007, established an information sharing environment for the sharing of terrorism-related information while protecting the privacy, civil rights, and civil liberties of individuals. The *Guidelines to Ensure That Information Privacy and Other Legal Rights of Americans Are Protected in the Development and Use of the Information Sharing Environment* (“ISE Privacy Guidelines”) require that relevant entities, including fusion centers, have a written privacy protection policy in place that is “at least as comprehensive” as the ISE Privacy Guidelines.

This policy, produced by the Boston Regional Intelligence Center Privacy Committee, in collaboration with Boston Police Department’s Office of the Legal Advisor, was reviewed and approved by the U.S. Department of Homeland Security Privacy and Civil Liberties Sub-Interagency Policy Committee on November 3, 2010, and was determined to be “at least as comprehensive” as the ISE Privacy Guidelines. The policy as implemented is intended to govern how the Boston Regional Intelligence Center will handle personally identifiable information and all other personal, sensitive information it seeks, receives, and uses in the normal course of law enforcement, public safety, and intelligence operations.

## **A. Table of Contents**

<b>A. PURPOSE STATEMENT.....</b>	<b>3</b>
<b>B. POLICY APPLICABILITY AND LEGAL COMPLIANCE .....</b>	<b>3</b>
<b>C. GOVERNANCE AND OVERSIGHT .....</b>	<b>3</b>
<b>D. TERMS AND DEFINITIONS .....</b>	<b>4</b>
<b>E. INFORMATION.....</b>	<b>4</b>
<b>F. ACQUIRING AND RECEIVING INFORMATION.....</b>	<b>7</b>
<b>G. INFORMATION QUALITY ASSURANCE .....</b>	<b>8</b>
<b>H. COLLATION AND ANALYSIS .....</b>	<b>8</b>
<b>I. MERGING RECORDS .....</b>	<b>9</b>
<b>J. SHARING AND DISCLOSURE .....</b>	<b>9</b>
<b>K. REDRESS.....</b>	<b>11</b>
K.1 DISCLOSURE.....	11
K.2 CORRECTIONS .....	11
K.3 APPEALS.....	11
K.4 COMPLAINTS.....	11
<b>L. SECURITY SAFEGUARDS.....</b>	<b>12</b>
<b>M. INFORMATION RETENTION AND DESTRUCTION .....</b>	<b>13</b>
<b>N. ACCOUNTABILITY AND ENFORCEMENT.....</b>	<b>13</b>
N.1 INFORMATION SYSTEM TRANSPARENCY .....	13
N.2 ACCOUNTABILITY.....	14
N.3 ENFORCEMENT .....	14
<b>O. TRAINING.....</b>	<b>15</b>
<b>APPENDIX A: TERMS AND DEFINITIONS .....</b>	<b>16</b>
<b>APPENDIX B: APPLICABLE LEGAL REFERENCES.....</b>	<b>26</b>

## **A. PURPOSE STATEMENT**

The purpose of this privacy, civil rights, and civil liberties protection policy is to help ensure that the Boston Regional Intelligence Center (hereafter “BRIC” or “the center”) personnel and individuals assigned to the BRIC comply with applicable federal, state, local, and tribal law and assist the center and its participants in:

- Ensuring individual privacy, civil rights, civil liberties, and other protected interests.
- Increasing public safety and improving national security.
- Protecting the integrity of systems for the observation and reporting of public safety matters, including terrorism-related and other criminal activity and information.
- Encouraging individuals or community groups to trust and cooperate with the justice system.
- Promoting governmental legitimacy and accountability.
- Making the most effective use of public resources allocated to public safety agencies.

## **B. POLICY APPLICABILITY AND LEGAL COMPLIANCE**

1. All BRIC personnel (including, but not limited to, individuals assigned to the BRIC from other agencies and individuals providing various support services) and authorized users will comply with:
  - a. Applicable provisions of this privacy policy.
  - b. Applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to, the U.S. Constitution, the Massachusetts Constitution, and applicable law protecting privacy, civil rights, and civil liberties, including, but not limited to, M.G.L. c. 4 §7, M.G.L. c. 6 §172, M.G.L. c. 12 §11H, M.G.L. c. 66 §10, and M.G.L. c. 66A §2, M.G.L. c. 151B, and 42 U.S.C.A. 1983.

This policy applies to information the center gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to center personnel, governmental agencies (including Information Sharing Environment [ISE] participating centers and agencies), and participating justice and public safety agencies, as well as to private contractors, private entities, and the general public.

2. The BRIC will provide a printed or electronic copy of this policy to all of its personnel and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with applicable provisions of this policy.
3. The BRIC has adopted internal operating policies that are in compliance with the U.S. Constitution, the Massachusetts Constitution, and applicable law protecting privacy, civil rights, and civil liberties, including, but not limited to, M.G.L. c. 4 §7, M.G.L. c. 6 §172, M.G.L. c. 12 §11H, M.G.L. c. 66 §10, and M.G.L. c. 66A §2, M.G.L. c. 151B, and 42 U.S.C.A. 1983.

## **C. GOVERNANCE AND OVERSIGHT**

1. Primary responsibility for the operation of the BRIC; its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the Bureau Chief of the Boston Police Department’s Bureau of Intelligence and Analysis and/or the director of the BRIC.

2. The BRIC is guided by a designated Privacy Committee. Members of the committee will be available to address questions and concerns regarding the BRIC's privacy policy, privacy and civil rights protections as provided in this policy, and the center's information gathering and collection, retention, and dissemination processes and procedures. The committee will periodically review and, as necessary, recommend updates to the policy in response to changes in law and implementation experience, including the results of internal reviews. The committee is guided by the BRIC's trained privacy officer, an individual having supervisory responsibilities within the BRIC as appointed by the bureau chief of the Boston Police Department's Bureau of Intelligence and Analysis. The privacy officer serves as the liaison for the Information Sharing Environment, overseeing implementation of and compliance with the ISE Privacy Guidelines and ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies.
3. The BRIC's Privacy Committee will be composed of personnel appointed by the bureau chief of the Boston Police Department's Bureau of Intelligence and Analysis. The Privacy Committee shall consist of individuals, both civilian and sworn law enforcement, having supervisory responsibilities in (a) homeland security, (b) criminal intelligence, and (c) legal compliance. The privacy officer and the Privacy Committee can be contacted at the following address:

Boston Regional Intelligence Center  
Boston Police Department  
Privacy Committee  
One Schroeder Plaza  
Boston, MA 02120  
(617) 343-4328

The Privacy Committee receives reports regarding alleged errors and violations of the provisions of this policy and receives and coordinates complaint resolution under the center's redress policy.

4. The BRIC's Privacy Committee ensures that enforcement procedures and sanctions outlined in Section N.3, Enforcement, are adequate and enforced.

#### **D. TERMS AND DEFINITIONS**

1. The primary terms and definitions used in this privacy policy are set forth in Appendix A, Terms and Definitions.

#### **E. INFORMATION**

1. The BRIC will seek or retain information that:
  - Is based on a possible threat to public safety or the enforcement of the criminal law, or
  - Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal (including terrorist) conduct or activity, or
  - Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime, or

**UNCLASSIFIED**

- Is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches), and
- Is reliable and verifiable or limitations on the quality of the information are identified, and
- Is based on the source agency's good faith belief that the information was acquired in accordance with agency policy and in a lawful manner.

The BRIC may retain protected information that is based on a level of suspicion that is less than "reasonable suspicion," such as tips and leads (including suspicious activity reports [SARs] and ISE-SARs), subject to BRIC policies, procedures, and guidelines.

2. The BRIC will not seek or retain (and originating agencies will agree not to submit) information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations.
3. The BRIC applies labels to agency-originated information to indicate to the accessing authorized user that:
  - The information is protected information as defined in Appendix A of the policy and, to the extent expressly provided in this policy, includes organizational entities.
  - The information is subject to Massachusetts General Law and federal regulations restricting access, use, or disclosure.
4. The BRIC personnel will, upon receipt of information, assess the information to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency has assigned categories to the information) prior to retention to reflect the assessment, such as:
  - Whether the information consists of tips and leads data via formal e-mail, phone, Internet, or incident report submission; criminal history; intelligence information; case records; conditions of supervision; case progress; or other information category.
  - The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector).
  - The reliability of the source (for example, completely reliable, usually reliable, unreliable, unknown reliability).
  - The validity of the content (for example, verified, unverified, and unable to verify).
5. At the time a decision is made by the BRIC to retain information, it will be labeled (by record, data set, or system of records), to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:
  - Protect confidential sources and police undercover techniques and methods.
  - Not interfere with or compromise pending criminal investigations.
  - Protect individuals' right of privacy or their civil rights and civil liberties.
  - Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

6. The labels assigned to existing information under Section E.5, above, will be reevaluated whenever:
  - New information is added that has an impact on access limitations or the sensitivity of disclosure of the information.
  - There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.
7. BRIC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads and SAR information. Center personnel will:
  - Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful. The center will use a standard reporting format and data collection codes for SAR information.
  - Store the information using the same storage method used for data which rises to the level of reasonable suspicion and which includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.
  - Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, “need-to-know” and “right-to-know” access for dissemination for personally identifiable information).
  - Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.
  - Retain information for up to five (5) years in order to work an unvalidated tip or lead or SAR information to determine its credibility and value or assign a “disposition” category (for example, undetermined or unresolved, cleared or unfounded, verified, or under active investigation) so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition category.
  - Adhere to and follow the center’s physical, administrative, and technical security measures to ensure the protection and security of tips and leads.
8. The BRIC incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as information privacy, civil rights, and civil liberties.
9. The BRIC will identify and review all protected information that may be accessed from or disseminated by the center prior to sharing that information. The BRIC will provide notice mechanisms, via document labeling caveats, that will enable authorized users to determine

the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

10. The BRIC requires certain basic descriptive information labels to be entered and electronically associated with data or content for which there are special laws, rules, or policies regarding access, use, and disclosure, including terrorism-related information shared through the ISE. The types of information include:
  - The name of the originating center, department or agency, component, and subcomponent.
  - The name of the center's justice information system from which the information is disseminated.
  - The date the information was collected and, where feasible, the date its accuracy was last verified.
  - The title and contact information for the person to whom questions regarding the information should be directed.
11. The BRIC will attach (or ensure that the originating agency has attached) specific labels and descriptive metadata to information that will be used, accessed, or disseminated to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification.
12. The BRIC will keep a record of the source of all information sought and collected by the center.

#### **F. ACQUIRING AND RECEIVING INFORMATION**

1. Information acquisition and access, as well as investigative techniques used by the BRIC and source agencies, must comply with and adhere to applicable law, regulations, and guidelines, including, but not limited to, M.G.L. c. 6 §172, M.G.L. c. 12 §11H, M.G.L. c. 41 §98, and M.G.L. c. 151B.
2. The BRIC's SAR process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. Law enforcement officers and appropriate center and participating agency staff members will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.
3. The BRIC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights (race, religion, national origin, ethnicity, etc.) and civil liberties (speech, assembly, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.
4. Information-gathering and investigative techniques used by the BRIC and those used by originating agencies should be the least intrusive means necessary in the particular circumstances to gather information the BRIC is authorized to seek or retain.
5. External agencies that access the BRIC's information or share information with the center are governed by the laws and rules governing those individual agencies, including applicable federal and state laws.



6. The BRIC will contract only with commercial database entities that provide an assurance that their methods for gathering personally identifiable information comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and that these methods are not based on misleading information-gathering practices.
7. The BRIC will not directly or indirectly receive, seek, accept, or retain information from:
  - An individual who or a nongovernmental entity that may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or center policy.
  - An individual who or an information provider that is legally prohibited from obtaining or disclosing the information.

#### **G. INFORMATION QUALITY ASSURANCE**

1. The BRIC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources; accurate; current; complete, including the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable standard [refer to Section I, Merging Records] has been met.
2. At the time of retention in the system, the information will be labeled regarding its level of quality (accuracy, completeness, currency, and confidence [verifiability, and reliability]).
3. When errors and/or deficiencies are identified, the BRIC will correct the alleged errors and deficiencies or refer them to the originating agency, in a timely manner, and correct, delete, or refrain from using protected information found to be erroneous or deficient.
4. The labeling of retained information will be reevaluated by the BRIC or the originating agency when new information is gathered that has an impact on confidence (source reliability and content validity) in previously retained information.
5. The BRIC will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that the information will be corrected, deleted from the system, or not used when:
  - a. The center identifies information that is erroneous, misleading, obsolete, or otherwise unreliable; or,
  - b. The center did not have authority to gather the information or to provide the information to another agency.
6. Originating agencies external to the BRIC are responsible for reviewing the quality and accuracy of the data provided to the center. When identified, the BRIC will notify the appropriate contact person in the originating agency, in writing or electronically, if data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.
7. The BRIC will use written or electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the center because the information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

#### **H. COLLATION AND ANALYSIS**

1. Information acquired or received by the BRIC or accessed from other sources will be analyzed only by qualified individuals who have successfully completed a background check

and appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly.

2. Information subject to collation and analysis is information as defined and identified in [Refer to Section E, Information].
3. Information acquired or received by the BRIC or accessed from other sources is analyzed according to priorities and needs and will be analyzed only to:
  - Further crime prevention (including terrorism), law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the center.
  - Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal (including terrorist) activities.
4. At a minimum, all analytical products undergo peer review and, whenever practicable, a supervisory review prior to dissemination.

## I. MERGING RECORDS

1. Records about an individual or organization from two or more sources will not be merged by the BRIC unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization. The set of identifiers sufficient to allow merging will consist of all available attributes that can contribute to a higher accuracy of match.
2. If the matching requirements are not fully met but there is an identified partial match, the information may be associated by the BRIC if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.

## J. SHARING AND DISCLOSURE

1. Credentialed, role-based access criteria will be used by the BRIC, as appropriate, to control:
  - The information to which a particular group or class of users can have access based on the group or class.
  - The information a class of users can add, change, delete, or print.
  - To whom, individually, the information can be disclosed and under what circumstances.
2. The BRIC adheres to the current version of the ISE-SAR Functional Standard for its SAR process, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity with a potential nexus to terrorism.
3. Access to or disclosure of information retained by the BRIC will be provided at designated levels appropriate to the recipient's need and right to know only **to persons within the center or in other governmental agencies** who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health or justice purposes and only for the performance of official duties in accordance with law and procedures applicable to the agency for which the person is working. The center will have a mechanism in place sufficient to allow the identification of each individual who accessed information retained by the center, and the nature of the information accessed will be kept by the center.

UNCLASSIFIED

4. In regards to secondary dissemination, agencies external to the BRIC may not disseminate information accessed or disseminated from the center without approval from the center or other originator of the information, unless otherwise marked.
5. Records retained by the BRIC may be accessed by or disseminated **to those responsible for public protection, public safety, or public health** only for public protection, public safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. An audit trail sufficient to allow the identification of each individual who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.
6. Information gathered or collected and records retained by the BRIC may be accessed or disseminated **for specific purposes** upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law. An audit trail sufficient to allow the identification of each individual who requested, accessed, or received information retained by the center; the nature of the information requested, accessed, or received; and the specific purpose will be kept for no more than five years by the center.
7. Information gathered or collected and records retained by the BRIC may be accessed or disclosed **to a member of the public** only if the information is defined by law to be a public record or otherwise appropriate for release to further the center's mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the center for this type of information. An audit trail sufficient to allow the identification of each individual member of the public who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.
8. Information gathered or collected and records retained by the BRIC **will not** be:
  - Sold, published, exchanged, or disclosed for commercial purposes.
  - Disclosed or published without prior notice to the originating agency that such information is subject to disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency.
  - Disseminated to persons not authorized to access or use the information.
9. There are several categories of records that will ordinarily **not be provided** to the public. The following is not meant to be an exhaustive list but serves as examples of records that will not be subject to public disclosure:
  - Records required to be kept confidential by law. (M.G.L. c. 4 §7(26)(a)).
  - Information **that meets the** definition of "classified information" as that term is defined in the National Security Act, Public Law 235, Section 606, and in accord with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.
  - Investigatory records of law enforcement agencies. (M.G.L. c. 4 §7(26)(f)).
  - A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism, vulnerability assessments, risk planning documents, needs assessments, and threat assessments. (M.G.L. c. 4 §7(26)(n)).

- Protected federal, state, local, or tribal records that were originated and controlled by another agency and were shared with the Department on the condition of confidentiality and nondisclosure, unless otherwise required by law.
10. The BRIC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information unless otherwise required by law.

## **K. REDRESS**

### **K.1 DISCLOSURE**

1. While most personally identifiable information in records maintained by the BRIC is exempt from disclosure under 2. below, an individual who is entitled to know the existence of and to review the information about him or her that has been gathered and retained by the BRIC may obtain a copy of the information and challenge the accuracy or completeness of the information (correction). The center's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests and of what information is disclosed to an individual.
2. The existence, content, and source of the information will not be made available by the BRIC to an individual in certain circumstances, including, but not limited to, when:
  - Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution (M.G.L. c. 4 §7(26)(f)).
  - Disclosure would endanger the health or safety of an individual, an organization, or a community.
  - The information is in a criminal intelligence information system subject to 28 CFR Part 23 [see 28 CFR §23.20(e)].
  - Disclosure is not allowed by state and/or federal law (M.G.L. c. 4 §7(26)(a)).
  - Any other production that would violate state and/or federal law, including, but not limited to, M.G.L. c. 4 §7, M.G.L. c. 6 §172, or M.G.L. c. 66 §10.

### **K.2 CORRECTIONS**

1. If an individual requests correction of information ***originating with the BRIC*** that has been disclosed, the center's privacy officer, on behalf of the Privacy Committee, will inform the individual of the procedure for requesting and considering requested corrections, including appeal rights if requests are denied in whole or in part. A record will be kept of all requests for corrections and the resulting action, if any.

### **K.3 APPEALS**

1. The individual who has requested disclosure or to whom information has been disclosed will be given reasons if disclosure or requests for corrections are denied by the Privacy Committee. The individual will also be informed of the procedure for appeal when the center or originating agency has cited an exemption for the type of information requested or has declined to correct challenged information to the satisfaction of the individual to whom the information relates.

### **K.4 COMPLAINTS**

1. If an individual has a complaint with regard to the accuracy or completeness of criminal or terrorism-related protected information that (a) is exempt from disclosure, (b) has been or may be shared through the ISE, or (c) is held by the BRIC and allegedly has resulted in

**UNCLASSIFIED**

demonstrable harm to the complainant, the center will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the center's privacy officer, on behalf of the Privacy Committee, at the following address:

Boston Regional Intelligence Center  
Boston Police Department  
Privacy Committee  
One Schroeder Plaza  
Boston, MA 02120

The privacy officer, on behalf of the Privacy Committee, will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. If the information did not originate with the center, the privacy officer, on behalf of the Privacy Committee, will notify the originating agency in writing or electronically within ten (10) business days of the receipt of the complaint and, upon request, may assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All information held by the center that is the subject of a complaint will be reviewed within thirty (30) days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within thirty (30) days, the center will not share the information until such time as the complaint has been resolved. A record will be kept by the center of all complaints and the resulting action taken in response to the complaint.

#### **L. SECURITY SAFEGUARDS**

1. The bureau chief of the Boston Police Department's Bureau of Intelligence and Analysis and/or the director of the BRIC will ensure that a secure environment exists within the BRIC's facility.
2. The BRIC will operate in a secure facility protected from external intrusion. The center will utilize secure internal and external safeguards against network intrusions. Access to the center's databases from outside the facility will be allowed only over secure networks.
3. The BRIC will secure tips, leads, and SAR information in a separate repository system using security procedures and policies that are the same as or similar to those used for a system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.
4. The BRIC will store information in a manner that ensures it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.
5. Access to BRIC information will be granted only to center personnel whose positions and job duties require such access; who have successfully completed a background check and appropriate security clearance, if applicable; and who have been selected, approved, and trained accordingly.
6. Queries made to the BRIC's data applications will be logged into the data system, as appropriate, to identify the user initiating the query.
7. The BRIC will utilize appropriate mechanisms to maintain audit trails of requested and disseminated information.
8. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.
9. The BRIC will notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to

which threatens physical, reputational, or financial harm to the person. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release.

10. The BRIC will immediately notify the originating agency from which the center received personal information of a suspected or confirmed breach of such information.

#### **M. INFORMATION RETENTION AND DESTRUCTION**

1. All applicable information will be reviewed for record retention (validation or purge) by the BRIC at least every five (5) years, as provided by 28 CFR Part 23. The BRIC conducts quarterly reviews and ongoing maintenance to validate or purge information.
2. When information has no further value or meets the criteria for removal according to the BRIC's retention and destruction policy or according to applicable law, it will be purged, destroyed, and deleted or returned to the submitting (originating) agency.
3. The BRIC will delete information or return it to the originating agency once its retention period has expired as provided by this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.
4. No approval will be required from the originating agency before information held by the BRIC is destroyed or returned in accordance with this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.
5. Notification of proposed destruction or return of records may or may not be provided to the originating agency by the BRIC, depending on the relevance of the information and any agreement with the originating agency.
6. The BRIC keeps a record of dates when law enforcement and homeland security information is to be removed (purged) if not validated prior to the end of its period. An auto-generated notification is given prior to removal to prompt center personnel that a record is due for review and validation or purge.

#### **N. ACCOUNTABILITY AND ENFORCEMENT**

##### **N.1 INFORMATION SYSTEM TRANSPARENCY**

1. The BRIC will be open with the public in regard to information and intelligence collection practices. The center's privacy policy will be provided to the public for review, made available upon request, and posted to <http://www.bpdnews.com> and the National Fusion Center Association Web site (<http://new.nfcausa.org/>).
2. The BRIC's privacy officer, on behalf of the Privacy Committee, will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the center. The Privacy Committee can be contacted at:

Boston Regional Intelligence Center  
Boston Police Department  
Privacy Committee  
One Schroeder Plaza  
Boston, MA 02120

## **N.2 ACCOUNTABILITY**

1. The audit log of queries made to the BRIC will identify the user initiating the query.
2. The BRIC will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for not more than five (5) years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.
3. The BRIC follows agency-based user agreements for access to computer networks and systems. The BRIC will provide annual center-based personnel training to reinforce applicable laws and policies. The BRIC will adopt and implement procedures to evaluate the compliance of users with this policy and with applicable law, to include a review of logging access to BRIC information systems and periodic auditing of user compliance. These audits will be conducted at least annually, and a record of the audits will be maintained by the privacy officer on behalf of the Privacy Committee.
4. The BRIC's personnel or other authorized users shall report errors and suspected or confirmed violations of center policies relating to protected information to the center's Privacy Committee. See Section C.3.
5. The BRIC will annually conduct an audit and inspection of the information and intelligence contained in its information system(s). The audit will be conducted by the center's Privacy Committee. This committee has the option of conducting a random audit, without announcement, at any time and without prior notice to staff of the center. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the center's information and intelligence system(s).
6. The BRIC's Privacy Committee will review the provisions protecting privacy, civil rights, and civil liberties contained in this policy annually and recommend updates, as needed, to the BRIC director in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations.

## **N.3 ENFORCEMENT**

1. If center personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of information, the bureau chief of the Boston Police Department's Bureau of Intelligence and Analysis and/or the director of the BRIC may:
  - Suspend or discontinue access to information by the center personnel, the participating agency, or the authorized user.
  - Apply administrative and/or legal actions or sanctions as consistent with department rules and regulations or applicable law or as provided in agency/center personnel policies.
  - If the authorized user is from an agency external to the agency/center, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions.
2. The BRIC reserves the right to restrict the qualifications and number of personnel having access to center information and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating the center's privacy policy.

## O. TRAINING

1. All BRIC personnel will be trained regarding implementation of and adherence to the privacy, civil rights, and civil liberties policy prior to granting access.
2. The BRIC will provide special training regarding the center's requirements and policies for collection, use, and disclosure of protected information to personnel authorized to share protected information through the Information Sharing Environment.
3. The BRIC's privacy policy training program will cover:
  - Purposes of the privacy, civil rights, and civil liberties protection policy.
  - Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the center.
  - How to implement the policy in the day-to-day work of the user, whether a paper or systems user.
  - The impact of improper activities associated with infractions within or through the agency.
  - Mechanisms for reporting violations of center privacy protection policies and procedures.
  - The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.



## APPENDIX A: TERMS AND DEFINITIONS

The following is a list of primary terms and definitions used throughout this policy.

**Access**—Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only and read/write access.

With regard to the ISE, access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

**Access Control**—The mechanisms for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role-based.

**Acquisition**—The means by which an ISE participant obtains information through the exercise of its authorities, for example, through human intelligence collection or from a foreign partner. For the purposes of this definition, acquisition does not refer either to the obtaining of information widely available to other ISE participants through, for example, news reports, or to the obtaining of information shared with them by another ISE participant who originally acquired the information.

**Agency**—The Boston Regional Intelligence Center (BRIC) and all agencies that access, contribute, and share information in the BRIC's justice information systems.

**Audit Trail**—A generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc.

Audit trails are a fundamental part of computer security, used to trace (usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

**Authentication**—The process of validating the credentials of a person, a computer process, or a device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords. See Biometrics.

**Authorization**—The process of granting a person, a computer process, or a device access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access that is verified through authentication. See Authentication.

**Biometrics**—Biometrics methods can be divided into two categories: physiological and behavioral. Implementations of the former include face, eye (retina or iris), finger (fingertip, thumb, finger length or pattern), palm (print or topography), and hand geometry. The latter includes voiceprints and handwritten signatures.

**Center**—Refers to the Boston Regional Intelligence Center (BRIC) and all participating agencies.

**Civil Liberties**—Fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights, the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference. Generally, the term “civil rights” involves positive (or affirmative) government action, while the term “civil liberties” involves restrictions on government.

**Civil Rights**—Refers to the government’s role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed on government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.

**Computer Security**—The protection of information assets through the use of technology, processes, and training.

**Confidentiality**—The obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for and to protect and preserve the privacy of others. See Privacy.

**Credentials**—Information that includes identification and proof of identification that is used to gain access to local and network resources. Examples of credentials are user names, passwords, smart cards, and certificates.

**Criminal Intelligence Information**—Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal activity. Criminal intelligence records are maintained in a criminal intelligence system per 28 CFR Part 23.

**Data**—Elements of information.

**Data Breach**—The unintentional release of secure information to an untrusted environment. This may include incidents such as theft or loss of digital media such as computer tapes, hard drives, or laptop computers containing such media upon which such information is stored unencrypted; posting such information on the World Wide Web or on a computer otherwise accessible from the Internet without proper information security precautions; transfer of such information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail; or transfer of such information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques.

**Data Protection**—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure of information.

**Disclosure**—The release, transfer, provision of access to, sharing, publication, or divulging of personal information in any manner—electronic, verbal, or in writing—to an individual, an agency, or an organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

**Electronically Maintained**—Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disc optical media.

**Electronically Transmitted**—Information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media or transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, or faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voicemail.

**Fair Information Principles**—The Fair Information Principles (FIPs) are contained within the Organisation for Economic Co-operation and Development's (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. These were developed around commercial transactions and the transborder exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles and a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system.

The eight FIPs are:

1. Collection Limitation Principle
2. Data Quality Principle
3. Purpose Specification Principle
4. Use Limitation Principle
5. Security Safeguards Principle
6. Openness Principle
7. Individual Participation Principle
8. Accountability Principle

**Firewall**—A security solution that segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic-filtering rules.

**General Information or Data**—Information that may include records, documents, or files pertaining to law enforcement operations, such as computer-aided dispatch (CAD) data, incident data, and management information. Information that is maintained in a records management system, CAD system, etc., for statistical/retrieval purposes. Information may be either resolved or unresolved. The record is maintained per statute, rule, or policy.

**Homeland Security Information**—As defined in Section 892(f)(1) of the Homeland Security Act of 2002 and codified at 6 U.S.C. § 482(f)(1), homeland security information means any information possessed by a federal, state, or local agency that (a) relates to a threat of terrorist activity; (b) relates to the ability to prevent, interdict, or disrupt terrorist activity; (c) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (d) would improve the response to a terrorist act.

**Identification**—A process whereby a real-world entity is recognized and its identity established. Identity is operationalized in the abstract world of information systems as a set of information about an entity that uniquely differentiates it from other similar entities. The set of information may be as small as a single code, specifically designed as an identifier, or a collection of data, such as a given and family name, date of birth, and address. An organization's identification process consists of the acquisition of the relevant identifying information.

**Individual Responsibility**—Because a privacy notice is not self-implementing, an individual within an organization's structure must also be assigned responsibility for enacting and implementing the notice.

**Information**—Includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into four general areas: general data, tips and leads data, suspicious activity reports, and criminal intelligence information.

**Information Quality**—Refers to various aspects of the information; the accuracy and validity of the actual values of the data, data structure, and database/data repository design. Traditionally, the basic elements of information quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, information quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy.

**Information Sharing Environment (ISE) Suspicious Activity Report (SAR) (ISE-SAR)**—A SAR that has been determined, pursuant to a two-step process established in the ISE-SAR Functional Standard, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism).

**Intelligence-Led Policing (ILP)**—A process for enhancing law enforcement agency effectiveness toward reducing crimes, protecting community assets, and preparing for responses. ILP provides law enforcement agencies with an organizational framework to gather and use multisource information and intelligence to make timely and targeted strategic, operational, and tactical decisions.

**Invasion of Privacy**—Intrusion on one's solitude or into one's private affairs, public disclosure of embarrassing private information, publicity that puts one in a false light to the public, or appropriation of one's name or picture for personal or commercial advantage. See also Right to Privacy.

**ISE-SAR**—A suspicious activity report (SAR) that has been determined, pursuant to a two-part process, to have a potential terrorism nexus. ISE-SAR business rules will serve as a unifying process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.

**ISE-SAR Information Exchange Package Documentation (IEPD)**—A schema that facilitates the posting and sharing of ISE-SAR information. The ISE-SAR IEPD is used to represent ISE information in two different data formats:

1. The **detailed format** includes information contained in all data elements set forth in Section IV of the ISE-SAR FS ("ISE-SAR Exchange Data Model"), including fields denoted as privacy fields.
2. The **summary format** excludes certain privacy fields as identified in the ISE-SAR FS. The ISE-SAR FS identifies the minimum privacy fields that must be excluded. Each ISE participant may exclude additional privacy fields from its Summary ISE-SARs, in accordance with applicable legal requirements.

**Label**—Marking(s) applied to disseminated information and products with indications to the accessing authorized user that the information is protected information, including organizational entities, and the information is subject to Massachusetts General Law and Federal Regulations restricting access, use, or disclosure.

**Law**—As used by this policy, law includes any local, state, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

**Law Enforcement Information**—For purposes of the ISE, law enforcement information means any information obtained by or of interest to a law enforcement agency or official that is both (a)

related to terrorism or the security of our homeland and (b) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

**Lawful Permanent Resident**—A foreign national who has been granted the privilege of permanently living and working in the United States.

**Least Privilege Administration**—A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks he or she is authorized to perform.

**Logs**—Logs are a necessary part of an adequate security system because they are needed to ensure that data is properly tracked and that only authorized individuals are getting access to the system and the data. See Audit Trail.

**Maintenance of Information**—Applies to all forms of information storage. This includes electronic systems (for example, databases) and nonelectronic storage systems (for example, filing cabinets). To meet access requirements, an organization is not required to create new systems to maintain information or to maintain information beyond a time when it no longer serves an organization's purpose.

**Metadata**—In its simplest form, metadata is information (data) about information—more specifically, information about a particular aspect of the collected information. An item of metadata may describe an individual content item or a collection of content items. Metadata is used to facilitate the understanding, use, and management of information. The metadata required for this will vary based on the type of information and the context of use.

**Need to Know**—As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information in the performance of a law enforcement, homeland security, or counterterrorism activity, such as to further an investigation or meet another law enforcement requirement.

**Nonrepudiation**—A technique used to ensure that someone performing an action on a computer cannot falsely deny that he or she performed that action. Nonrepudiation provides undeniable proof that a user took a specific action, such as transferring money, authorizing a purchase, or sending a message.

**Originating Agency**—The agency or organizational entity that documents information or data, including source agencies that document SAR (and, when authorized, ISE-SAR) information that is collected by a fusion center.

**Participating Agencies**—Participating agencies include source (the agency or entity that originates SAR [and, when authorized, ISE-SAR] information), submitting (which is the agency or entity posting ISE-SAR information to the SAR Data Repository), and user (which is an agency or entity authorized by the submitting agency or other authorized agency or entity to access ISE-SAR information, including information in the SAR Data Repository, and which may include analytical or operational component(s) of the submitting or authorizing agency or entity)

agencies, in support of their responsibility to collect, document, process, access, or use SAR and ISE-SAR information.

**Personal Information**—Information that can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in an activity or incident potentially related to terrorism.

**Personally Identifiable Information**—One or more pieces of information that, when considered together or in the context of how the information is presented or gathered, are sufficient to specify a unique individual. The pieces of information can be:

- Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).
- A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Automated Integrated Fingerprint Identification System [AIFIS] identifier, or booking or detention system number).
- Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).
- Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

**Persons**—Executive Order 12333 defines "United States persons" as United States citizens, aliens known by the intelligence agency concerned to be permanent resident aliens, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. For the intelligence community and for domestic law enforcement agencies, "persons" means United States citizens and lawful permanent residents.

**Preoperational Planning**—Describes activities associated with a known or particular planned criminal operation or with terrorist operations generally.

**Privacy**—Individuals' interests in preventing the inappropriate collection, use, and release of personal information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the right to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

**Privacy Fields**—Data fields in ISE-SAR IEPDs that contain personal information.

**Privacy Policy**—A written, published statement that articulates the policy position of an organization on how it handles the personal information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, disclosure, and access. The purpose of the privacy policy is to articulate that the center will adhere to those legal requirements and center policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

**Privacy Protection**—A process of maximizing the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health.

**Protected Information**—Personal information about any individual that is subject to information privacy or other protections by law, including the U.S. Constitution, the Massachusetts Constitution, and other applicable law.

**Public**—Public includes:

- Any person and any for-profit or nonprofit entity, organization, or association.
- Any governmental entity for which there is no existing specific law authorizing access to the agency's/center's information.
- Media organizations.
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit and without distinction as to the nature or intent of those requesting information from the agency.

Public does not include:

- Employees of the agency.
- People or entities, private or governmental, who assist the agency/center in the operation of the justice information system.
- Public agencies whose authority to access information gathered and retained by the agency/center is specified in law.

**Public Access**—Relates to what information can be seen by the public; that is, information whose availability is not subject to privacy interests or rights.

**Reasonably Indicative**—This operational concept for documenting and sharing suspicious activity reports takes into account the circumstances in which the observation is made, which creates in the mind of the reasonable observer, including a law enforcement officer, an articulable concern that the behavior may indicate preoperational planning associated with terrorism or other criminal activity. It also takes into account the training and experience of a reasonable law enforcement officer, in cases in which an officer is the observer or documenter of the observed behavior reported to a law enforcement agency.

**Record**—Any item, collection, or grouping of information that includes personally identifiable information and is maintained, collected, used, or disseminated by or for the collecting agency or organization.

**Redress**—Laws, policies, and procedures that address public agency responsibilities with regard to access/disclosure and correction of information and the handling of complaints from persons regarding protected information about them which is under the agency's/center's control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.

**Repudiation**—The ability of a user to deny having performed an action that other parties cannot prove otherwise. For example, a user who deleted a file can successfully deny doing so if no mechanism (such as audit files) can contradict that claim.

**Retention**—See Storage.

**Right to Know**—Based on having legal authority or responsibility or pursuant to an authorized agreement, an agency or organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, or counterterrorism activity.

**Right to Privacy**—The right to be left alone, in the absence of some reasonable public interest in gathering, retaining, and sharing information about a person's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating a person's privacy.

**Role-Based Access**—A type of access that uses roles to determine rights and privileges. A role is a symbolic category of users that share the same security privilege.

**Security**—The range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

**Sharing**—The act of one ISE participant disseminating or giving homeland security information, terrorism information, or law enforcement information to another ISE participant.

**Source Agency**—The agency or entity that originates SAR (and, when authorized, ISE-SAR) information.

**Storage**—In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor. There are two general usages:

1. Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This meaning is probably more common in the IT industry than meaning 2.
2. In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory or RAM) and other “built-in” devices, such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism-related information, to include homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland by both the originator of the information and any recipient of the information.

**Submitting Agency**—The agency or entity providing ISE-SAR information to the SAR Data Repository.

**Suspicious Activity**—Observed behavior reasonably indicative of preoperational planning associated with terrorism or other criminal activity. Examples of suspicious activity include surveillance, photography of facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

**Suspicious Activity Reports (SARs)**—Official documentation of observed behavior reasonably indicative of preoperational planning associated with terrorism or other criminal



activity. SAR information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

**Terrorism Information**—Consistent with Section 1016(a)(4) of IRTPA, all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign or international terrorist groups or individuals or of domestic groups or individuals involved in transnational terrorism, (b) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations, (c) communications of or by such groups or individuals, or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

**Terrorism-Related Information**—In accordance with IRTPA, as recently amended by the 9/11 Commission Act enacted on August 3, 2007 (P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also *Information Sharing Environment Implementation Plan* (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of “terrorism information,” as defined in IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute “terrorism information”: (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information includes intelligence information.

Weapons of Mass Destruction (WMD) information was defined and included in the definition of “terrorism information” by P.L. 110-53.

**Tips and Leads Information or Data**—Generally uncorroborated reports or information generated from inside or outside a law enforcement agency that allege or indicate some form of possible criminal activity. Tips and leads are sometimes referred to as suspicious incident report (SIR), suspicious activity report (SAR), and/or field interview report (FIR) information. However, SAR information should be viewed, at most, as a subcategory of tip or lead data. Tips and leads information does not include incidents that do not have a criminal offense attached or indicated, criminal history records, or CAD data. Tips and leads information should be maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information may be based on mere suspicion or on a level of suspicion that is less than “reasonable suspicion” and, without further information or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of little or no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.

**Urban Area Fusion Center**—A collaborative effort of two or more agencies that provide resources, expertise, and information to a designated government agency or agency component with the goal of maximizing its ability to detect, prevent, investigate, and respond to criminal and terrorist activity.

**User**—An individual representing a participating agency who is authorized to access or receive and use a center’s information and intelligence databases and resources for lawful purposes.

UNCLASSIFIED

**User Agency**—The agency or entity authorized by the submitting agency or other authorized agency or entity to access ISE-SAR information in the SAR Data Repository, which may include analytical or operational component(s) of the submitting or authorizing agency or entity.

UNCLASSIFIED

## APPENDIX B: APPLICABLE LEGAL REFERENCES

**Effective: October 31, 2007**

Massachusetts General Laws Annotated Currentness

Part I. Administration of the Government (Ch. 1–182)

Title X. Public Records (Ch. 66-66A)

Chapter 66A. Fair Information Practices (Refs & Annos)

§ 2. Holders maintaining personal data system; duties

Every holder maintaining personal data shall:–

(a) identify one individual immediately responsible for the personal data system who shall insure that the requirements of this chapter for preventing access to or dissemination of personal data are followed;

(b) inform each of its employees having any responsibility or function in the design, development, operation, or maintenance of the personal data system, or the use of any personal data contained therein, of each safeguard required by this chapter, of each rule and regulation promulgated pursuant to section three which pertains to the operation of the personal data system, and of the civil remedies described in section three B of chapter two hundred and fourteen available to individuals whose rights under chapter sixty-six A are allegedly violated;

(c) not allow any other agency or individual not employed by the holder to have access to personal data unless such access is authorized by statute or regulations which are consistent with the purposes of this chapter or is approved by the data subject whose personal data are sought if the data subject is entitled to access under clause

(i). Medical or psychiatric data may be made available to a physician treating a data subject upon the request of said physician, if a medical or psychiatric emergency arises which precludes the data subject's giving approval for the release of such data, but the data subject shall be given notice of such access upon termination of the emergency. A holder shall provide lists of names and addresses of applicants for professional licenses and lists of professional licensees to associations or educational organizations recognized by the appropriate professional licensing or examination board. A holder shall comply with a data subject's request to disseminate his data to a third person if practicable and upon payment, if necessary, of a reasonable fee; provided, however, that nothing in this section shall be construed to prohibit disclosure to or access by the bureau of special investigations to the records or files of the department of transitional assistance for the purposes of fraud detection and control;

(d) take reasonable precautions to protect personal data from dangers of fire, identity theft, theft, flood, natural disaster, or other physical threat;

(e) comply with the notice requirements set forth in section sixty-three of chapter thirty;

(f) in the case of data held in automated personal data systems, and to the extent feasible with data held in manual personal data systems, maintain a complete and accurate record of every access to and every use of any personal data by persons or organizations outside of or other than the holder of the data, including the identity of all such persons and organizations which have gained access to the personal data and their intended use of such data and the holder need not record any such access of its employees acting within their official duties;

(g) to the extent that such material is maintained pursuant to this section, make available to a data subject upon his request in a form comprehensible to him, a list of the uses made of his

personal data, including the identity of all persons and organizations which have gained access to the data;

(h) maintain personal data with such accuracy, completeness, timeliness, pertinence and relevance as is necessary to assure fair determination of a data subject's qualifications, character, rights, opportunities, or benefits when such determinations are based upon such data;

(i) inform in writing an individual, upon his request, whether he is a data subject, and if so, make such data fully available to him or his authorized representative, upon his request, in a form comprehensible to him, unless doing so is prohibited by this clause or any other statute. A holder may withhold from a data subject for the period hereinafter set forth, information which is currently the subject of an investigation and the disclosure of which would probably so prejudice the possibility of effective law enforcement that such disclosure would not be in the public interest, but this sentence is not intended in any way to derogate from any right or power of access the data subject might have under administrative or judicial discovery procedures. Such information may be withheld for the time it takes for the holder to complete its investigation and commence an administrative or judicial proceeding on its basis, or one year from the commencement of the investigation or whichever occurs first. In making any disclosure of information to a data subject pursuant to this chapter the holder may remove personal identifiers relating to a third person, except where such third person is an officer or employee of government acting as such and the data subject is not. No holder shall rely on any exception contained in clause Twentysixth of section seven of chapter four to withhold from any data subject personal data otherwise accessible to him under this chapter;

(j) establish procedures that (1) allow each data subject or his duly authorized representative to contest the accuracy, completeness, pertinence, timeliness, relevance or dissemination of his personal data or the denial of access to such data maintained in the personal data system and (2) permit personal data to be corrected or amended when the data subject or his duly authorized representative so requests and there is no disagreement concerning the change to be made or, when there is disagreement with the data subject as to whether a change should be made, assure that the data subject's claim is noted and included as part of the data subject's personal data and included in any subsequent disclosure or dissemination of the disputed data;

(k) maintain procedures to ensure that no personal data are made available in response to a demand for data made by means of compulsory legal process, unless the data subject has been notified of such demand in reasonable time that he may seek to have the process quashed;

(l) not collect or maintain more personal data than are reasonably necessary for the performance of the holder's statutory functions.

M.G.L.A. 66A § 2 Page 2

© 2009 Thomson Reuters/West. No Claim to Orig. US Gov. Works.

CREDIT(S)

Added by St.1975, c. 776, § 1. Amended by St.1976, c. 249, § 2; St.1977, c. 691, §§ 7 to 12; St.1995, c. 5, § 34;

St.2007, c. 82, § 2, eff. Oct. 31, 2007.

Current through Chapter 10 of the 2009 1st Annual Sess.

---

**Effective: December 13, 2003**

United States Code Annotated Currentness

Title 6. Domestic Security (Refs & Annos)

Chapter 1. Homeland Security Organization

Subchapter VIII. Coordination with Non-Federal Entities; Inspector General; United States Secret Service;

Coast Guard; General Provisions

Part I. Information Sharing

§ 482. Facilitating homeland security information sharing procedures

(a) Procedures for determining extent of sharing of homeland security information

(1) The President shall prescribe and implement procedures under which relevant Federal agencies—

(A) share relevant and appropriate homeland security information with other Federal agencies, including the Department, and appropriate State and local personnel;

(B) identify and safeguard homeland security information that is sensitive but unclassified; and

(C) to the extent such information is in classified form, determine whether, how, and to what extent to remove classified information, as appropriate, and with which such personnel it may be shared after such information is removed.

(2) The President shall ensure that such procedures apply to all agencies of the Federal Government.

(3) Such procedures shall not change the substantive requirements for the classification and safeguarding of classified information.

(4) Such procedures shall not change the requirements and authorities to protect sources and methods.

(b) Procedures for sharing of homeland security information

(1) Under procedures prescribed by the President, all appropriate agencies, including the intelligence community, shall, through information sharing systems, share homeland security information with Federal agencies and appropriate State and local personnel to the extent such information may be shared, as determined in accordance with subsection (a) of this section, together with assessments of the credibility of such information.

(2) Each information sharing system through which information is shared under paragraph (1) shall—

(A) have the capability to transmit unclassified or classified information, though the procedures and recipients for each capability may differ;

(B) have the capability to restrict delivery of information to specified subgroups by geographic location, type of organization, position of a recipient within an organization, or a recipient's need to know such information;

(C) be configured to allow the efficient and effective sharing of information; and

(D) be accessible to appropriate State and local personnel.

**UNCLASSIFIED**

(3) The procedures prescribed under paragraph (1) shall establish conditions on the use of information shared under paragraph (1)—

(A) to limit the redissemination of such information to ensure that such information is not used for an unauthorized purpose;

(B) to ensure the security and confidentiality of such information;

(C) to protect the constitutional and statutory rights of any individuals who are subjects of such information; and

(D) to provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.

(4) The procedures prescribed under paragraph (1) shall ensure, to the greatest extent practicable, that the information sharing system through which information is shared under such paragraph include existing information sharing systems, including, but not limited to, the National Law Enforcement Telecommunications System, the Regional Information Sharing System, and the Terrorist Threat Warning System of the Federal Bureau of Investigation.

(5) Each appropriate Federal agency, as determined by the President, shall have access to each information sharing system through which information is shared under paragraph (1), and shall therefore have access to all information, as appropriate, shared under such paragraph.

(6) The procedures prescribed under paragraph (1) shall ensure that appropriate State and local personnel are authorized to use such information sharing systems—

(A) to access information shared with such personnel; and

(B) to share, with others who have access to such information sharing systems, the homeland security information of their own jurisdictions, which shall be marked appropriately as pertaining to potential terrorist activity.

(7) Under procedures prescribed jointly by the Director of Central Intelligence and the Attorney General, each appropriate Federal agency, as determined by the President, shall review and assess the information shared under paragraph (6) and integrate such information with existing intelligence.

(c) Sharing of classified information and sensitive but unclassified information with State and local personnel

(1) The President shall prescribe procedures under which Federal agencies may, to the extent the President considers necessary, share with appropriate State and local personnel homeland security information that remains classified or otherwise protected after the determinations prescribed under the procedures set forth in subsection (a) of this section.

(2) It is the sense of Congress that such procedures may include 1 or more of the following means:

(A) Carrying out security clearance investigations with respect to appropriate State and local personnel.

(B) With respect to information that is sensitive but unclassified, entering into nondisclosure agreements with appropriate State and local personnel.

(C) Increased use of information-sharing partnerships that include appropriate State and local personnel, such as the Joint Terrorism Task Forces of the Federal Bureau of Investigation, the Anti-Terrorism Task Forces of the Department of Justice, and regional Terrorism Early Warning Groups.

(3)(A) The Secretary shall establish a program to provide appropriate training to officials described in subparagraph

(B) in order to assist such officials in--

(i) identifying sources of potential terrorist threats through such methods as the Secretary determines appropriate;

(ii) reporting information relating to such potential terrorist threats to the appropriate Federal agencies in the appropriate form and manner;

(iii) assuring that all reported information is systematically submitted to and passed on by the Department for use by appropriate Federal agencies; and

(iv) understanding the mission and roles of the intelligence community to promote more effective information sharing among Federal, State, and local officials and representatives of the private sector to prevent terrorist attacks against the United States.

(B) The officials referred to in subparagraph (A) are officials of State and local government agencies and representatives of private sector entities with responsibilities relating to the oversight and management of first responders, counterterrorism activities, or critical infrastructure.

(C) The Secretary shall consult with the Attorney General to ensure that the training program established in subparagraph (A) does not duplicate the training program established in section 908 of the USA PATRIOT Act (Public Law 107-56; 28 U.S.C. 509 note).

(D) The Secretary shall carry out this paragraph in consultation with the Director of Central Intelligence and the Attorney General.

(d) Responsible officials

For each affected Federal agency, the head of such agency shall designate an official to administer this chapter with respect to such agency.

(e) Federal control of information

Under procedures prescribed under this section, information obtained by a State or local government from a Federal agency under this section shall remain under the control of the Federal agency, and a State or local law authorizing or requiring such a government to disclose information shall not apply to such information.

(f) Definitions

As used in this section:

(1) The term "homeland security information" means any information possessed by a Federal, State, or local agency that—

(A) relates to the threat of terrorist activity;

(B) relates to the ability to prevent, interdict, or disrupt terrorist activity;

(C) would improve the identification or investigation of a suspected terrorist or terrorist organization; or

(D) would improve the response to a terrorist act.

(2) The term "intelligence community" has the meaning given such term in section 401a(4) of Title 50.

(3) The term “State and local personnel” means any of the following persons involved in prevention, preparation, or response for terrorist attack:

(A) State Governors, mayors, and other locally elected officials.

(B) State and local law enforcement personnel and firefighters.

(C) Public health and medical professionals.

(D) Regional, State, and local emergency management agency personnel, including State adjutant generals.

(E) Other appropriate emergency response agency personnel.

(F) Employees of private-sector entities that affect critical infrastructure, cyber, economic, or public health security, as designated by the Federal Government in procedures developed pursuant to this section.

(4) The term “State” includes the District of Columbia and any commonwealth, territory, or possession of the United States.

(g) Construction

Nothing in this chapter shall be construed as authorizing any department, bureau, agency, officer, or employee of the Federal Government to request, receive, or transmit to any other Government entity or personnel, or transmit to any State or local entity or personnel otherwise authorized by this chapter to receive homeland security information, any information collected by the Federal Government solely for statistical purposes in violation of any other provision of law relating to the confidentiality of such information.

CREDIT(S)

6 U.S.C.A. § 482 Page 4

© 2009 Thomson Reuters/West. No Claim to Orig. US Gov. Works.

(Pub.L. 107–296, Title VIII, § 892, Nov. 25, 2002, 116 Stat. 2253; Pub.L. 108–177, Title III, § 316(a), Dec. 13, 2003, 117 Stat. 2610.)

2002 Acts. This section effective 60 days after Nov. 25, 2002, see Pub.L. 107–296, § 4, set out as a note under 6 U.S.C.A. § 101.

Current through P.L. 111–15 (excluding P.L. 111–11 and 111–13) approved 4-24-09

Westlaw. (C) 2009 Thomson Reuters. No Claim to Orig. U.S. Govt. Works.

END OF DOCUMENT

6 U.S.C.A. § 482 Page 5

---

**Effective: March 30, 2009**

Massachusetts General Laws Annotated Currentness

Part I. Administration of the Government (Ch. 1–182)

Title I. Jurisdiction and Emblems of the Commonwealth, the General Court, Statutes and Public Documents



(Ch. 1–5)

Chapter 4. Statutes (Refs & Annos)

§ 7. Definitions of statutory terms; statutory construction

In construing statutes the following words shall have the meanings herein given, unless a contrary intention clearly appears:

First, “Aldermen”, “board of aldermen”, “mayor and aldermen”, “city council” or “mayor” shall, in a city which has no such body or officer, mean the board or officer having like powers or duties.

Second, “Annual meeting”, when applied to towns, shall mean the annual meeting required by law to be held in the month of February, March or April.

Second A, “Appointing authority”, when used in connection with the operation of municipal governments shall include the mayor of a city and the board of selectmen of a town unless some other local office is designated as the appointing authority under the provisions of a local charter.

Third, “Assessor” shall include any person chosen or appointed in accordance with law to perform the duties of an assessor.

Third A, “Board of selectmen”, when used in connection with the operation of municipal governments shall include any other local office which is performing the duties of a board of selectmen, in whole or in part, under the provisions of a local charter.

<[There is no clause Fourth.]>

Fifth, “Charter”, when used in connection with the operation of city and town government shall include a written instrument adopted, amended or revised pursuant to the provisions of chapter forty-three B which establishes and defines the structure of city and town government for a particular community and which may create local offices, and distribute powers, duties and responsibilities among local offices and which may establish and define certain procedures to be followed by the city or town government. Special laws enacted by the general court applicable only to one city or town shall be deemed to have the force of a charter and may be amended, repealed and revised in accordance with the provisions of chapter forty-three B unless any such special law contains a specific prohibition against such action.

Fifth A, “Chief administrative officer”, when used in connection with the operation of municipal governments, shall include the mayor of a city and the board of selectmen in a town unless some other local office is designated to be the chief administrative officer under the provisions of a local charter.

Fifth B, “Chief executive officer”, when used in connection with the operation of municipal governments shall include the mayor in a city and the board of selectmen in a town unless some other municipal office is designated to be the chief executive officer under the provisions of a local charter.

Sixth, “City solicitor” shall include the head of the legal department of a city or town.

Sixth A, “Coterminous”, shall mean, when applied to the term of office of a person appointed by the governor, the period from the date of appointment and qualification to the end of the term of said governor; provided that such person shall serve until his successor is appointed and qualified; and provided, further, that the governor may remove such person at any time, subject however to the condition that if such person receives notice of the termination of his appointment he shall have the right, at his request, to a hearing within thirty days from receipt of such notice at which hearing the governor shall show cause for such removal, and that during

**UNCLASSIFIED**

the period following receipt of such notice and until final determination said person shall receive his usual compensation but shall be deemed suspended from his office.

Seventh, "District", when applied to courts or the justices or other officials thereof, shall include municipal.

Eighth, "Dukes", "Dukes county" or "county of Dukes" shall mean the county of Dukes county.

Ninth, "Fiscal year", when used with reference to any of the offices, departments, boards, commissions, institutions or undertakings of the commonwealth, shall mean the year beginning with July first and ending with the following June thirtieth.

Tenth, "Gaming", "illegal gaming" or "unlawful gaming" shall include every act punishable under any law relative to lotteries, policy lotteries or policy, the buying and selling of pools or registering of bets.

Eleventh, "Grantor" may include every person from or by whom a freehold estate or interest passes in or by any deed; and "grantee" may include every person to whom such estate or interest so passes.

Twelfth, "Highway", "townway", "public way" or "way" shall include a bridge which is a part thereof.

Thirteenth, "In books", when used relative to the records of cities and towns, shall not prohibit the making of such records on separate leaves, if such leaves are bound in a permanent book upon the completion of a sufficient number of them to make an ordinary volume.

Fourteenth, "Inhabitant" may mean a resident in any city or town.

<[There is no clause Fifteenth.]>

Sixteenth, "Issue", as applied to the descent of estates, shall include all the lawful lineal descendants of the ancestor.

Seventeenth, "Land", "lands" and "real estate" shall include lands, tenements and hereditaments, and all rights thereto and interests therein; and "recorded", as applied to plans, deeds or other instruments affecting land, shall, as affecting registered land, mean filed and registered.

Eighteenth, "Legal holiday" shall include January first, July fourth, November eleventh, and Christmas Day, or the day following when any of said days occurs on Sunday, and the third Monday in January, the third Monday in February, the third Monday in April, the last Monday in May, the first Monday in September, the second Monday in October, and Thanksgiving Day. "Legal holiday" shall also include, with respect to Suffolk county only, March seventeenth and June seventeenth, or the day following when said days occur on Sunday; provided, however, that the words "legal holiday" as used in section forty-five of chapter one hundred and forty-nine shall not include March seventeenth, or the day following when said day occurs on Sunday.

Eighteenth A, "Commemoration day" shall include March fifteenth, in honor of Peter Francisco day, May twentieth, in honor of General Marquis de Lafayette and May twenty-ninth, in honor of the birthday of President John F. Kennedy. The governor shall issue a proclamation in connection with each such commemoration day.

Eighteenth B, "Legislative body", when used in connection with the operation of municipal governments shall include that agency of the municipal government which is empowered to enact ordinances or by-laws, adopt an annual budget and other spending authorizations, loan orders, bond authorizations and other financial matters and whether styled a city council, board of aldermen, town council, town meeting or by any other title.

**UNCLASSIFIED**

Nineteenth, "Month" shall mean a calendar month, except that, when used in a statute providing for punishment by imprisonment, one "month" or a multiple thereof shall mean a period of thirty days or the corresponding multiple thereof; and "year", a calendar year.

Nineteenth A, "Municipality" shall mean a city or town.

Twentieth, "Net indebtedness" shall mean the indebtedness of a county, city, town or district, omitting debts created for supplying the inhabitants with water and other debts exempted from the operation of the law limiting their indebtedness, and deducting the amount of sinking funds available for the payment of the indebtedness included.

Twenty-first, "Oath" shall include affirmation in cases where by law an affirmation may be substituted for an oath.

Twenty-second, "Ordinance", as applied to cities, shall be synonymous with by-law.

Twenty-third, "Person" or "whoever" shall include corporations, societies, associations and partnerships. Twenty-fourth, "Place" may mean a city or town.

Twenty-fifth, "Preceding" or "following", used with reference to any section of the statutes, shall mean the section last preceding or next following, unless some other section is expressly designated in such reference.

Twenty-sixth, "Public records" shall mean all books, papers, maps, photographs, recorded tapes, financial statements, statistical tabulations, or other documentary materials or data, regardless of physical form or characteristics, made or received by any officer or employee of any agency, executive office, department, board, commission,

bureau, division or authority of the commonwealth, or of any political subdivision thereof, or of any authority established by the general court to serve a public purpose, unless such materials or data fall within the following exemptions in that they are:

- (a) specifically or by necessary implication exempted from disclosure by statute;
- (b) related solely to internal personnel rules and practices of the government unit, provided however, that such records shall be withheld only to the extent that proper performance of necessary governmental functions requires such withholding;
- (c) personnel and medical files or information; also any other materials or data relating to a specifically named individual, the disclosure of which may constitute an unwarranted invasion of personal privacy;
- (d) inter-agency or intra-agency memoranda or letters relating to policy positions being developed by the agency; but this subclause shall not apply to reasonably completed factual studies or reports on which the development of such policy positions has been or may be based;
- (e) notebooks and other materials prepared by an employee of the commonwealth which are personal to him and not maintained as part of the files of the governmental unit;
- (f) investigatory materials necessarily compiled out of the public view by law enforcement or other investigatory officials the disclosure of which materials would probably so prejudice the possibility of effective law enforcement that such disclosure would not be in the public interest;
- (g) trade secrets or commercial or financial information voluntarily provided to an agency for use in developing governmental policy and upon a promise of confidentiality; but this subclause shall not apply to information submitted as required by law or as a condition of receiving a governmental contract or other benefit;

(h) proposals and bids to enter into any contract or agreement until the time for the opening of bids in the case of proposals or bids to be opened publicly, and until the time for the receipt of bids or proposals has expired in all other cases; and inter-agency or intra-agency communications made in connection with an evaluation process for reviewing bids or proposals, prior to a decision to enter into negotiations with or to award a contract to, a particular person;

(i) appraisals of real property acquired or to be acquired until (1) a final agreement is entered into; or (2) any litigation relative to such appraisal has been terminated; or (3) the time within which to commence such litigation has expired;

(j) the names and addresses of any persons contained in, or referred to in, any applications for any licenses to carry or possess firearms issued pursuant to chapter one hundred and forty or any firearms identification cards issued pursuant to said chapter one hundred and forty and the names and addresses on sales or transfers of any firearms, rifles, shotguns, or machine guns or ammunition therefor, as defined in said chapter one hundred and forty and the names and addresses on said licenses or cards;

<[There is no subclause (k).]>

(l) questions and answers, scoring keys and sheets and other materials used to develop, administer or score a test, examination or assessment instrument; provided, however, that such materials are intended to be used for another test, examination or assessment instrument;

(m) contracts for hospital or related health care services between (i) any hospital, clinic or other health care facility operated by a unit of state, county or municipal government and (ii) a health maintenance organization arrangement approved under chapter one hundred and seventy-six I, a nonprofit hospital service corporation or medical service corporation organized pursuant to chapter one hundred and seventy-six A and chapter one hundred and seventy-six B, respectively, a health insurance corporation licensed under chapter one hundred and seventy-five or any legal entity that is self insured and provides health care benefits to its employees.

(n) records, including, but not limited to, blueprints, plans, policies, procedures and schematic drawings, which relate to internal layout and structural elements, security measures, emergency preparedness, threat or vulnerability assessments, or any other records relating to the security or safety of persons or buildings, structures, facilities, utilities, transportation or other infrastructure located within the commonwealth, the disclosure of which, in the reasonable judgment of the record custodian, subject to review by the supervisor of public records under subsection (b) of section 10 of chapter 66, is likely to jeopardize public safety.

(o) the home address and home telephone number of an employee of the judicial branch, an unelected employee of the general court, an agency, executive office, department, board, commission, bureau, division or authority of the commonwealth, or of a political subdivision thereof or of an authority established by the general court to serve a public purpose, in the custody of a government agency which maintains records identifying persons as falling within those categories; provided that the information may be disclosed to an employee organization under chapter 150E, a nonprofit organization for retired public employees under chapter 180, or a criminal justice agency as defined in section 167 of chapter 6.

(p) the name, home address and home telephone number of a family member of a commonwealth employee, contained in a record in the custody of a government agency which maintains records identifying persons as falling within the categories listed in subclause (o).

(q) Adoption contact information and indices therefore of the adoption contact registry established by section 31 of chapter 46.

(r) Information and records acquired under chapter 18C by the office of the child advocate.

(s) trade secrets or confidential, competitively-sensitive or other proprietary information provided in the course of activities conducted by a governmental body as an energy supplier under a license granted by the department of public utilities pursuant to section 1F of chapter 164, in the course of activities conducted as a municipal aggregator under section 134 of said chapter 164 or in the course of activities conducted by a cooperative consisting of governmental entities organized pursuant to section 136 of said chapter 164, when such governmental body, municipal aggregator or cooperative determines that such disclosure will adversely affect its ability to conduct business in relation to other entities making, selling or distributing electric power and energy; provided, however, that this subclause shall not exempt a public entity from disclosure required of a private entity so licensed. Any person denied access to public records may pursue the remedy provided for in section ten of chapter sixtysix.

Twenty-seventh, "Salary" shall mean annual salary.

Twenty-eighth, "Savings banks" shall include institutions for savings.

<[There is no clause Twenty-ninth.]>

Thirtieth, "Spendthrift" shall mean a person who is liable to be put under guardianship on account of excessive drinking, gaming, idleness or debauchery.

Thirty-first, "State", when applied to the different parts of the United States, shall extend to and include the District of Columbia and the several territories; and the words "United States" shall include said district and territories.

Thirty-second, "State auditor" and "state secretary" shall mean respectively the auditor of the commonwealth and the secretary of the commonwealth. "State treasurer" or "treasurer of the commonwealth" shall mean the treasurer and receiver general as used in the constitution of the commonwealth, and shall have the same meaning in all contracts, instruments, securities and other documents. Thirty-third, "Swear" shall include affirm in cases in which an affirmation may be substituted for an oath. When applied to public officers who are required by the constitution to take oaths therein prescribed, it shall refer to those oaths; and when applied to any other officer it shall mean sworn to the faithful performance of his official duties.

Thirty-fourth, "Town", when applied to towns or officers or employees thereof, shall include city.

Thirty-fifth, "Valuation", as applied to a town, shall mean the valuation of such town as determined by the last preceding apportionment made for the purposes of the state tax.

Thirty-sixth, "Water district" shall include water supply district.

Thirty-seventh, "Will" shall include codicils.

Thirty-eighth, "Written" and "in writing" shall include printing, engraving, lithographing and any other mode of representing words and letters; but if the written signature of a person is required by law, it shall always be his own handwriting or, if he is unable to write, his mark.

Thirty-ninth, "Annual election", as applied to municipal elections in cities holding such elections biennially, shall mean biennial election.

Fortieth, "Surety" or "Sureties", when used with reference to a fidelity bond of an officer or employee of a county, city, town or district, shall mean a surety company authorized to transact business in the commonwealth.

Forty-first, "Population", when used in connection with the number of inhabitants of a county, city, town or district, shall mean the population as determined by the last preceding national census.

<[There is no clause Forty-second.]>

**UNCLASSIFIED**

Forty-third, "Veteran" shall mean (1) any person, (a) whose last discharge or release from his wartime service as defined herein, was under honorable conditions and who (b) served in the army, navy, marine corps, coast guard, or air force of the United States, or on full time national guard duty under Titles 10 or 32 of the United States Code or under sections 38, 40 and 41 of chapter 33 for not less than 90 days active service, at least 1 day of which was for wartime service; provided, however, than any person who so served in wartime and was awarded a service-connected disability or a Purple Heart, or who died in such service under conditions other than dishonorable, shall be deemed to be a veteran notwithstanding his failure to complete 90 days of active service; (2) a member of the American Merchant Marine who served in armed conflict between December 7, 1941 and December 31, 1946, and who has received honorable discharges from the United States Coast Guard, Army, or Navy; (3) any person (a) whose last discharge from active service was under honorable conditions, and who (b) served in the army, navy, marine corps, coast guard, or air force of the United States for not less than 180 days active service; provided, however, that any person who so served and was awarded a service-connected disability or who died in such service under conditions other than dishonorable, shall be deemed to be a veteran notwithstanding his failure to complete 180 days of active service.

"Wartime service" shall mean service performed by a "Spanish War veteran", a "World War I veteran", a

"World War II veteran", a "Korean veteran", a "Vietnam veteran", a "Lebanese peace keeping force veteran", a "Grenada rescue mission veteran", a "Panamanian intervention force veteran", a "Persian Gulf veteran", or a member of the "WAAC" as defined in this clause during any of the periods of time described herein or for which such medals described below are awarded.

"Spanish War veteran" shall mean any veteran who performed such wartime service between February fifteenth, eighteen hundred and ninety-eight and July fourth, nineteen hundred and two.

"World War I veteran" shall mean any veteran who (a) performed such wartime service between April sixth, nineteen hundred and seventeen and November eleventh, nineteen hundred and eighteen, or (b) has been awarded the World War I Victory Medal, or (c) performed such service between March twenty-fifth, nineteen hundred and seventeen and August fifth, nineteen hundred and seventeen, as a Massachusetts National Guardsman. "World War II veteran" shall mean any veteran who performed such wartime service between September 16, 1940 and July 25, 1947, and was awarded a World War II Victory Medal, except that for the purposes of chapter 31 it shall mean all active service between the dates of September 16, 1940 and June 25, 1950. "Korean veteran" shall mean any veteran who performed such wartime service between June twenty-fifth, nineteen hundred and fifty and January thirty-first, nineteen hundred and fifty-five, both dates inclusive, and any person who has received the Korea Defense Service Medal as established in the Bob Stump National Defense Authorization Act for fiscal year 2003.

"Korean emergency" shall mean the period between June twenty-fifth, nineteen hundred and fifty and January thirty-first, nineteen hundred and fifty-five, both dates inclusive.

"Vietnam veteran" shall mean (1) any person who performed such wartime service during the period commencing August fifth, nineteen hundred and sixty-four and ending on May seventh, nineteen hundred and seventyfive, both dates inclusive, or (2) any person who served at least one hundred and eighty days of active service in the armed forces of the United States during the period between February first, nineteen hundred and fifty-five and August fourth, nineteen hundred and sixty-four; provided, however, that for the purposes of the application of the provisions of chapter thirty-one, it shall also include all active service between the dates May seventh, nineteen hundred and seventy-five and June fourth, nineteen hundred and seventy-six;

**UNCLASSIFIED**

and provided, further, that any such person who served in said armed forces during said period and was awarded a service-connected disability or a Purple Heart, or who died in said service under conditions other than dishonorable, shall be deemed to be a veteran notwithstanding his failure to complete one hundred and eighty days of active service.

“Lebanese peace keeping force veteran” shall mean any person who performed such wartime service and received a campaign medal for such service during the period commencing August twenty-fifth, nineteen hundred and eighty-two and ending when the President of the United States shall have withdrawn armed forces from the country of Lebanon.

“Grenada rescue mission veteran” shall mean any person who performed such wartime service and received a campaign medal for such service during the period commencing October twenty-fifth, nineteen hundred and eighty-three to December fifteenth, nineteen hundred and eighty-three, inclusive.

“Panamanian intervention force veteran” shall mean any person who performed such wartime service and received a campaign medal for such service during the period commencing December twentieth, nineteen hundred and eighty-nine and ending January thirty-first, nineteen hundred and ninety.

“Persian Gulf veteran” shall mean any person who performed such wartime service during the period commencing August second, nineteen hundred and ninety and ending on a date to be determined by presidential proclamation or executive order and concurrent resolution of the Congress of the United States. “WAAC” shall mean any woman who was discharged and so served in any corps or unit of the United States established for the purpose of enabling women to serve with, or as auxiliary to, the armed forces of the United States and such woman shall be deemed to be a veteran.

None of the following shall be deemed to be a “veteran”:

(a) Any person who at the time of entering into the armed forces of the United States had declared his intention to become a subject or citizen of the United States and withdrew his intention under the provisions of the act of Congress approved July ninth, nineteen hundred and eighteen.

(b) Any person who was discharged from the said armed forces on his own application or solicitation by reason of his being an enemy alien.

(c) Any person who has been proved guilty of willful desertion.

(d) Any person whose only service in the armed forces of the United States consists of his service as a member of the coast guard auxiliary or as a temporary member of the coast guard reserve, or both.

(e) Any person whose last discharge or release from the armed forces is dishonorable.

“Armed forces” shall include army, navy, marine corps, air force and coast guard.

“Active service in the armed forces”, as used in this clause shall not include active duty for training in the army national guard or air national guard or active duty for training as a reservist in the armed forces of the United States.

Forty-fourth, “Registered mail”, when used with reference to the sending of notice or of any article having no intrinsic value shall include certified mail.

Forty-fifth, “Pledge”, “Mortgage”, “Conditional Sale”, “Lien”, “Assignment” and like terms, when used in referring to a security interest in personal property shall include a corresponding type of

**UNCLASSIFIED**

security interest under chapter one hundred and six of the General Laws, the Uniform Commercial Code.

Forty-sixth, "Forester", "state forester" and "state fire warden" shall mean the commissioner of environmental management or his designee.

Forty-seventh, "Fire fighter", "fireman" or "permanent member of a fire department", shall include the chief or other uniformed officer performing similar duties, however entitled, and all other fire officers of a fire department, including, without limitation, any permanent crash crewman, crash boatman, fire controlman or assistant fire controlman employed at the General Edward Lawrence Logan International Airport, or members of the Massachusetts military reservation fire department.

Forty-eighth, "Minor" shall mean any person under eighteen years of age.

Forty-ninth, "Full age" shall mean eighteen years of age or older.

Fiftieth, "Adult" shall mean any person who has attained the age of eighteen.

Fifty-first, "Age of majority" shall mean eighteen years of age.

Fifty-second, "Superior court" shall mean the superior court department of the trial court, or a session thereof for holding court.

Fifty-third, "Land court" shall mean the land court department of the trial court, or a session thereof for holding court.

Fifty-fourth, "Probate court", "court of insolvency" or "probate and insolvency court" shall mean a division of the probate and family court department of the trial court, or a session thereof for holding court.

Fifty-fifth, "Housing court" shall mean a division of the housing court department of the trial court, or a session thereof for holding court.

Fifty-sixth, "District court" or "municipal court" shall mean a division of the district court department of the trial court, or a session thereof for holding court, except that when the context means something to the contrary, said words shall include the Boston municipal court department.

Fifty-seventh, "Municipal court of the city of Boston" shall mean the Boston municipal court department of the trial court, or a session thereof for holding court.

Fifty-eighth, "Juvenile court" shall mean a division of the juvenile court department of the trial court, or a session thereof for holding court.

**CREDIT(S)**

Amended by St.1934, c. 283; St.1935, c. 26; St.1936, c. 180; St.1937, c. 38; St.1938, c. 245; St.1941, c. 91, § 1; St.1941, c. 509, § 1; St.1945, c. 242, § 1; St.1945, c. 637, § 1; St.1946, c. 190; St.1948, c. 241; St.1951, c. 215, § 1; St.1953, c. 319, § 2; St.1954, c. 128, § 1; St.1954, c. 627, § 1; St.1955, c. 99, §§ 1, 2; St.1955, c. 403, § 1; St.1955, c. 683; St. 1956, c. 281, §§ 1, 2; St.1957, c. 164, § 1; St.1957, c. 765, § 3; St.1958, c. 140; St.1958, c. 626, § 1; St.1960, c. 299; St.1960, c. 544, § 1; St.1960, c. 812, § 1; St.1962, c. 427, § 1; St.1962, c. 616, § 1; St.1964, c. 322; St.1965, c. 875, §§ 1, 2; St.1966, c. 716; St.1967, c. 437; St.1967, c. 844, § 23; St.1968, c. 24, § 1; St.1968, c. 531, § 1; St.1969, c. 544, § 1; St.1969, c. 831, § 2; St.1970, c. 215, § 1; St.1973, c. 925, § 1; St.1973, c. 1050, § 1; St.1974, c. 205, § 1; St.1974, c. 493, § 1; St.1975, c. 706, § 2; St.1976, c. 112, § 1; St.1976, c. 156; St.1977, c. 130; St.1977, c. 691, § 1; St.1977, c. 977; St.1978, c. 12; St.1978, c. 247; St.1978, c. 478, § 2; St.1979, c. 230; St.1982, c. 189, § 2; St.1983, c. 113; St.1984, c. 363, §§ 1 to 4; St.1985, c. 114; St.1985, c. 220; St.1985, c. 451, § 1;



St.1986, c. 534, §§ 1, 2; St.1987, c. 465, §§ 1, 1A; St.1987, c. 522, § 1; St.1987, c. 587, § 1; St.1988, c. 180, § 1; St.1989, c. 665, § 1; St.1991, c. 109, §§ 1, 2; St.1992, c. 133, § 169; St.1992, c. 286, § 1; St.1992, c. 403, § 1; St.1996, c. 204, § 3; St.1996, c. 450, §§ 1 to 4; St.2002, c. 313, § 1; St.2004, c. 116, § 1, eff. Aug. 26, 2004; St.2004, c. 122, § 2, eff. Sept. 1, 2004; St.2004, c. 149, § 8, eff. July 1, 2004; St.2004, c. 349, eff. Dec. 15, 2004; St.2005, c. 130, § 1, eff. Nov. 11, 2005; St.2007, c. 109, § 1, eff. Dec. 5, 2007; St.2008, c. 176, § 2, eff. July 8, 2008; St.2008, c. 308, § 1, eff. Sept. 1, 2008; St.2008, c. 445, § 1, eff.

Mar. 30, 2009.

Current through Chapter 10 of the 2009 1st Annual Sess.

(c) 2009 Thomson Reuters.

END OF DOCUMENT

M.G.L.A. 4 § 7 Page 11

---

**Effective:[See Text Amendments]**

Massachusetts General Laws Annotated Currentness

Part I. Administration of the Government (Ch. 1–182)

Title II. Executive and Administrative Officers of the Commonwealth (Ch. 6–28A)

Chapter 6. The Governor, Lieutenant Governor and Council, Certain Officers Under the Governor and

Council, and State Library (Refs & Annos)

§ 172. Dissemination of record information; certification; eligibility for access; scope of inquiry; listing; access limited; rules; use of information except as otherwise provided in this section and sections one hundred and seventy-three to one hundred and seventy-five, inclusive, criminal offender record information, and where present, evaluative information, shall be disseminated, whether directly or through any intermediary, only to (a) criminal justice agencies; (b) such other agencies and individuals required to have access to such information by statute including United States Armed Forces recruiting offices for the purpose of determining whether a person enlisting has been convicted of a felony as set forth in Title 10, section 504 of the United States Code; to the active or organized militia of the commonwealth for the purpose of determining whether a person enlisting has been convicted of a felony, and (c) any other agencies and individuals where it has been determined that the public interest in disseminating such information to these parties clearly outweighs the interest in security and privacy. The extent of such access shall be limited to that necessary for the actual performance of the criminal justice duties of criminal justice agencies under clause (a); to that necessary for the actual performance of the statutory duties of agencies and individuals granted access under clause (b); and to that necessary for the actual performance of the actions or duties sustaining the public interest as to agencies or individuals granted access under clause (c). Agencies or individuals granted access under clause (c) shall be eligible to receive criminal offender record information obtained through interstate systems if the board determines that such information is necessary for the performance of the actions or duties sustaining the public interest with respect to such agencies or individuals. The board shall certify those agencies and individuals requesting access to criminal offender record information that qualify for such access under clauses (a) or (b) of this section, and shall specify for each such agency or individual certified, the extent of its access. The board shall make a finding in writing of eligibility, or noneligibility of each such agency or

individual which requests such access. No such information shall be disseminated to any agency or individual prior to the board's determination of eligibility, or, in cases in which the board's decision is appealed, prior to the final judgment of a court of competent jurisdiction that such agency or individual is so eligible.

No agency or individual shall have access to criminal offender record information under clause (c), unless the board, by a two-thirds majority of the members present and voting, determines and certifies that the public interest in disseminating such information to such party clearly outweighs the interest in security and privacy. The extent of access to such information under clause (c) shall also be determined by such a two-thirds majority vote of the board. Certification for access under clause (c) may be either access to information relating to a specific identifiable individual, or individuals, on a single occasion; or a general grant of access for a specified period of time not to exceed two years. A general grant of access need not relate to a request for access by the party or parties to be certified. Except as otherwise provided in this paragraph the procedure and requirements for certifying agencies and individuals under clause (c) shall be according to the provisions of the preceding paragraphs of this section.

Each agency holding or receiving criminal offender record information shall maintain, for such period as the board shall determine, a listing of the agencies or individuals to which it has released or communicated such information.

Such listings, or reasonable samples thereof, may from time to time be reviewed by the board or the council to determine whether any statutory provisions or regulations have been violated.

Dissemination of criminal offender record information shall, except as provided in this section and for purposes of research programs approved under section one hundred and seventy-four, be permitted only if the inquiry is based upon name, fingerprints, or other personal identifying characteristics. The board shall adopt rules to prevent dissemination of such information where inquiries are based upon categories of offense or data elements other than said characteristics; provided, however, that access by criminal justice agencies to criminal offender record information on the basis of data elements other than personal identifying characteristics, including but not limited to, categories of offense, mode of operation, photographs and physical descriptive data generally, shall be permissible, except as may be limited by the regulations of the board. Except as authorized by this chapter it shall be unlawful to request or require a person to provide a copy of his criminal offender record information. At the time of making any criminal record inquiry pursuant to clause (b) or (c) of the first paragraph of this section, the party certified to receive criminal offender record information shall submit to the board an acknowledgement that such inquiry will be undertaken, signed by the person who is the subject of such inquiry on a form prepared or approved by the board.

Notwithstanding any other provisions of this section, the following information shall be available to any person upon request: (a) criminal offender record information consisting of conviction data; provided, however, that all requests for such conviction data shall be made to the board; and provided, further, that the board shall disclose only conviction data which it maintains in a standardized format in its automated criminal history file, and (b) information indicating custody status and placement within the correction system; provided, however, that no information shall be disclosed that identifies family members, friends, medical or psychological history, or any other personal information unless such information is directly relevant to such release or custody placement decision, and no information shall be provided if its release would violate any other provisions of state or federal law. The parole board, except as required by section one hundred and thirty of chapter one hundred and twentyseven, the department of correction, a county correctional authority, or a probation department with the approval

**UNCLASSIFIED**

of a justice to the appropriate division of the trial court, may, in its discretion, make available a summary, which may include references to evaluative information, concerning a decision to release an individual on a permanent or temporary basis, to deny such release, or to change his custody status.

Information shall be provided or made available pursuant to the preceding paragraph only if the individual named in the request or summary has been convicted of a crime punishable by imprisonment for a term of five years or more, or has been convicted of any crime and sentenced to any term of imprisonment, and at the time of the request: is serving a sentence of probation or incarceration, or is under the custody of the parole board; or having been convicted of a misdemeanor, has been released from all custody or supervision for not more than one year; or having been convicted of a felony, has been released from all custody or supervision for not more than two years; or, having been sentenced to the custody of the department of correction, has finally been discharged therefrom, either having been denied release on parole or having been returned to penal custody for violation of parole, for not more than three years. In addition to the provisions of the preceding sentence, court records for all criminal cases shall be made available for public inspection for a period of one week following conviction and imposition of sentence.

Any individual or agency, public or private, that receives or obtains criminal offender record information, in violation of the provisions of this statute, whether directly or through any intermediary, shall not collect, store, disseminate, or use such criminal offender record information in any manner or for any purpose. Notwithstanding the provisions of this section, the dissemination of information relative to a person's conviction of automobile law violations as defined by section one of chapter ninety C, or information relative to a person's charge of operating a motor vehicle while under the influence of intoxicating liquor which resulted in his assignment to a driver alcohol program as described in section twenty-four D of chapter ninety, shall not be prohibited where such dissemination is made, directly or indirectly, by the motor vehicle insurance merit rating board established pursuant to section one hundred and eighty-three of chapter six, to an insurance company doing motor vehicle insurance business within the commonwealth, or to such insurance company's agents, independent contractors or insurance policyholders to be used exclusively for motor vehicle insurance purposes. Notwithstanding the provisions of this section or chapter sixty-six A, the following shall be public records: (1) police daily logs, arrest registers, or other similar records compiled chronologically, provided that no alphabetical arrestee, suspect, or similar index is available to the public, directly or indirectly; (2) chronologically maintained court records of public judicial proceedings, provided that no alphabetical or similar index of criminal defendants is available to the public, directly or indirectly; (3) published records of public court or administrative proceedings, and of public judicial administrative or legislative proceedings; and (4) decisions of the parole board as provided in section one hundred and thirty of chapter one hundred and twenty-seven.

**CREDIT(S)**

Added by St.1972, c. 805, § 1. Amended by St.1977, c. 365, § 1; St.1977, c. 691, § 4; St.1977, c. 841; St.1982, c. 31; St.1989, c. 268, § 1; St.1990, c. 177, § 6; St.1990, c. 319, §§ 7 to 12.

Current through Chapter 10 of the 2009 1st Annual Sess.

(c) 2009 Thomson Reuters.

END OF DOCUMENT

M.G.L.A. 6 § 172 Page 3

---

**Effective:[See Text Amendments]**

Massachusetts General Laws Annotated Currentness

Part I. Administration of the Government (Ch. 1–182)

Title II. Executive and Administrative Officers of the Commonwealth (Ch. 6–28A)

Chapter 12. Department of the Attorney General, and the District Attorneys (Refs & Annos)

§ 11H. Violations of constitutional rights; civil actions by attorney general; venue

Whenever any person or persons, whether or not acting under color of law, interfere by threats, intimidation or coercion, or attempt to interfere by threats, intimidation or coercion, with the exercise or enjoyment by any other person or persons of rights secured by the constitution or laws of the United States, or of rights secured by the constitution or laws of the commonwealth, the attorney general may bring a civil action for injunctive or other appropriate equitable relief in order to protect the peaceable exercise or enjoyment of the right or rights secured.

Said civil action shall be brought in the name of the commonwealth and shall be instituted either in the superior court for the county in which the conduct complained of occurred or in the superior court for the county in which the person whose conduct complained of resides or has his principal place of business.

CREDIT(S)

Added by St.1979, c. 801, § 1. Amended by St.1982, c. 634, § 4.

Current through Chapter 10 of the 2009 1st Annual Sess.

(c) 2009 Thomson Reuters.

END OF DOCUMENT

M.G.L.A. 12 § 11H Page 1

---

**Effective: July 8, 2008**

Massachusetts General Laws Annotated Currentness

Part I. Administration of the Government (Ch. 1–182)

Title X. Public Records (Ch. 66–66A)

Chapter 66. Public Records (Refs & Annos)

§ 10. Public inspection and copies of records; presumption; exceptions

(a) Every person having custody of any public record, as defined in clause Twenty-sixth of section seven of chapter four, shall, at reasonable times and without unreasonable delay, permit it, or any segregable portion of a record which is an independent public record, to be inspected and examined by any person, under his supervision, and shall furnish one copy thereof upon payment of a reasonable fee. Every person for whom a search of public records is made shall, at the direction of the person having custody of such records, pay the actual expense of such search. The following fees shall apply to any public record in the custody of the state police, the Massachusetts bay transportation authority police or any municipal police department or fire

department: for preparing and mailing a motor vehicle accident report, five dollars for not more than six pages and fifty cents for each additional page; for preparing and mailing a fire insurance report, five dollars for not more than six pages plus fifty cents for each additional page; for preparing and mailing crime, incident or miscellaneous reports, one dollar per page; for furnishing any public record, in hand, to a person requesting such records, fifty cents per page. A page shall be defined as one side of an eight and one-half inch by eleven inch sheet of paper.

(b) A custodian of a public record shall, within ten days following receipt of a request for inspection or copy of a public record, comply with such request. Such request may be delivered in hand to the office of the custodian or mailed via first class mail. If the custodian refuses or fails to comply with such a request, the person making the request may petition the supervisor of records for a determination whether the record requested is public. Upon the determination by the supervisor of records that the record is public, he shall order the custodian of the public record to comply with the person's request. If the custodian refuses or fails to comply with any such order, the supervisor of records may notify the attorney general or the appropriate district attorney thereof who may take whatever measures he deems necessary to insure compliance with the provisions of this section. The administrative remedy provided by this section shall in no way limit the availability of the administrative remedies provided by the commissioner of administration and finance with respect to any officer or employee of any agency, executive office, department or board; nor shall the administrative remedy provided by this section in any way limit the availability of judicial remedies otherwise available to any person requesting a public record.

If a custodian of a public record refuses or fails to comply with the request of any person for inspection or copy of a public record or with an administrative order under this section, the supreme judicial or superior court shall have jurisdiction to order compliance.

(c) In any court proceeding pursuant to paragraph (b) there shall be a presumption that the record sought is public, and the burden shall be upon the custodian to prove with specificity the exemption which applies.

(d) The clerk of every city or town shall post, in a conspicuous place in the city or town hall in the vicinity of the clerk's office, a brief printed statement that any citizen may, at his discretion, obtain copies of certain public records from local officials for a fee as provided for in this chapter.

The executive director of the criminal history systems board, the criminal history systems board and its agents, servants, and attorneys including the keeper of the records of the firearms records bureau of said department, or any licensing authority, as defined by chapter one hundred and forty shall not disclose any records divulging or tending to divulge the names and addresses of persons who own or possess firearms, rifles, shotguns, machine guns and ammunition therefor, as defined in said chapter one hundred and forty and names and addresses of persons licensed to carry and/or possess the same to any person, firm, corporation, entity or agency except criminal justice agencies as defined in chapter six and except to the extent such information relates solely to the person making the request and is necessary to the official interests of the entity making the request.

The home address and home telephone number of law enforcement, judicial, prosecutorial, department of youth services, department of children and families, department of correction and any other public safety and criminal justice system personnel, and of unelected general court personnel, shall not be public records in the custody of the employers of such personnel or the public employee retirement administration commission or any retirement board established under chapter 32 and shall not be disclosed, but such information may be disclosed to an

employee organization under chapter 150E, a nonprofit organization for retired public employees under chapter 180 or to a criminal justice agency as defined in section 167 of chapter 6. The name and home address and telephone number of a family member of any such personnel shall not be public records in the custody of the employers of the foregoing persons or the public employee retirement administration commission or any retirement board established under chapter 32 and shall not be disclosed. The home address and telephone number or place of employment or education of victims of adjudicated crimes, of victims of domestic violence and of persons providing or training in family planning services and the name and home address and telephone number, or place of employment or education of a family member of any of the foregoing shall not be public records in the custody of a government agency which maintains records identifying such persons as falling within such categories and shall not be disclosed.

CREDIT(S)

Amended by St.1948, c. 550, § 5; St.1973, c. 1050, § 3; St.1976, c. 438, § 2; St.1978, c. 294; St.1982, c. 189, § 1; St.1982, c. 477; St.1983, c. 15; St.1991, c. 412, § 55; St.1992, c. 286, § 146; St.1996, c. 39, § 1; St.1996, c. 151, § 210; St.1998, c. 238; St.2000, c. 159, § 133; St.2004, c. 149, § 124, eff. July 1, 2004; St.2008, c. 176, § 61, eff. July 8, 2008.

Current through Chapter 10 of the 2009 1st Annual Sess.

(c) 2009 Thomson Reuters.

END OF DOCUMENT

M.G.L.A. 66 § 10 Page 2

---



## DATA USE AGREEMENT

New Hire ☐
 Intern ☐
 Contractor ☐
 Special Officer ☐
 Other (Describe below) ☐
 Renewal ☐

This Agreement is entered into effective as of \_\_\_\_\_ between the Boston Police Department (“Department”) and \_\_\_\_\_ (“Recipient”).

As a condition to and in consideration of the Department’s allowing access to confidential information within the Boston Police Department Network, as well as BPD Record Management System (“RMS”) to Recipient, Recipient agrees to the restrictions and undertakings contained in this Agreement.

Recipient hereby acknowledges that he/she is employed by \_\_\_\_\_, an organization to which he/she is in good standing. Recipient agrees (1) not to disclose any information that can be accessed when logged into any Boston Police Department system/RMS, with the exception of information contained in incident reports authored by the Recipient, unless for legitimate law enforcement purposes; (2) to identify himself/herself within the narrative of authored incident reports; (3) not to view or access information which he/she has not been granted access and to immediately notify the Department in the event of any unauthorized or improper use or disclosure of the information contained within any BPD system/RMS; and (4) to renew this Agreement with the Department annually.

Recipient hereby acknowledges that unauthorized disclosure or use of confidential information could cause irreparable harm and significant injury, which may be difficult to ascertain. Accordingly, Recipient agrees that the Department shall have the right to seek and obtain immediate injunctive relief from breaches of this Agreement, in addition to any other rights and remedies it may have.

This Agreement shall bind and inure to the benefit of the parties hereto, except that confidential information available within any BPD system/RMS and the rights and obligations under this Agreement may not be assigned by Recipient without prior written consent of the Department. This document contains the entire agreement between the parties with respect to the subject matter hereof, and may not be amended, nor any obligation waived, except by a writing signed by both parties hereto. Any failure to enforce any provision of this Agreement shall not constitute a waiver. This Agreement shall be governed by and construed and enforced in accordance with the laws of the State of Massachusetts and the parties hereto agree to submit to the exclusive jurisdiction of the courts of Massachusetts any disputes arising out of the subject matter.

### UNDERSTOOD AND AGREED:

\_\_\_\_\_  
Recipient Signature:

\_\_\_\_\_  
Date:

\_\_\_\_\_  
Name:

\_\_\_\_\_  
Telephone Number

\_\_\_\_\_  
Company:

\_\_\_\_\_  
Email Address

\_\_\_\_\_  
**BPD Sponsor Name**

\_\_\_\_\_  
**BPD Sponsor Signature**

\_\_\_\_\_  
**BPD Sponsor Phone #**

Approved \_\_\_\_\_

Denied \_\_\_\_\_

Reason \_\_\_\_\_

\_\_\_\_\_  
**BPD Technology Services Signature**

\_\_\_\_\_  
**Date.**



## DATA USE AGREEMENT

### INTERNS ONLY

**Below indicate the dates of internship.** Your access will be terminated upon internship end date. Any change of date must be approved by a supervisor and the appropriate parties must be notified in order to maintain access.

Start Date \_\_\_\_\_

End Date \_\_\_\_\_

Check the application(s) you request access to and the reason for the access. Some applications will require additional training and/or certification before access can be granted.

Application Name	Reason for Access	Additional Requirements
CAD/NetViewer		CJIS Certification
Mark43		Mark43 Report Writing Training
Booking Applications		CJIS Certification
CJISweb		CJIS Certification / NexTEST
Gateway Applications (Please Describe)		
Other (Please Describe)		

All persons who may have physical or logical access to Criminal Justice Information (CJI) must complete Criminal Justice Information System (CJIS) security awareness training and pass the Level 4 CJISonline exam. Any person needing direct access to a CJIS terminal must complete CJIS training at the Boston Police Academy and pass the CJIS nexTEST exam for CJIS credentials. CJIS training will be coordinated by ISG when required.





---

## Standard Operating Procedures Manual

---

## Table of Contents

<b>1. INTRODUCTION</b>	<b>4</b>
<b>2. SAFETY</b>	<b>5</b>
2.1 Safety Program Overview	
2.2 Design of Laboratory	
2.3 Basic Rules & Procedures for Lab Safety	
2.4 Fire and Emergency Evacuation Plan	
2.5 Exposure Control Plan	
2.6 Chemical Hygiene Plan	
2.7 Crime Scene Safety	
<b>3. EVIDENCE</b>	<b>17</b>
3.1 Case Files & Barcodes	
3.2 Case & Evidence Information	
3.3 Evidence Examination	
<b>4. PROCESSING</b>	<b>19</b>
4.1 Guidelines for Examination & General Considerations	
4.2 Porous Evidence	
4.3 Non-Porous Evidence	
4.4 Vacuum Metal Deposition Chamber - Physical	
4.5 Blood-Stained Surfaces	
4.6 Adhesive Surfaces	
4.7 Post Processing Procedures	
4.8 Mideo	
4.9 Maintenance Program	
4.10 Conflicts & Workflow	
<b>5. CRIME SCENE</b>	<b>58</b>
5.1 Callout Guidelines	
5.2 Vehicles	
5.3 Notifications and Request for Services	
5.4 Crime Scene Documentation	
<b>6. COMPARISON</b>	<b>60</b>
6.1 Latent Print Fundamentals	
6.2 Comparison Case Strategies	
6.3 Method of Friction Ridge Examination (ACE-V)	
6.4 Mideo	
6.5 Conflicts and Workflows	
6.6 Automated Fingerprint Identification Systems (AFIS)	

<b>7. STORAGE AREA NETWORK (SAN)/DIGITAL IMAGING</b>	<b>74</b>
7.1 Storage Area Network (SAN)	
7.2 General Digital Image Capture	
7.3 Image Download	
7.4 Image Processing	
7.5 Workflow for Digital Images	
<b>8. CASE RECORD AND REPORTS</b>	<b>77</b>
<b>9. CASE REVIEW</b>	<b>81</b>
<b>10. DISCOVERY REQUESTS</b>	<b>82</b>
<b>11. TESTIMONY</b>	<b>83</b>
<b>12. ABBREVIATIONS &amp; TERMS</b>	<b>84</b>

## 1. INTRODUCTION

Any procedures manual pertaining to the latent print discipline shall provide general guidelines and available options without prescribing definitive methods assuring specific results. The composition of impression residue, in either visible or latent form, may consist of a variety of materials. It is possible that these components can be affected by the properties of the substrate on which they reside and by environmental conditions. Because it may not be possible to accurately determine all factors affecting impression evidence when processing items for their presence, examination procedures must be directed by reason and selected by specific goals according to the totality of the evidence under examination.

The comparison process includes analysis, comparison, evaluation, and verification (ACE-V). The analysis, comparison, evaluation, and verification of impressions can be a complex process with significant variations in the degree of difficulty involved. These examinations are documented and preserved to support the evaluations reported.

Procedures included in this manual serve to guide the Latent Print Team through methods to produce thorough, informed, and supported decisions.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 4 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

## 2. SAFETY

### 2.1 SAFETY PROGRAM OVERVIEW

The Latent Print Unit (LPU) is committed to ensuring a safe and injury-free work environment. The General Safety Plan, Exposure Control Plan, and Chemical Hygiene Plan are the written programs developed and implemented by the unit which set forth procedures and practices concerning safety in the workplace. These procedures and practices will provide a safer environment, which is a fundamental prerequisite to accident, injury, and illness prevention.

The LPU has established the philosophy and principles that govern decisions regarding safety. The following are the unit's safety principles:

- All accidents and injuries can be prevented.
- Management is responsible for providing a safe work environment.
- Working safely is a responsibility of all employees.
- Prevention of personal accidents and injuries is a good working practice.
- Deficiencies must be corrected immediately.
- All exposures can be safeguarded.
- Properly trained employees are the key to a safe and injury-free work environment.
- Employees are responsible for reporting all chemical accidents or incidents involving all types of potential exposure.
- Management is responsible for setting and implementing training requirements.

### 2.2 DESIGN OF LABORATORY

Adequate and proper space shall be allocated for each laboratory activity and function. Each employee should have enough working space to efficiently accomplish assigned duties without the risk of mishandling or contaminating evidence. Laboratory personnel will have, in addition to the space needed for technical examinations, space available for report writing and for storage of official laboratory records necessary for their assigned duties. Sufficient space will be provided for each instrument (and its accessories) to facilitate its proper use and operation. There will also be a space provided for storage of infrequently used instruments and equipment.

Fume hoods should be kept uncluttered, ventilation slots should not be blocked, and the sash should be kept as low as possible. Work shall be kept as far inside the hood as possible. The operation of the hood should be checked regularly to guard against airflow blockage, and the hoods shall be inspected annually. Records of the inspections are maintained in the equipment database. Fume hoods should be cleaned on a regular basis. When feasible, work involving flammable gases, toxic vapors, and noxious odors will be performed in the fume hood.

All wiring, plumbing, heating, cooling, and humidity of the laboratory is controlled by the BPD Facilities Management Division.

The Boston Police Headquarters building is equipped with a fire detection system and has fire alarms located throughout the building.

### 2.3 BASIC RULES AND PROCEDURES FOR LAB SAFETY

Employees working in a laboratory environment must be aware of the potential for physical, biological, and chemical hazards. Physical hazards may include, but are not limited to, fire, explosion, firearm discharge, electric shock, or broken glass and other sharp objects. Biological hazards are most typically encountered when handling objects that may have been exposed to biological fluids and may be a potential source of bloodborne pathogens. Chemical hazards are associated with the toxic effects of handling chemicals. These types of hazards may include acute reactions such as burns, allergic responses, or chronic problems such as lead exposure and carcinogenic effects.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 5 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

The hazard of such evidence will vary according to the nature and concentration of the infecting agent, the route of transmission, and the susceptibility of the exposed laboratory employee. Each evidence specimen must be considered a potential hazard and handled in a manner that protects the lab worker and others in the immediate vicinity from contamination.

### **Methods of Contamination**

**Absorption:** Open cuts or scratches on the skin, particularly the hands, provide a point of entry for infectious agents. Penetration of intact skin is possible by some infecting agents and chemicals, whereas others may enter through the eye or other mucous membranes as a result of contact with contaminated hands.

**Direct Inoculation:** Broken glassware, needles, syringes, forceps, staples on packaging materials, and other sharp objects provide a means of direct injection of infecting agents into the bloodstream.

**Vectors:** Ticks, fleas, body lice and other ectoparasites are potential sources of contamination.

**Ingestion:** Smoking, eating, or drinking after handling evidence specimens and prior to hand washing may result in oral ingestion of infective agents or hazardous chemicals.

**Airborne Contaminants:** Infectious agents or hazardous chemicals may become airborne through accidents, such as spilling or breaking a container, or through a variety of standard laboratory procedures, such as during processing of evidentiary items (dye staining) or through physical handling of evidence. Splashing liquids and flaking material from dried stains are additional sources of airborne agents. Proper ventilation or breathing protection is imperative to reduce the danger of airborne infection.

**Inhalation:** Inhalation of toxic vapors, mists, gases, or dusts can produce poisoning by absorption through the mucous membranes of the mouth, throat, and lungs and can seriously damage these tissues or be carried into the circulatory system.

### **Protective Measures**

The Boston Police Department will provide all employees who work with hazardous materials an opportunity to receive medical attention including any follow-up examinations whenever an employee develops signs or symptoms associated with an exposure to hazardous material or whenever an event takes place such as a spill, leak, or explosion resulting in the likelihood of a hazardous exposure. These examinations will be provided in a timely fashion without cost to the employee, without loss of pay, and at a reasonable time and place. If a new laboratory operation, procedure, or activity involving hazardous materials is to be implemented, it shall be reviewed by the Safety Manager in order to define the risk and preventative measure involved.

### **Personnel Responsibilities**

**Director:** The Director is ultimately responsible for providing a safe working environment and for ensuring that all laboratory personnel are trained in safety and follow proper health and safety precautions and plans. The Director will also work with laboratory employees to develop and administer department specific policies and practices needed to support effective implementation of all safety plans.

**Safety Manager/Back-Up Safety Manager:** The Safety Manager and back-up positions are held by qualified Criminalists. These individuals are responsible for implementing all required plans according to the appropriate regulations, overseeing various laboratory safety plans and programs, ensuring compliance with the safety program, enforcing timely and effective remedial actions to safety concerns, interacting with personnel regarding safety matters, and facilitating safety training.

**Laboratory Personnel:** All laboratory personnel are required to comply with the safety program and are also responsible for the general cleanliness and housekeeping of work areas. It is the responsibility of all employees to conduct their work in a safe manner within the limits of their scientific knowledge, training, and experience. Personnel are encouraged to bring safety concerns to the Safety Manager or the Director.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 6 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

### Elements for Safe Operation

Chemical exposure from reagent use and evidence handling is similar to biological exposure. Therefore, most of the regulations followed are applicable to both chemical and biological risks. The regulations are based on the premise that avoiding contamination is largely a matter of training, organization, housekeeping, personal hygiene, technique, and discipline. The key to laboratory safety is awareness and a sensible approach based on prudent laboratory behavior.

- Appropriate eye protection should be worn whenever a hazard to the eye exists.
- When handling potentially hazardous materials, gloves will be worn that are impervious to the hazard.
- Hands should be washed when any potential contamination was made and before leaving the processing area. Touching the face or any other unprotected body areas with hands or gloves should be avoided.
- All broken, chipped and used glassware, pipettes, hypodermic needles, scalpel blades, etc. will be disposed of in a manner that eliminates potential accidental injury to laboratory and janitorial personnel. These materials will be disposed of either in a "sharps" plastic container or in a cardboard glass disposal container.
- No eating, drinking, or smoking will be permitted in the processing areas of the laboratory.
- Where practical, procedures involving hazardous substances and/or chemical spraying will be performed in chemical hoods.
- Any laboratory situation which is perceived as a hazard by any employee must be reported immediately to the Safety Manager or Director, who will investigate the situation and, if warranted, take steps necessary to alleviate the hazard.
- Chemical and biological evidence will be stored and handled with consideration for both the hazards it presents and its security as evidence.
- A laboratory safety inspection will be conducted annually in order to identify potential hazards or any areas that may require additional safety considerations. The inspection will be led by the Safety Manager to include all laboratory work areas, waste disposal, receiving and storage areas during work hours.

### Safety Training and Information

Each individual is expected to learn and observe all prescribed safety regulations and to use professional judgment concerning the safe conduct of his/her work. If an individual feels that his/her safety is jeopardized by the circumstances of his/her work or of others in the area, he/she should make this known immediately to the other staff member(s) involved as well as to management.

Each new employee completes Safety Training as a part of the training program. All employees review the Safety section of the Manual and complete refresher safety training. Training may include review of:

- General Safety Plan
- Exposure Control Plan
- Hepatitis B Vaccination Program
- Chemical Hygiene Plan
- Boston Police Department Rule 110
- Fire Safety and Evacuation Plan
- General Safety Videos

### Safety concerns

Safety concerns may be submitted as a Form 26 to the Safety Manager, Quality Manager, or Director.

All Safety Concern forms will be maintained in the LPU files. The Safety Manager shall consult with appropriate personnel on how to resolve a safety concern and monitor and document progress toward resolution. When the

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 7 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

concern is resolved, the Safety Manager shall notify the submitter, Quality Manager, and Director of any action taken.

### **Housekeeping**

Each laboratory employee is directly responsible for the cleanliness of his/her workspace, and jointly responsible for common areas of the laboratory.

The following procedures apply to the housekeeping standards of the laboratory:

- All chemical waste shall be disposed of properly.
- Spills on benches and floors will be mopped up immediately and appropriately.
- Bench tops should be kept free from chemicals and equipment not in immediate use.
- Employees will clean counter tops with disinfectant after any potential contamination by chemical or biological material.
- All floors, aisles, exits, fire extinguishing equipment, eye washes, showers, and other emergency equipment shall remain unobstructed.
- Reagents and chemicals should be returned to the proper shelf after use, with their labels facing the front of the shelf. Spills on the sides of bottles should be cleaned off.
- Drawers and cabinet doors should always be completely closed and secured.

### **Safety and Personal Protective Equipment**

The laboratory shall provide safety equipment including laboratory coats, safety glasses, goggles, face shields, gloves, fire extinguishers, and additional equipment necessary for the Criminalists to carry out their assigned duties in a safe manner. Equipment and materials shall be available for the clean-up and disposal of spilled chemicals. Spill kits are located in the Chemical Processing Room.

Visitors, whether BPD staff or from an outside agency, who have obtained permission to enter the unit in which active work is in progress, are expected to comply with all safety regulations.

### **Eye Protection**

Eye protection, such as glasses, goggles, or face shields, will be provided for every employee and should be worn at all appropriate times when using hazardous chemicals, glassware under pressure, explosives, UV light, or biohazards. Eye safety equipment should be capable of being cleaned and disinfected and should always be kept in good condition. Eyewash and shower stations must be located in areas of need and be readily accessible.

### **Laboratory Coats**

Laboratory coats are provided for all employees. All employees should wear clean laboratory coats in work areas when handling chemical and/or biological material. Laboratory coats should not be worn in any administrative areas.

### **Gloves**

Gloves will be provided for every employee and are to be worn whenever an employee anticipates hand contact with potentially hazardous materials. Gloves are to be removed if they are visibly soiled, contaminated, torn, or punctured. Gloves should be removed before touching telephones, door handles, or any other surface outside of the processing room that may be touched routinely by ungloved hands. Gloves will be appropriate for each type of hazard being handled. Proper choice and use of gloves are necessary to ensure maximum safety of staff. The following are examples of available gloves that may be found in the LPU:

- **Latex / Polyvinyl / Nitrile Gloves**

These gloves are routinely worn during evidence examinations and recommended whenever contact with blood or bodily fluids is anticipated in the processing of evidence.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 8 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	



These gloves are designed for single use. Hands should be washed immediately after the removal of gloves. Gloves visibly soiled with blood or bodily fluids must be discarded in the biohazard waste container. If they do not appear to be visibly soiled with blood or body fluids, they may be discarded in the routine waste disposal.

- **Utility Gloves**

These gloves are used in decontamination procedures and clean-up of accidental spills involving biohazardous material. These gloves may be cleaned and reused. Hands should be washed after removal of utility gloves. Gloves should be discarded if holes or tears develop.

- **Cryo Gloves**

These gloves are designed to protect hands against the hazards of working in cold and hot temperatures. Cryo gloves will protect against temperatures from -160°C to 150°C.

### **Footwear**

No open-toed shoes should be worn in the Processing Rooms.

### **First Aid Kits**

First aid kits are available in the laboratory and administrative areas. The first aid kits are inspected as part of the annual safety inspection. Expired contents are replaced as necessary.

### **Safety Showers and Eyewashes**

The laboratory is equipped with a safety shower, one eye/face wash station, and two eye rinsing kits. Eyewashes and the safety shower are checked as part of the annual safety inspection.

In the event of a chemical splash to the eye area:

- Eyelids may have to be forcibly opened to attempt an eye rinse.
- Flood eyes and eyelids with water/eye solution for 15 minutes.
- Notify the Safety Manager and seek further medical attention if needed.

In the event of a chemical splash to the body area:

- Grasp ring chain or triangular rod.
- The safety shower should supply a continuous stream of water to cover the entire body.
- Individual should remove clothing, including shoes and jewelry while under an operating shower.

Notify the Safety Manager or Director and seek further medical attention if needed.

### **Laboratory Equipment Hazards**

Refer to manufacturer's instructions and manuals specific to equipment for information regarding hazards or precautions. No alteration of the manufacturer's safety features will be allowed. Any electrical failure or evidence of undue heating of equipment should be reported immediately to a supervisor. All maintenance will be done by qualified personnel.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 9 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

## Safety Equipment Locations

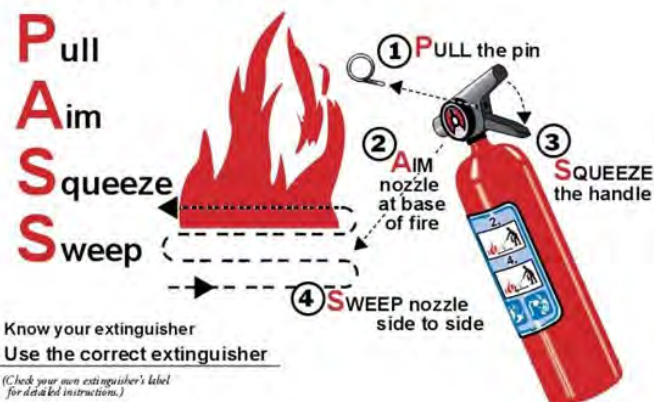


## 2.4 FIRE AND EMERGENCY EVACUATION PLAN

### Fire Safety

The laboratory facilities are equipped with ABC fire extinguishers suitable for paper, wood, cloth (Type A), gas, oil, grease (Type B), or electrical equipment (Type C) type fires, or some combination of the above. The fire extinguishers shall be checked periodically to ensure function. Fire extinguishers are meant for use on small fires only.

To operate an extinguisher:



Safety blankets are also located in the laboratory area.



## Evacuation

The BPD has developed an evacuation plan to aid in the safety of personnel in the case of fire or another emergency situation. The LPU will follow the BPD Headquarters Evacuation plan.

In the event of a fire, bomb threat, explosion, or other emergency, the evacuation plan should be implemented. The BPD Headquarters facility is equipped with an audible alarm and public address system which is activated during an emergency. Floor plans with outlined evacuation routes shall be prominently posted at the exit door of each floor of the LPU.

## 2.5 EXPOSURE CONTROL PLAN

### Overview

The Exposure Control Plan is designed to assist employees in eliminating or minimizing exposure to bloodborne pathogens or other potentially hazardous materials. The degree of risk of acquiring bloodborne pathogens on the job is directly related to the frequency of exposure to blood. The degree of risk of coming in contact with potentially hazardous materials on the job is directly related to the evidentiary items processed.

### Definitions

**Bloodborne Pathogens:** Microorganisms that are present in human blood and can cause disease in humans.

**Potentially Infectious Materials:** Includes body fluids (including but not limited to blood, semen, and vaginal secretions) and any body tissue.

**Occupational Exposure:** Actual or potential skin, eye, or mucous membrane contact with blood or other potentially hazardous materials that may result from the performance of an employee's duties.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 11 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

**Universal Blood and Body Fluid Precautions:** An approach to infection control. According to the concept of universal precautions, all human blood and body components including serum, tissue, and other body fluids are treated as if they are infectious.

**Fentanyl:** a synthetic opioid that mimics the effects of morphine in the human body and has a potency 50-100 times that of morphine. Fentanyl can be ingested orally, inhaled through the nose or mouth, or absorbed through the skin or eyes. Any substance suspected to contain fentanyl should be treated with extreme caution as exposure to a small amount can lead to significant health-related complications, respiratory depression, or death.

**Carfentanil:** a synthetic drug that is used as a tranquilizing agent for elephants and other large mammals. The lethal dose range for carfentanil in humans is unknown. Carfentanil is approximately 100 times more potent than fentanyl.

### Universal Precautions

Employees shall practice universal precautions including wearing appropriate personal protective equipment. The following are assumed to be infected with bloodborne pathogens:

- Blood
- Semen
- Vaginal secretions
- Saliva
- Body Tissue

The laboratory shall have a list of names and phone numbers of agencies to contact in case of an emergency. This information is posted in the laboratory areas.

### Workplace Controls

Employees are responsible for the following in order to help eliminate exposure to bloodborne pathogens or other potentially hazardous materials:

- Eating, drinking, smoking, applying cosmetics, and handling contact lenses is prohibited in work areas where there is potential for exposure.
- Food and drink are not to be kept in refrigerators, freezers, on countertops, or in other storage areas where blood or other potentially hazardous materials are present.
- Employees should maintain clean work areas. When contact with biological fluids is possible, bench tops and equipment should be sanitized using a disinfectant such as 10 percent bleach.
- Any work procedures allowing for generation of aerosols, splashes and spills of potentially hazardous materials should be confined to under a chemical hood, when possible. If working under a hood is not feasible, all involved laboratory personnel shall work only in exam rooms with full protective clothing, goggles, facemasks, and gloves. Contaminated disposable lab coats should be disposed of properly. If contaminated with biological hazards, the coat will be placed in a biohazard receptacle.
- Items or surfaces contaminated with bodily fluids are a potential health hazard to processing Criminalists, particularly when wet. Proper Personal Protective Equipment (PPE) shall be worn during the processing of these types of surfaces, to include, at a minimum, impermeable gloves, and a barrier to any exposed skin. If possible, items or surfaces should be dried prior to the performance of latent print processing techniques.
- Equipment which has become contaminated with blood or other potentially hazardous materials shall be examined prior to servicing or shipping and shall be decontaminated as necessary unless the decontamination of the equipment is not feasible.
- All contaminated sharps shall be disposed of in sharps containers.
- Items with dry or wet blood should be disposed of in accordance with Waste Packaging Procedures.
- For instances when an item arrives without proper labeling it shall be labelled accordingly.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 12 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

**Procedure for Employee Exposure/Injury**

If an employee sustains an accidental exposure/injury, the circumstances involving the accidental exposure/injury are investigated and the employee receives medical consultation (and treatment if required) as expeditiously as possible.

When an inadvertent exposure to blood or other potentially hazardous materials occurs or an injury, **employees** shall:

- Remove contaminated personal protective equipment and place it in a biohazard labeled container.
- Wash exposed areas with soap and water. Flush exposed mucous membranes with water.
- If there is a spill, decontaminate with a disinfectant, such as 10% bleach. If appropriate, arrange for professional cleaning of hazardous substances.
- Seek medical care if needed.
- When the exposure involves traces of fentanyl, carfentanil, or any of its derivatives, the Unit is equipped with Narcan, which will be administered to the employee. Medical attention will follow.
- Report the exposure incident to the Safety Manager or designee.
- Obtain and complete a Safety Concern (Form 26) and return it to the Safety Manager in compliance with BPD Rule 110.
- If necessary, obtain and complete an Unprotected Exposure Form found on the Intranet under On-Line Forms and return it to the Safety Manager.

When an inadvertent exposure to blood or other potentially hazardous materials or an injury occurs, the **Safety Manager** or designee shall:

- Ask the employee to generate a letter documenting the Safety Concern (Form 26) and submit it to the Director/designee.
- Provide the employee an Unprotected Exposure Form.

When an inadvertent exposure to blood or other potentially hazardous materials or an injury occur, the **Director**, or designee, shall provide the following information to the Commander of the Forensic Division regarding post-exposure evaluation:

- The date and time when the incident occurred.
- The location within the LPU where the incident occurred.
- Potentially hazardous materials that were involved in the incident.
- Source of the material.
- Under what circumstances the incident occurred including type of work being performed.
- How the incident was caused.
  - Accident
  - Unusual circumstances (such as equipment malfunction, power outage etc.)
- Personal Protective Equipment being used at the time of the incident.
- Actions taken as a result of the incident.
  - Employee decontamination
  - Cleanup
  - Notifications made

**Proper Disposal of Hazardous Material**

The LPU submits any potentially hazardous material to the Boston Police Department Crime Laboratory for appropriate disposal. The Crime Laboratory complies with the Massachusetts Department of Public Health regulations in handling regulated Hazardous Infectious Waste (HIW) including contaminated sharps and other potentially infectious materials. A commercial hazard waste company is responsible for the collection and handling of all HIW.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 13 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	



## Waste Packaging Procedures

The following waste packaging procedures are used:

- Potentially hazardous waste is bagged in containers that are:
  - Closable
  - Puncture resistant (when necessary)
  - Leak proof if the potential for fluid spill or leakage exists
  - Red in color or labeled with the appropriate biohazard warning label
- Containers and/or bags for hazardous waste are located in the laboratory.
- Waste containers are maintained upright, routinely replaced, and not overfilled.
- Disposable lab coats, gloves, paper towels, bench coverings, and plastic pipettes that are contaminated with dried blood, liquid blood, or bodily fluids should be disposed of in biohazardous waste. Non-contaminated items used in the lab may be placed in regular waste.

## Hepatitis B Vaccination Program

The Boston Police Department has implemented a Hepatitis B Vaccination Program. This program is available, at no cost, to all employees who have the potential for occupational exposure to bloodborne pathogens. The vaccination program consists of a series of three inoculations over a six- month period in accordance with US Public Health Service recommendations. As part of safety training, employees shall receive information regarding Hepatitis B vaccination, including its safety and effectiveness. The Boston Police Department Occupational Health Service is responsible for setting up and operating the Boston Police Department vaccination program. Vaccinations are performed under the supervision of a licensed physician or other healthcare professional. Employees who decline to take part in the program are required to sign a declination form.

## 2.6 CHEMICAL HYGIENE PLAN

### Overview

The Chemical Hygiene Plan is a program that sets forth procedures, equipment, personal protective equipment, and work practices that are capable of protecting employees from the health hazards presented by hazardous chemicals used in the workplace.

### Receipt of Chemicals

Receiving, transporting, unpacking, and dispensing of chemicals and other hazardous materials shall be carried out by trained personnel. Before a substance is received, information on proper handling, storage and disposal should be known to those who will be involved. No container will be accepted without an adequate identifying label.

### Handling of Chemicals

Before the initial use of a chemical, the user shall be familiar with its hazards and the other information in the Safety Data Sheet (SDS). When working with chemicals, hands should be kept clean and away from the face. Most chemicals are harmful to some degree, so direct contact with any chemical should be avoided. Employees will use appropriate Personal Protective Equipment. Chemicals labeled as acute respiratory hazards should not be used in a confined area in large amounts. Such chemicals should be dispensed and handled only where there is adequate ventilation such as in a hood. Only the necessary amount of a chemical should be taken at once. Chemicals should never be returned to their original containers or combined within a container unless instructed by the manufacturer. If chemicals need to be transported, they should be placed in an unbreakable container or in a chemical bottle carrier.

### Labeling of Chemicals

**Flammable:** A material can catch fire or explode above 20°F.

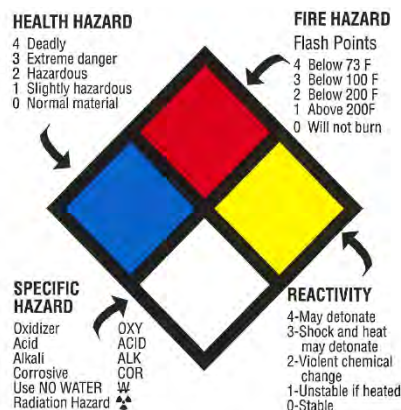
ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 14 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

**Extremely Flammable:** A material can catch fire or explode below 20°F.

**Skin irritation** or **Avoid contact with skin:** The material may cause skin damage and can be extremely hazardous to the eyes. Eye protection is recommended with such material.

**Toxic:** The material is poisonous. Some toxins are absorbed through the skin, some are hazardous when dust or vapors are inhaled, and ALL are harmful if swallowed.

**Causes burns** or **Causes severe irritation:** Contact with the skin will cause a rash or tissue destruction.



All containers of chemicals must be labeled clearly. No unlabeled or improperly labeled substances shall be used. All chemical containers entering and leaving the laboratory will be clearly labeled as to contents, with the label in English, prominently displayed, and not damaged. The label will include appropriate hazard warnings and the manufacturer's name and address. The lot number will be indicated and when a lot number does not already exist, the number shall consist of the date received. Chemical users shall read the manufacturer's label and note the hazards indicated. When chemicals are transferred from the manufacturer's original container to a secondary container, that new container should be appropriately labeled as to chemical identity and hazard warning.

### Labeling Prepared Reagents

Reagents prepared in the laboratory shall be labeled with, at a minimum, the name of the reagent, date of preparation, initials of the preparer, a label indicating the NFPA (National Fire Protection Association) required storage conditions, and a lot number. Preparation of reagents will be documented in the Reagent Preparation Log. Further instruction on the preparation of reagents may be found in other sections of this manual.

### Storage of Chemicals

Chemical storage should be planned with personnel safety in mind. **Chemicals shall be stored according to the chemical properties.** Chemicals should be purchased in quantities that will be utilized in a reasonable period of time. Chemicals not needed should be discarded. Chemicals which are highly toxic should be in unbreakable secondary containers. Stored chemicals shall be examined periodically for replacement, deterioration, and container integrity. Storage of chemicals on bench tops and in hoods is inadvisable. Exposure of chemicals to direct sunlight should be avoided. Acids, bases, and corrosives shall NOT be stored on shelves above head level.

### Safety Data Sheets (SDS)

The Safety Data Sheet (SDS) is the primary means the laboratory will use to convey the necessary information about the hazards of the chemicals used in the laboratory. The chemical manufacturer is responsible for providing us with the SDS. Copies of SDS for all hazardous chemicals to which employees are exposed will be maintained and readily available to all employees. If the SDS's are omitted from a shipment, the Safety Manager, or designee, will contact the manufacturer to request the SDS or go to the seller's website to print a copy for use.

### Chemical Reagents

Reagents posing an inhalation hazard should be used in well-ventilated areas, under a fume hood, or in specified processing chambers. An organic vapor respirator is recommended to be used if the reagent is not able to be applied in one of the aforementioned areas. Caution should be exercised with certain reagents containing flammable

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 15 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

solvents and carriers. These reagents should be stored in air-tight containers within flame resistant cabinets when not in use and should not be exposed to heat sources. Unopened reagents of a corrosive nature should be stored in air-tight containers within corrosion resistant cabinets, and care should be taken to avoid contact between these reagents and exposed skin.

### Spill Control

If a chemical spill occurs, isolate the spill and secure the immediate area, notify the Safety Manager or supervisor then determine the source and type of spill and whether you can safely handle it. Laboratory work areas shall contain spill kits to aid in certain types of chemical spills. If the spill is small, determine the best technique for cleanup according to the type and size of spill. Use the following spill kits as required:

**Acid Spills** - The contaminated area should be isolated. For an *Acid* spill use Spill-X-A (Acid Neutralizer). Encircle the spill and cover with agent. Mix agent into spill. Clean up, label and dispose of properly.

**Solvent Spills** - The contaminated area should be isolated. For a *Solvent* spill use Spill-X-S (Solvent Absorbent). Encircle the spill and cover with agent. Mix agent into spill. Clean up, label and dispose of properly.

**Caustic Spill** - The contaminated area should be isolated. For a *Caustic* spill use Spill-X-C (Caustic Neutralizer). Encircle the spill and cover with agent. Mix agent into spill. Clean up, label, and dispose of properly.

**Infectious Blood and Body Fluids Spills** – The contaminated area should be isolated. A kit used to clean-up potentially infectious and harmful blood/body fluid spills will be used. The kits are located in the lab areas. Each kit is self-contained and carries the complete instructions on the packaging. Body fluids may also be cleaned up using a solution of 10% bleach.

A universal spill control kit is located in the processing room and may be used when a spill is not identifiable.

### Disposal of Chemicals

Chemical waste material shall be disposed of in accordance with good safety practices and applicable regulations of the Commonwealth of Massachusetts. Hazardous waste containers shall be labeled with the hazard such as Acid or Organic waste. Volatile chemicals shall be disposed of only under hoods or in well ventilated areas.

## 2.7 Crime Scene Safety

The safety and wellbeing of Criminalists at a crime scene is of the highest priority. The possibility of exposure to chemical, biological, and other environmental hazards is a real and ever-present concern. Hazardous objects or materials such as knives, firearms, drugs, and explosives may be encountered at a scene. Criminalists responding to scenes must be aware of the hazards which may be present and know how to protect themselves from such hazards. Personnel entering a crime scene should do so with proper safety and protective equipment to safeguard against biological and chemical hazards. Crime scene clothing is provided and may be worn to all scenes.

Criminalists will consult with the investigating officer(s) prior to entry to a location or the start of processing a vehicle to evaluate safety concerns that may affect all personnel entering the scene.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 16 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	



### 3. EVIDENCE

Reference the Forensic Division Evidence Manual.

#### 3.1 CASE FILE & BARCODES

Some cases require the creation of a physical case file which will retain minimal documentation. Documents are scanned and retained in the evidence tracking system and/or the SAN under the appropriate incident number. Documents bearing original notes, elimination prints, non-evidentiary CD's, and any additional documentation deemed appropriate by a member of the LPU should be contained within the case file. When new or additional work is completed in Mideo on pre-Mideo cases, a notation should be recorded onto the case file.

Operational areas of the unit, all LPU personnel as well as their inboxes will have an assigned location (unique ID) that can be scanned as a barcode. The inbox barcodes will be treated the same as the individual barcodes with the exception of evidence transfers to another unit. The individual barcodes shall be used for transfers to the other forensic units (Example: Evidentiary items will be transferred from the processing room to an individual when bringing the items to the CLU or FAU evidence window).

#### 3.2 CASE & EVIDENCE INFORMATION

##### Case Assignment

The LPU prioritizes the following case types: homicides, cases with pending court dates, cases with lifts submitted, firearm evidence, sexual assaults, assault & batteries, robberies (to include home invasions), and priority request cases. Cases that do not fall under the priority criteria are processed and/or compared in numerical order starting with the recent backlog cases and working backwards through the previous years. Assignments and priorities are subject to flexibility in order to address the needs of the unit under extenuating circumstances.

Any request for prioritization should be made on a LPU Priority Request Form. This form is located on the Boston Police Intranet Forms On-Line. This form should be submitted to and shall be signed by the Director/designee if approved. A copy of the Priority Request Form will be maintained in the case record. The assigned Criminalist is responsible for the case management, which includes case evaluation, communication with the customer and facilitation of requested analysis. When items are submitted with lifts, the items should be added to the processing queue of the Criminalist that completed the analysis of the lifts.

##### Off-Hours Comparison Requests

Off-hours (evenings, weekends, and holidays) comparison requests will only be made through the Forensic Division chain of command. The Director, Captain of the Forensic Division, Deputy of BIS, and/or Superintendent of BIS should be made aware of the request. A member of the command staff must authorize any off-hours requests for rushed/priority comparisons. If the on-call Criminalist receives a request for a comparison, they will notify the requesting individual that the request must be submitted through the Forensic Division chain of command.

##### Case Responsibility

If a Criminalist is unable to complete a "rush" case within the requested time frame, it is his/her responsibility to make arrangements to accommodate the case deadline to the extent possible. For example, the Criminalist may coordinate with the Customer to amend the case deadline or to determine the necessary extent of work. The Criminalist may seek out another qualified Criminalist to complete the work if required.

##### Case Information Dissemination

Case information should be kept confidential. It is understood that communication is a required element of establishing the forensic service to be performed by the LPU. When necessary, communication shall occur to clarify any requests for service, determine which items will be examined, and make clear the type of examinations to be

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 17 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

performed. To ensure that the work performed is that requested by the customer, communication must be direct and clear. When assigned a case, Criminalists will request/identify the name of the primary investigator and relay case information to that individual. The primary investigator can disseminate information to other interested individuals as necessary. Should multiple individuals wish to have input into the requests for service (example: names for comparison), this information should come through the primary investigator. Having a single point of contact ensures that information is relayed in a clear manner and reduces the potential for miscommunication. There may be times where names are obtained from an additional source: the primary investigator should be contacted regarding any additional names provided. All communication will be documented and maintained in the case record.

## **REQUESTS FOR EXAMINATION**

Communication between customers and the unit is essential for the efficient examination of physical evidence submitted to the LPU. The LPU may request the name and contact telephone number of the customer for the incident to facilitate the expeditious examination of submitted evidence and to facilitate communication. The customer or his/her representative may specify the examination(s) to be conducted on each item of evidence at the time of submission using the pre-log service request or when contacted by a member of the LPU. Methods of testing will ultimately be selected by LPU personnel.

Requests for examination are communicated to the assigned Criminalist in the LPU. Hand-written notes attached to evidence containers are not appropriate requests for examination. If a request for examination is unclear, the assigned Criminalist should contact the primary investigator(s) to establish a clear understanding of the request before proceeding. If a request for examination is received for a type of testing that is beyond the scope of those currently performed at the LPU, the assigned Criminalist will contact the primary investigator to discuss testing options and may refer the request to an outside agency or laboratory. Any unresolved issues should be brought to the attention of the Director/designee.

Case evidence submissions may require examination by more than one unit (Crime Lab or Firearms Analysis). The pre-log service request should outline the examination required per item. The Criminalist assigned to the case may determine that a transfer of the evidence to the proper Unit of the Forensic Division is required. If there is a request for DNA analysis, this evidence should be submitted to the Crime Laboratory Unit prior to the LPU (example: A water bottle from a B&E).

### **3.3 EVIDENCE EXAMINATION**

Specific protocols and additional information regarding the examination of evidence in the LPU can be found in the technical sections of this manual.

#### **Processing**

At the conclusion of processing, each item of evidence and/or its proximal container shall be marked at the minimum with the case number, item number, initials, and re-packaged date. During the course of evidence examination, if a derivative is made, refer to the Forensic Division Evidence Manual sections 8: Barcodes.

Camera cards (for overall and evidentiary photos) in process should be secured by each Criminalist to ensure the images are secured during the processing of evidentiary items. The downloading of these images should be completed following the completion of processing the case(s). In the event that downloading is not immediate, refer to the Forensic Division Evidence Manual section 15: Evidence Handling and Storage.

#### **Comparison**

Each CD and/or lift when examined/processed, will be initialed and dated by the Criminalist.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 18 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

## 4. PROCESSING

Latent prints can be found on all types of surfaces. The goal of latent print processing is to recover and preserve ridge detail that has the potential to be identified to a source. Criminalists may move through a sequence of processing techniques that maximizes the potential to obtain such ridge detail. This section is focused on the various techniques available in the unit to improve the likelihood of latent print recovery.

### 4.1 GUIDELINES FOR EXAMINATION AND GENERAL CONSIDERATIONS

Surfaces on which latent prints are deposited can generally be divided into two categories: porous and non-porous. This protocol lists **suggested** processes for porous and non-porous surfaces, as well as some unique surfaces and circumstances. To minimize the destruction of and to increase the possible enhancement of latent prints, examination of items may require a variety of processing stages ranging from visual inspection to sequential physical, chemical, or digital techniques. Factors that may influence the approach taken include the following:

- Type of surface
- Matrix
- Transfer medium
- Physical condition of the surface
- Environmental conditions
- Sequential environmental changes
- Evidence collection methods
- Packaging
- Elapsed time since contact
- Conflict in examinations required
- Destructive consequences of technique
- Additional techniques available

When a latent print is developed and may be suitable for capture, it is left to the discretion of the Criminalist to determine if the latent print should be preserved by photography prior to treatment of the latent print through additional steps.

#### Chemical Reagents and Quality Control

Processing reagents can be purchased ready for use in the LPU from a vendor. All reagents received will be entered into the LIMS for the purpose of printing a label.

**Reagents will be quality control tested when a new container is opened, at the first use of the day, and/or prior to use. Results of these tests (positive or negative) will be recorded on the Reagent QC Log. The desired quality control result is documented in the method for each reagent.**

**Cyanoacrylate fuming, iodine fuming, Wetwop and Vacuum Metal Deposition (VMD) are quality control tested at each time of use, with results pertaining specifically to the items tested. Therefore, visualization results are recorded in case notes only and no quality control results are recorded on the Reagent QC Log.**

Any reagents that produce expected results in a quality control test are suitable for use in casework. The quality control test results for any reagent used will be documented on the QC box on the first page of the Processing Package Contained Worksheet or in Mideo at the time of processing. If the quality check fails, the chemical will be disposed of promptly and properly.

#### Reagent Application Techniques

Many processing reagents can be applied using common techniques depending on surface type, size of the area to be processed, and availability of the reagent. The following is a list of suggested chemical application techniques

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 19 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

that may be applied in casework. **All techniques should be applied in a well-ventilated area or under a fume hood.**

The following techniques may be applied multiple times as deemed necessary by the processing Criminalist.

**Spraying:**

A reagent is placed into a bottle with an attached spray nozzle. The item/surface is coated with an even covering of the reagent while avoiding over-saturation. The item/surface may be rinsed with water or a designated rinse solution, and/or allowed to air dry.

**Immersion:**

A reagent is poured into an appropriately sized tray or container, large enough to accommodate the size of the item to be processed. Using tongs or forceps, the item is immersed into the reagent until the surface is coated, for a period of time as deemed necessary by the Criminalist, then removed. The item may be rinsed with water or a designated rinse solution, and/or allowed to air dry.

**Cascading:**

A reagent is placed into a wash bottle, pipette, or a container with a pour spout. The reagent is then gently poured over the item/surface, covering the area to be processed for a period of time as deemed necessary by the Criminalist. The item/surface may be rinsed with water or a designated rinse solution, and/or allowed to air dry.

**Pooling:**

If an item/surface is flat and/or concave, a reagent is poured onto/into the area to be processed and left in place for a period of time as deemed necessary by the Criminalist. The reagent is then poured off of the item/surface. The item/surface may be rinsed with water or a designated rinse solution, and/or allowed to air dry.

**Toweling:**

The item/surface is covered with a thin, non-textured, permeable paper towel or other suitable material. A reagent is then gently pooled, poured, or sprayed on the towel to cover the area to be processed. The towel is then left in contact with the item/surface for a period of time as deemed necessary by the Criminalist. Care is taken to avoid air pockets or bubbles underneath the towel/material, ensuring contact between the reagent and the item/surface. The towel/material is carefully removed from the item/surface, and the item/surface may be rinsed with water or a designated solution, and/or allowed to air dry.

**Brushing:**

A brush is dipped into a small quantity of reagent placed aside from the main container. The brush containing the reagent is then wiped across the area to be processed, allowing the reagent to coat the surface. The item/surface may be rinsed with water or a designated rinse solution, and/or allowed to air dry.

**Alternate Light Source (ALS)**

An alternate light source (ALS) is a device that allows its user to examine objects with various wavelengths of light. The detection of latent prints, semen, fibers, and other trace materials may be achieved due to their fluorescence or absorption (quenching) when illuminated with specific wavelengths of light. The fluorescence can be seen with the aid of special barrier filters.

Some latent prints may fluoresce simply by illumination with a specific wavelength of light. The fluorescence of latent prints without prior treatment is sometimes referred to as "inherent luminescence." Evidentiary items may be processed with a fluorescent substance such as a chemical dye stain or a fluorescent powder to detect latent prints with an ALS.

An ALS may also be used to detect trace materials such as fibers, semen, paint, etc. These materials do not require treatment with chemicals prior to an examination with an ALS, but are detected because of fluorescence caused by

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 20 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

illumination with certain wavelengths of light. The high intensity light emitted from the alternate light sources may be harmful to the eyes, and thus one should avoid looking directly at its source. Barrier filters or goggles should be used to shield the eyes.

An annual quality performance check of the ALS will be completed with known fingerprint samples and recorded in the equipment database.

## **Non-Latent Print Evidence**

### ***General evidence examinations***

Processing Criminalists may encounter various types of non-latent print evidence when examining items or surfaces. It is the responsibility of the processing Criminalist to determine whether any requests exist concerning biological evidence. The Criminalist should consult with Crime Laboratory staff to determine the best possible sequence for detection and collection of these materials, unless the Crime Laboratory Criminalist has communicated that their examination of the item has been completed. Decisions should be made with the circumstances of the case and the evidentiary material in mind. Sequence of collection or documentation may vary depending on these factors. If after consultation with the customer and/or the Crime Laboratory any questions exist as to whether or not samples are necessary, caution should be exercised, and samples should be preserved by Criminalists.

If necessary, authorized Criminalists may swab evidentiary items prior to processing using the following technique:

- With gloved hands, moisten 1 to 2 sterile swabs with water, depending on the size of the area/stain. If the stain is wet, it may not be necessary to moisten the swab(s).
- Swab the area/stain, transferring as much of the suspected material on the swab(s) as possible.
- Package the swab(s) back into its original packaging or equivalent.
- Place the packaged swab(s) inside of a labeled evidence envelope.

### ***Non-ridge detail impressions***

Non-ridge detail impressions may be encountered when processing items.

When observing a footwear/tool mark impression, the Crime Lab will be called and will be responsible for collection if needed. Any other non-ridge detail impression may be documented and/or photographed. Images captured will be saved on a CD, an item created in the evidence tracking systems, and the CD transferred to the Photo Unit.

## **4.2 POROUS EVIDENCE**

A porous item consists of a material that allows the passage of liquids and gases through itself with retention quantities varying from slight to great. Examples: paper, cardboard, unfinished wood.

### **General Considerations**

**Indented writing** - If the detection of indented writing is required on a document, it must be performed **prior to** processing for latent prints. Treating a document with chemicals will usually prevent the detection of indented writing.

**Handwriting/Typed Documents** - Documents requiring additional forensic analysis **must** be photographed with a scale on a high-resolution camera for documentation prior to processing. The customer has the discretion to send the evidence elsewhere to have the additional forensic analysis performed.

**Contamination** - To prevent the introduction of additional latent prints by the Criminalist, gloves shall be used when handling evidence items. If necessary, forceps should be used in addition to gloves.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 21 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

**Caution:** Prints placed on a document, after it has been previously treated for latent prints, may also develop.

### Sequence of Examination

The following is the recommended sequence of examination and is in no way prescriptive as the sequence in which all items of evidence will be processed. The sequence of processes will be performed at the discretion of a Criminalist.

- Visual Examination
- Inherent Fluorescence/Alternate Light Source
- Iodine Fuming (*\*may be used when no other processing technique is appropriate due to the surface*)
- DFO
- Alternate Light Source
- Ninhydrin **OR** 1,2-Indanedione
- Alternate Light Source
- Vacuum Metal Deposition can occur before, during, or after this sequence

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 22 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

**Iodine Fuming - Chemical**

Caution: very hazardous in cases of skin/eye contact (irritant), ingestion, and inhalation

**Description**

Iodine is a sensitive indicator of various fatty oils, which are often present in latent print residue. Iodine is typically not destructive and may detect deposits with insufficient amino acids for effective Ninhydrin reaction. Iodine is highly toxic and very corrosive to nearly all metals. It can be used to process nearly all types of surfaces but is typically used with porous surfaces.

**Reagent**

Iodine crystals (Iodette ampoules)  
Fumette Disposable Iodine Fuming Gun/Silver Plates  
Search Iodine Print Enhancer

**Method****Control Print**

A test print of known origin should be processed at the time of use to ensure the desired reaction is being obtained. Ridge detail should appear brown in color, as seen here:

**Application**

Fuming of evidence should be carried out in well ventilated areas or in fume hoods, within cabinets or containers that allow adequate space for evidentiary items.

**Iodine crystals (Iodette ampoules):**

Small items can be fumed in a heat sealed or zip lock bag. A small amount of Iodine crystals is poured into the bag. The evidence is inserted, and the bag is sealed.

Larger items can be placed into an airtight cabinet with a heat source. A small tray of Iodine crystals is added to the heat source inside the cabinet, and the resulting Iodine fumes are allowed to coat the item.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 23 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	



#### **Fumette Disposable Iodine Fuming Gun/Silver Plates:**

Large or immobile items can be processed with direct iodine vapors from a disposable iodine gun fuming applicator. The fuming applicator is used to apply vapors through a tube onto the surface to be examined through forced air.

The fuming gun is grasped in the palm of the hand, covering the area where the crystals are located for at least one minute. Body heat will accelerate sublimation of the crystals. When the crystals have warmed slightly, the enclosed glass ampoule is crushed, and the nozzle of the tube aimed at the surface to be processed. An air pump or a Criminalist's breath is then used to force air through the fuming gun, directing the resulting fumes to the surface of the item. Care is taken to NOT INHALE through the blowing tube.

Because the residue is exposed to the vapors for a brief duration, any iodine absorbed is released quickly demanding prompt documentation (photography of resulting ridge detail).

If needed, especially in the case of human skin, iodine-enhanced ridge detail can be transferred to silver plates using the following method:

- A portion of the skin is fumed with iodine vapors
- The silver plate is pressed directly onto the processed area
- The silver plate is removed and exposed to a strong light source
- Any developed latent prints are photographed

#### Visualization

The latent prints will appear brown in color.

Impressions may be fixed onto the surface by adding a small amount of Search Iodine Print Enhancer. One glass ampoule is broken inside the tube and the liquid dabbed onto any developed impressions. The impressions will turn a blue/purple color, allowing for greater contrast. **Please note that the fixer should not be used on receipts/thermal paper.**

On porous surfaces, other porous processing techniques may be used after iodine fuming.

#### **Storage/Disposal**

Iodine is stored in a sealed container.

Excess iodine can be reused or allowed to vaporize in the hood or well-ventilated area.

Used fuming applicators are placed in a heat seal plastic bag, and devices used as chambers can be disposed of in the trash.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 24 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	



**DFO (1,8-Diazafluoren-9-One) - Chemical**

Caution: highly flammable

**Description**

DFO is a synthetic analogue of Ninhydrin used in developing latent prints on porous items. DFO reacts with the amino acids in latent print residue and produces a fluorescent reaction that can be visualized using an alternate light source. On some specimens, Ninhydrin or 1,2-Indanedione will develop latent prints that DFO fails to develop. Therefore, in most instances, Ninhydrin or 1,2-Indanedione should also be used.

Because the DFO reaction with latent prints may be inhibited by Ninhydrin processing, DFO processing should be performed **prior** to Ninhydrin processing.

If there is a concern that treating a document with the DFO solution may cause ink or printed material to run, the document should be tested in a small area or on a sample of a similar substrate and ink before treating the entire document.

**Reagent**

DFO is available in a pre-mixed form.

**Method****Control Print**

A test print of known origin should be processed at the first use of the day to ensure the desired reaction is being obtained. Ridge detail should be visible under the ALS under various wavelengths with orange or red barrier filters, as seen here:

**Application**

DFO can be applied to an item or surface using the immersion, spraying, or brushing methods (see reagent application techniques for a description of these methods).

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 25 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

Items are then allowed to dry completely and are placed into a development chamber at the following settings:

Temperature	Humidity	Time
100°C	0%	20 minutes

An iron without steam may also be used, or the item can be left out overnight at room temperature. If an iron is utilized, an indication in the case notes will be made.

#### Visualization

The item is examined with an ALS under various wavelengths in the 495-550nm range with orange or red barrier filters. Photographs of ridge detail must be taken with the appropriate barrier filter.

#### **Storage/Disposal**

DFO pre-mixed solution can be stored at room temperature in an airtight container in a flammables cabinet for approximately six months, or until a quality control test no longer yields the expected results.

Excess solution is disposed of in a dedicated container for DFO/Ninhydrin in a fume hood.

**1,2-Indanedione - Chemical****Description**

1,2-Indanedione is a synthetic analogue of Ninhydrin used in developing latent prints on porous items. 1,2-Indanedione reacts with the amino acids in the print residue and produces a fluorescent reaction that can be visualized using an alternate light source. Because the 1,2-Indanedione reaction with latent prints may be inhibited by Ninhydrin processing, 1,2-Indanedione processing should be performed in place of Ninhydrin processing.

1,2-Indanedione is **not** known to cause ink and print to run.

**Reagent**

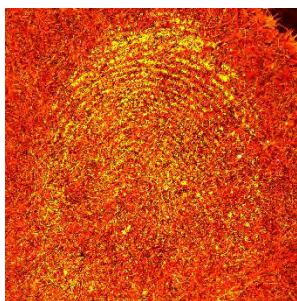
1,2-Indanedione is available in a kit form. Mixing instructions are as follows:

“Part A” liquid is added to “Part B” powder and shaken thoroughly to dissolve crystals.

The mixture of “Part A” and “Part B” is added into “Part C” bottle and shaken thoroughly, with care taken to avoid transferring any undissolved crystals into “Part C” bottle.

**Method****Control Print**

A test print of known origin should be processed at the first use of the day to ensure the desired reaction is being obtained. Ridge detail should be visible under the ALS under various wavelengths with orange or red barrier filters, as seen here:

**Application**

1,2-Indanedione can be applied to an item or surface using the spraying or brushing methods (see reagent application techniques for a description of these methods).

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 27 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

Items are then allowed to dry completely and are placed into a development chamber at the following settings:

Temperature	Humidity	Time
100°C	60%	20 minutes

An iron with steam may also be used, or the item can be left out overnight at room temperature. If an iron is utilized, an indication in the case notes will be made.

#### Visualization

The item is examined with an ALS under various wavelengths in the 495-550nm range with orange or red barrier filters. Photographs of ridge detail must be taken with the appropriate barrier filter.

#### **Storage/Disposal**

1,2-Indanedione kits can be stored at room temperature in an airtight container. 1,2-Indanedione kits have an indefinite shelf life.

Mixed 1,2-Indanedione solutions can be stored at room temperature in an airtight container for up to two weeks or until a quality control test no longer yields the expected results.

Excess solution can be disposed of down the drain with water.

**Ninhydrin/Ninhydrin HT (1,2,3-triketohydrindene hydrate) - Chemical****Description**

Ninhydrin is a general-purpose fingerprint reagent for paper and many porous and semi-porous surfaces. Ninhydrin or triketohydrindene hydrate is an extremely sensitive indicator of amino acids and other components in fingerprints. The reaction produces a violet to blue-violet color known as 'Ruhemann's Purple'. This technique is effective with long duration deposits and minute amounts of amino acids.

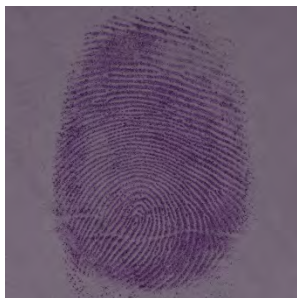
The Ninhydrin HT description is the same as the reagent noted above, with the advantage of being used for the processing of thermal paper.

**Reagent**

Ninhydrin/NinhydrinHT are available in pre-mixed form.

**Method****Control Print**

A test print of known origin should be processed at the first use of the day to ensure the desired reaction is being obtained. Ridge detail should appear purple in color after allowing to dry completely, as seen here:

**Application**

Ninhydrin/Ninhydrin HT can be applied to an item or surface using the spraying, immersion, or brushing methods (see reagent application techniques for a description of these methods).

Items are then allowed to dry completely and are placed into a development chamber at the following settings:

Temperature	Humidity	Time
80°C	65%	5 minutes

An iron with steam may also be used, or the item can be left out overnight at room temperature. If an iron is utilized, an indication in the case notes will be made.

Retreatment of faint or fragmentary impressions may intensify the reaction, provided no background discoloration is observed.

#### Visualization

The Ruhemann's Purple reaction does not require an ALS for visualization.

Ninhydrin coloration is not permanent, and while some impressions have remained visible for years, others have faded in a matter of days. Photographic preservation is essential and should be accomplished as soon as possible.

#### **Storage/Disposal**

Ninhydrin solutions can be stored at room temperature in an airtight container for up to one year or until a quality control test no longer yields the expected results.

Excess solution is discarded in a dedicated container for DFO/Ninhydrin located in the fume hood.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 30 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

#### 4.3 NON-POROUS EVIDENCE

Non-porous surfaces repel or tend to repel liquids and gases while not permitting saturation or passage of liquids or gases through. Examples: glass, metal, plastic, finished wood

##### General Considerations

##### Firearms and Firearm related evidence

Cartridge cases will not be processed for latent prints unless specific information is provided to indicate contact with the cartridge case after it was fired and expelled by the firearm, and approval of the Director or designee is obtained. In homicide cases, when the cartridge case is the only evidentiary item, processing may be completed with the approval of the Director or designee.

Any items determined by a Criminalist to be too small to yield ridge detail suitable for capture (example: BBs, springs) will be considered not conducive to the recovery of latent prints and may not be processed.

##### Items requiring physical match examination

If there is a request for an examination for a physical match between two items and/or an item and its possible source, the physical match examination should be conducted prior to examination of the item for latent prints. Crime Laboratory Criminalists and the customer should be consulted in order to determine the best sequence for examination.

##### Contamination

To prevent the introduction of additional latent prints by the Criminalist, gloves shall be used when handling evidence items.

##### Sequence of Examination

The following is the recommended sequence of examination and is in no way prescriptive as the sequence in which all items of evidence will be processed. The processing of items will be performed at the discretion of a Criminalist.

- Visual Examination
- Inherent Fluorescence/Alternate Light Source
- Cyanoacrylate Fuming
- Chemical Dyes
- Alternate Light Source
- Powder(s)
- Alternate Light Source
- Vacuum Metal Deposition can occur before, during, or after this sequence

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 31 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

**Cyanoacrylate (Super Glue) and PolyCyano UV Fuming - Chemical**

Caution: heating above 400°F/ 204°C  
(Cyanoacrylate) or 446°F/ 230°C  
(PolyCyano UV) produces a toxic gas

**Description**

Cyanoacrylate fuming is a method for developing friction ridge impressions on non-porous materials, such as plastic, glass and metal, and on semi-porous materials, such as leather and vinyl. Cyanoacrylate vapor is thought to polymerize due to a reaction with water and possibly other latent print constituents to form a white deposit. Treatment with dye stains or powders may enhance latent prints developed by the cyanoacrylate.

PolyCyano UV is a one-stage cyanoacrylate fuming and dye staining reagent for developing friction ridge impressions on non-porous materials. PolyCyano UV is a powder containing a mixture of 95% polymerized ethyl cyanoacrylate, approximately 5% dimethylamino benzaldehyde (DMAB), a fluorescent staining dye, and trace additives (< 1%). When stimulated with ultraviolet light (UV), the fluorescent response from DMAB is in the blue region of the electromagnetic spectrum.

**Reagent**

Cyanoacrylate and PolyCyano UV are available in commercial form.

**Method****Chamber/Device Selection**

The Unit is equipped with multiple chambers (MVC-3000/D and MVC-1000 models) for routine superglue fuming of evidentiary items.

MVC-5000/D may be used for larger items that do not fit into the above listed chambers. The MVC-5000/D is located in the Crime Scene Response Unit.

The MVC-Lite is a portable mini chamber that can be used in the lab for small items and/or at crime scene locations. All MVC chambers have an automatic and manual mode of processing.

A portable cyanoacrylate device can be used as an alternative to the MVC units. A portable device is typically used to superglue fume evidentiary items at crime scenes prior to transport but can also be used in a well-ventilated location in the laboratory to target specific or hard to reach areas of items requiring cyanoacrylate fuming.

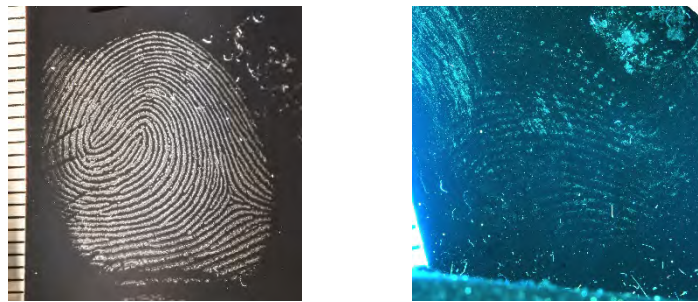
**Control Print**

A control print can be a print placed on a suitable surface and processed simultaneously with evidentiary items. The control print is used to ensure that the fuming process is working properly. The control print is placed in a visible location in order to monitor development. Ridge detail should appear white in color as seen here (left image).

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 32 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	



When using PolyCyano UV, the ridge detail should be observed under oblique light, UV light, or an ALS, as seen here (right image):



### Application

Automatic Chamber Processing is recommended. All MVC chambers are preset for an automatic cycle. See the user manual instructions found in the LPU and on the server.

Glue time and temperature settings should be checked each time before starting the automatic cycle.

The recommended quantity for cyanoacrylate and polycyano in the chambers is dependent on the size of the chamber, number of items to be processed, type/size of items, and whether they have been previously superglue fumed. Recommendations listed below are guidelines only for the processing of one item and not all encompassing, exceptions may exist based on the item.

Cyanoacrylate: about 1 drop in the MVC1000 and about 2 drops (dime size) in the MVC3000.

PolyCyano: about ¼ scoop of powder in the MVC1000 and up to ½ scoop in the MVC3000.

### Visualization

Items and the control print are periodically checked for development. Latent print development may take from several minutes to hours depending on the materials being processed and the size of the fuming chamber.

Fuming should be stopped before the items become coated with a heavy white film, otherwise any latent prints may be over developed. The process is completed when prints are visible, or a faint white coating develops on the evidence.

It may be necessary to allow the cyanoacrylate to set for a period of time before handling the processed items.

Items are examined for ridge detail and any prints that are suitable for capture are photographed.

For automatic/manual chamber PolyCyano UV processing, items can be examined for ridge detail with white light, ALS (350 nm), and/or UV light. Using the ALS or the UV Crime-Lite, items can be examined without a filter, or with a yellow or orange filter. Any prints that are suitable for capture are photographed.

Additional dye stain processing (Ardrox, RH6G, etc.) can be followed after PolyCyano UV processing.

### **Storage/Disposal**

The working cyanoacrylate can be stored in a plastic container at room temperature or between 32°F/0°C and 37°F/5°C.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 33 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

Cyanoacrylate can be used until it solidifies. There is no special disposal procedure for cyanoacrylate.

PolyCyano UV powder has a shelf life of 6 months stored at room temperature and 12 months stored between 32°F/0°C and 37°F/5°C. PolyCyano can be used past the shelf life until a quality control test no longer yields the expected results.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 34 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

**Rhodamine 6G (RH6G) - Chemical****Description**

Staining with Rhodamine 6G fluorescent dye can enhance and improve the quality of cyanoacrylate developed prints. The dye is absorbed by the cyanoacrylate and can be visualized with an ALS due to fluorescence.

**Reagent**

Rhodamine 6G is available in a pre-mixed solution (methanol or aqueous carriers). Varnished surfaces tend to be destroyed by some carriers; thus a water carrier is a better alternative.

**Method****Control Print**

A test print is processed at the first use of the day to ensure that the desired reaction is being obtained. Ridge detail should be visible under the ALS at various wavelengths with orange or red barrier filters, as seen here:

**Application**

Items are processed in a fume hood or well-ventilated area.

Rhodamine 6G can be applied to an item or surface using the spraying, immersion, toweling, cascading, pooling, or brushing methods (see reagent application techniques for a description of these methods). The item is immediately rinsed after application with the appropriate solvent or water and allowed to dry.

**Visualization**

The item is examined with an ALS under various wavelengths in the 495-540nm range while viewing with an orange or red barrier filter. Any prints that are suitable for capture are photographed and/or lifted with black gel lifts.

**Storage/Disposal**

Rhodamine 6G is stored in an airtight container at room temperature. The working solution has an indefinite shelf life. Residual Rhodamine 6G may be allowed to evaporate in the hood or disposed of down the drain with excess water.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 35 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

**Ardrox - Chemical**

Caution: highly flammable

**Description**

Staining with Ardrox fluorescent dye can enhance and improve the quality of cyanoacrylate developed prints. The dye is absorbed by the cyanoacrylate and can be visualized with an ALS due to fluorescence.

**Reagent**

Ardrox is available in a pre-mixed solution.

**Method****Control Print**

A test print is processed at the first use of the day to ensure that the desired reaction is being obtained. Ridge detail should be visible under the ALS at various wavelengths with a yellow barrier filter, as seen here:

**Application**

Items are processed in a fume hood or well-ventilated area.

Ardrox can be applied to an item or surface using the spraying, immersion, toweling, cascading, pooling, or brushing methods (see reagent application techniques for a description of these methods). The item is immediately rinsed after application with the appropriate solvent or water and allowed to dry.

**Visualization**

The item is examined with an ALS under various wavelengths in the 350-480nm range while viewing with a yellow barrier filter. Any prints that are suitable for capture are photographed and/or lifted with black gel lifts.

**Storage/Disposal**

Ardrox is stored in an airtight container at room temperature. The working solution has an indefinite shelf life.

Residual Ardrox may be allowed to evaporate in the hood or disposed of down the drain with excess water.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 36 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

**Small Particle Reagent (SPR) - Chemical****Description**

Small particle reagent (SPR) is a suspension of fine molybdenum disulphide particles. It adheres to the fatty constituents of latent prints to form a white or black deposit. Although the process is sensitive, it is much more effective on fresh fingerprints than older ones. SPR spray application is suitable for all non-porous surfaces but is recommended for those that are wet and/or oily/greasy.

SPR may also be used on non-porous surfaces such as polystyrene foam, ceiling tiles, and packaging foam.

**Reagent**

SPR is available in a pre-mixed form (white or black).

**Method****Control Print**

A test print is processed at the first use of the day to ensure that the desired reaction is being obtained. SPR is available in white or black. Ridge detail should appear to be white or black in color depending on the choice of the SPR. White can be seen here:

**Application**

Items are processed in a fume hood or well-ventilated area.

SPR should be well-agitated before use and can be applied to an item or surface using the spraying, immersion, cascading, or pooling methods (see reagent application techniques for a description of these methods).

The item or surface may be rinsed immediately with water and is then allowed to dry. A light to moderate flow of rinse water will not dislodge the SPR particles.

For outdoor application to very large items, such as a wet automobile, a dispenser spray head can be used.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 37 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

Visualization

The item or surface is examined for ridge detail under normal lighting conditions and any prints that are suitable for capture are photographed.

Once satisfactory photographs have been obtained, the prints may be lifted if desired. If necessary, the impressions can be lifted while the surface is still wet. However, it is easier if the surface can be allowed to dry.

**Storage/Disposal**

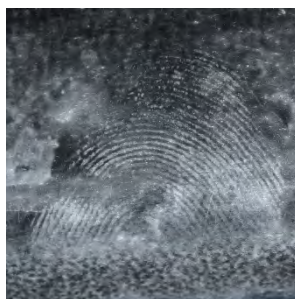
Small Particle Reagent can be stored at room temperature in an air-tight container indefinitely or until a quality control test no longer yields the expected results.

Excess solution can be disposed of down the drain with excess water.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 38 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

**Fingerprint Powders - Physical****Description**

Dusting with fingerprint powder is a common method employed to develop latent prints on non-porous materials. Powders develop latent prints by adhering to moisture or substances such as grease and oil, which are common constituents of latent prints.

**Types of Powders****Non-magnetic Powders**

The most common types of powder used in the development of latent prints are black (left image) and white (right image) non-magnetic powders. The color of the powder is chosen based on its contrast with the surface to be processed.

Black and white powders are preferred for routine use, and it is recommended that colored powders be used only when necessary.

**Magnetic Powders**

Magnetic powders are similar in appearance to non-magnetic powders except that they are composed mainly of iron filaments and are applied with a magnetic applicator. These powders should not be used on metallic or magnetic surfaces, or electronic devices.

**Fluorescent Powders**

Fluorescent powders may be useful on multi-colored materials when viewed with an ALS. A feather brush with a minimal amount of fluorescent powder typically provides optimal results. Fluorescent powders are not recommended for routine use.

**Application****Sequence of Processing**

Powders should be used as a singular process, or as the last process in a sequence of processing.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 39 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

If it has been determined that other latent print development methods are necessary, those methods should be applied prior to the application of powder.

### Dusting

Fingerprint powders are applied manually using either a conventional type brush such as a fiberglass brush or a magnetic applicator for magnetic powders. Cotton batting can be used for large areas requiring processing.

The surface to be processed should be dry before applying powder.

The powder should be applied carefully using small amounts and applying additional powder as needed. Care should also be taken not to use the brush too vigorously.

Visible prints (patent prints) may need to be photographed before dusting.

## **Collection and Preservation**

### Photographing Developed Prints

If it is uncertain that a developed latent print can be sufficiently lifted, it should be photographed to show its location on an item's surface, and an examination quality photograph should be captured of each latent before lifting is attempted.

### Collecting Developed Prints

Latent prints developed with powder may be lifted with three general types of fingerprint lifters: hinge lifts, gel lifts, and casting lifts.

Latent prints collected with hinge lifts may be placed onto a card for collection. Latent print lift cards should be used whenever possible, but other suitable surfaces such as a blank piece of paper may be used to collect a lift if necessary, or the lifts can be folded onto themselves. Hinge lifts are recommended for use on smooth, flat surfaces such as mirrors and windowpanes.

Gel lifts are recommended for use on slightly textured surfaces such as car dashboards and painted windowsills. Powder is lifted with the adhesive gelatin surface and protected with the included clear acetate sheet. Case information can be recorded on the back of the lift.

For highly textured or curved surfaces such as golf balls and door handles, casting lifts are recommended. For submittal, a latent print lift card containing case information can be attached to the lift as it dries or submitted alongside the lift.

### Marking Latent Lifts

Pertinent case information will be documented when lifts are made. This may include the incident number, lab case number, description of the surface from which the lift was taken, and the date and initials of the Criminalist collecting the lift(s).

When applicable, an indication of the orientation of the lift is marked on the lift card (example: an arrow showing the "up" direction).

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 40 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	



#### 4.4 Vacuum Metal Deposition Chamber - Physical



Caution: Refer to the West Technology VMD560 User Guide for detailed safety precautions.

#### **Description**

The vacuum metal deposition (VMD) chamber is a self-contained system that utilizes advanced vacuum technology to develop latent prints on non-porous surfaces (such as plastic and glass), porous surfaces (such as papers and magazines), and semi-porous surfaces (such as leather and vinyl). The VMD chamber deposits thin layers of metal onto surface imperfections to visualize impressions.

#### **Types of Metals**

Gold (Au) – 1 piece required for a standard process.

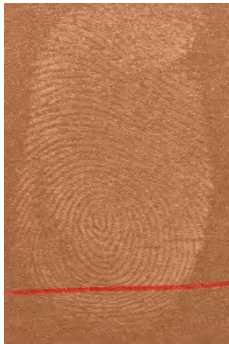
Zinc (Zn) – 1 pellet typically lasts 5-20 process runs, depending on the substrate.

Silver (Ag)/Sterling Silver (S. Ag) – 2-3 pieces of wire to start a process, adding more silver/sterling silver as/when needed.

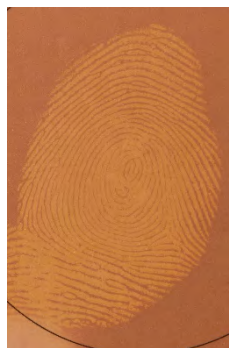
#### **Method**

##### Control Print

A control print can be placed on a suitable surface and processed simultaneously with evidentiary items. The control print is used to ensure that the vacuum process is working properly. The control print is placed in a visible location in order to monitor development. Ridge detail should appear as seen below:



Gold/Zinc



Silver



Silver/Zinc

##### Chamber Operation/Metal Selection

The Gold/Zinc process develops prints for many substrates and is the primary process that may be used; however, certain substrates may yield better results with a different metal process. Silver/Sterling Silver may produce better results on surfaces such as glossy clear plastics and flexible food packaging. Zinc may also be used alone to improve contrast after a primary metal process.

The following steps are taken in the use of the VMD:

1. The item and control print are placed on or suspended from the magnetic retractable tray, secured with the available magnets.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 41 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

2. The boats are checked for cracks. If damaged, the affected boat will be replaced (refer to User's Guide). If undamaged, the metal is placed in the appropriate boat. The amount of metal required to develop impressions varies from item to item. The front series of three boats are the same setup and design as the rear series of three boats. The front three boats will process items located in the front half of the chamber and the rear three boats will process items located in the rear half of the chamber.

3. The chamber is pumped to the correct pressure. Once this is completed, the display will automatically change to the SOURCES screen.

Pressure range for Source 1 is lower than  $3.0 \times 10^{-4}$  mbar.

Pressure range for Source 2 is between  $3.0$  to  $5.0 \times 10^{-4}$  mbar.

Pressure range for Source 3 is lower than  $3.0 \times 10^{-4}$  mbar.

4. The source in use is selected by the user. The selected boat on the display will be highlighted red to show it is ready for evaporation of the source metal.

5. The development control dial is used to increase the evaporation current. The boat(s) should start to glow, and the metal will heat up and start to melt. Observation can be made through the tinted portion of the viewing window. When the metal starts to evaporate, the development control dial will be adjusted according to the metal used:

Gold (Au) – (placed in the 1<sup>st</sup> and/or 4<sup>th</sup> boats) the development control dial is slowly adjusted until the piece of gold wire completely evaporates; once evaporated, the development control dial is turned as far to the right as possible (maximum level) for between 3-5 seconds, ensuring complete evaporation of all gold; the development control dial is then returned to the starting position (all the way to the left). Ridge detail will **not** be observed; this process needs to be followed with the zinc process.

Zinc (Zn) – (placed in the 2<sup>nd</sup> and/or 5<sup>th</sup> boats) the development control dial is slowly adjusted until the piece of zinc is "seated" in the boat (previously used pieces of zinc will have already been "seated"); the development control dial is adjusted until visible deposition is observed on the QC/evidence (a brief orange glow of the zinc may also be observed), and then the development control dial is immediately returned to the starting position and the zinc boat on the sources screen is deselected; on the selection screen, the "cleaning" option is chosen and the gold boat is heated to maximum for 3-5 seconds.

Silver (Ag)/Sterling Silver (S. Ag) – (placed in the 3<sup>rd</sup> and/or 6<sup>th</sup> boats) the development control dial is slowly adjusted until the piece(s) of silver form a cohesive liquid; the development control dial is adjusted until visible deposition is observed on the QC/evidence, and monitored until desired deposition is reached (evidence tray will have a color change from yellow to purple); the development control dial is then returned to the starting position and the silver boat on the sources screen is deselected.

6. If completing a two-step metal process, steps 4 and 5 are repeated to the desired enhancement.

7. The chamber is returned to atmospheric pressure and the item can be removed and examined.

Reference to the West Technology VMD560 User's Guide and Application Guide should be made if any problems are encountered or questions raised for specific metals and/or items.

Periodic cleaning of the evidence tray is required after every 3 to 5 runs, regardless of which metal deposition process is utilized. Additional cleaning of the chamber and chamber door may be necessary following the use of silver/sterling silver, followed by reapplication of vacuum grease to interior (viewing port, door seal, and LED light strips). Chamber oil may periodically need to be changed and cleaned. Only a specific vacuum pump oil will be used (Adixen by Pfeiffer vacuum oil).

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 42 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

The chamber is always placed into the vacuumed/pressurized state when not in use and prior to placing in standby mode.

#### Visualization

Items and the control print are periodically checked for development.

Items can be examined for ridge detail with light and/or an ALS. Any prints that are suitable for capture are photographed.

Latent prints developed with gold/zinc and silver/zinc are stable but single metal processed latent prints tend to be unstable and can deteriorate within 24 hours. It is recommended that latent prints developed using a single metal process are photographed right away.

Additional processing techniques can be utilized before and/or after the use of the VMD.

#### **Storage/Disposal**

The metals are stored in marked plastic containers at room temperature.

There are no special disposal procedures for the metals.

The metals have no expiration date and can be used as long as the quality control test yields the expected results.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 43 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

#### **4.5 BLOOD-STAINED SURFACES**

Occasionally, blood-stained items or items suspected of having traces of blood are submitted to the unit for latent print processing. Before processing, documentation of the appearance of the item and preservation of biological evidence for serological/DNA analysis should be considered.

##### **General Considerations**

##### **Documentation**

Documentation of reddish-brown stains may include photographs of stains with a scale and their relative position on the item/surface. A sketch of the item showing the location of the stain may also be included.

##### **Fixing Bloodstains for Processing**

Since blood is water soluble, use of a fixative is needed to “fix” the impression to the underlying substrate prior to application of any enhancement reagent. 5-Sulfosalicylic Acid (SSA) is the recommended fixing agent. Although some of the blood enhancement reagents used within the LPU contain SSA, it is still recommended to pre-fix a print in blood with SSA before treatment with any enhancement reagent. This is particularly important with prints in a lot of blood.

##### **Sequence of Examination**

The following is the recommended sequence of examination and is in no way prescriptive as the sequence in which all items of evidence will be processed. Processing techniques available and the order of their use may vary on a case-by-case basis. The processing of items will be performed at the discretion of the LPU Criminalist.

##### **Porous Items/Surfaces:**

- Visual Examination
- Inherent Fluorescence/Alternate Light Source
- Ninhydrin/1,2-Indanedione/DFO
- Alternate Light Source

##### **Non-Porous Items/Surfaces:**

- Visual Examination
- Inherent Fluorescence/Alternate Light Source
- Cyanoacrylate Fuming
- SSA
- LCV/Acid Yellow 7/Fuchsin Acid (Hungarian Red)
- Alternate Light Source
- Amido Black
- Rhodamine 6G/Ardrox
- Alternate Light Source
- Powder(s)

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 44 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

**5-Sulfosalicylic Acid – SSA - Chemical****Description**

Chemical fixing is a treatment to ensure that impressions in blood are not dissolved or washed away during the enhancement process. Impressions in blood are naturally fixed through aging, but that process can be accelerated with chemical treatment. Impressions in blood must be fixed to the substrate prior to any chemical enhancement. Fresh impressions in blood can be damaged or destroyed if not fixed.

**Reagent**

5-Sulfosalicylic Acid is available in a pre-mixed form.

**Method****Control Print**

A test print is processed at the first use of the day to ensure that the desired reaction is being obtained. The result of this test is reflected in the QC Log alongside the chosen enhancement reagent. SSA is quality checked when the impression in blood does not dissolve or wash away when the enhancement reagent is applied.

**Application**

Items are processed in a fume hood or well-ventilated area.

Application can be performed by immersing, cascading, spraying, pooling, or toweling (see reagent application techniques for a description of these methods).

Areas with suspected blood stains should be continually exposed to SSA for a minimum of 5 minutes. Excess SSA can be rinsed from the surface with water if desired.

The surface may be allowed to dry or may be blotted dry with a non-textured paper towel.

**Storage/Disposal**

SSA can be stored in an airtight container at room temperature.

The working solution has an indefinite shelf life.

Excess solution can be disposed of down the drain with excess water.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 45 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

**Fuchsin Acid (Hungarian Red) - Chemical****Description**

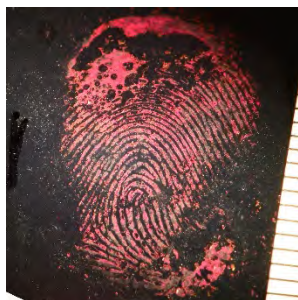
Fuchsin Acid is a water-soluble dye that reacts with the proteins in blood to form a deep magenta colored product. It can be further enhanced with the use of an alternate light source, which may prove to be useful on backgrounds that are dark or multi-colored. It can work well even if the item has been treated with cyanoacrylate fuming or LCV. Impressions on non-porous surfaces may be stained and then transferred with a white gelatin lift and then further enhanced with photography in the blue/green light range with the corresponding barrier filter. Bloodstains should be fixed prior to development.

**Reagent**

Fuchsin Acid is available in a pre-mixed form.

**Method****Control Print**

A test print is processed at the first use of the day to ensure that the desired reaction is being obtained. Ridge detail should appear to be magenta in color and may be visible under the ALS under various wavelengths with orange or red barrier filters, as seen here:

**Application**

Items are processed in a fume hood or well-ventilated area.

Blood impressions are fixed onto the evidence surface with 5-Sulfosalicylic acid fixer solution.

A small area of the object or surface being processed can be tested with the reagent to check for excessive background staining. If significant background staining occurs, a different enhancement reagent can be selected.

Application can be performed by the spraying, immersing, toweling, cascading, and pooling methods (see reagent application techniques for a description of these methods). The reagent should be left in contact with the impression for approximately 3 to 5 minutes.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 46 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

Excess reagent is rinsed from the item or surface by immersing or rinsing with tap water and the surface is allowed to dry.

If lifting is necessary, a white gel lifter is placed onto the impression and should remain on the area for 15 to 30 minutes.

#### Visualization

The item/surface is examined for ridge detail with white light, an ultraviolet light, or an ALS under various wavelengths (495-515nm) while viewing with an orange or red barrier filter.

Any prints that are suitable for capture are photographed.

The gel lifter should be photographed within 30 minutes, since the lifted impression will diffuse into the gelatin.

#### **Storage/Disposal**

Fuchsin Acid can be stored in an airtight container indefinitely.

Excess Fuchsin Acid solution can be disposed of down the drain with excess water.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 47 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	



**Amido Black (Aqueous Base) - Chemical****Description**

Amido Black is a protein stain particularly sensitive to those proteins present in blood. Amido Black is a safe, permanent procedure, which can be used on non-porous and in some instances, porous surfaces, and can work well even if the item has been treated with cyanoacrylate fuming or LCV. Bloodstains should be fixed prior to development.

**Reagent**

Amido Black is available in a pre-mixed form.

**Method****Control Print**

A test print is processed at the first use of the day to ensure that the desired reaction is being obtained. Ridge detail should appear to be blue/dark in color, as seen here:

**Application**

Items are processed in a fume hood or well-ventilated area.

Blood impressions are fixed onto the evidence surface with 5-Sulfosalicylic acid fixer solution.

A small area of the object or surface being processed can be tested with the reagent to check for excessive background staining. If significant background staining occurs, a different enhancement reagent can be selected.

Application can be performed by the spraying, immersing, toweling, cascading, and pooling methods (see reagent application techniques for a description of these methods). The reagent should be left in contact with the impression for approximately 3 to 5 minutes.

Excess reagent is rinsed from the item or surface by immersing or rinsing with tap water and the surface is then allowed to dry.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 48 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	



Visualization

The item/surface is examined for ridge detail with white light. Amido Black is extremely stable; however, developed impressions should be preserved photographically.

Any prints that are suitable for capture are photographed.

For latent prints on a fluorescent background, use of an ALS at varying wavelengths can cause Amido Black stained ridge detail to appear even darker, providing good contrast for photography.

**Storage/Disposal**

Amido Black stock solution can be stored at room temperature in a clear or dark airtight container indefinitely.

Excess Amido Black solution can be disposed of down the drain with excess water.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 49 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

**Leucocrystal Violet (LCV) - Chemical****Description**

Leucocrystal Violet is used to enhance and develop latent prints deposited in blood on non-porous and in some instances, porous surfaces. It reacts with the heme moiety in blood to produce a purple/violet color. Cyanoacrylate fuming may be detrimental to this process. Even though this reagent contains a blood fixative, fixing with SSA should occur prior to development. Various protein stains, such as Acid Yellow 7, Hungarian Red, and Amido Black, can be used AFTER the LCV process. Blood impressions should be completely dry before processing.

**Reagent**

Leucocrystal Violet is available in a kit form. Mixing Instructions are as follows:

“Part 2” contents are added to the bottle marked “Part 1.” The “Part 1” bottle is recapped and shaken well for several minutes.

“Part 3” contents are added to the “Part 1” bottle. The “Part 1” bottle is recapped and shaken well for several minutes.

**Method****Control Print**

A test print is processed at the first use of the day to ensure that the desired reaction is being obtained. Ridge detail should appear to be purple in color, as seen here:

**Application**

Items are processed in a fume hood or well-ventilated area.

Blood impressions are fixed onto the evidence surface with 5-Sulfosalicylic acid fixer solution.

Application can be performed by the spraying, immersing, toweling, cascading, and pooling methods (see reagent application techniques for a description of these methods). Development should occur within approximately 30 seconds.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 50 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

Excess LCV may cause the background to turn purple due to photoionization that may obscure the impression, thus, excess LCV should be rinsed with water and the surface allowed to dry.

#### Visualization

The item/surface is examined for ridge detail with a white light. Latent prints developed with LCV reagent will be a purple/violet color.

Any developed print suitable for capture should be photographed as soon as possible due to the possibility of photoionization.

For latent prints on a fluorescent background, use of an ALS at varying wavelengths can cause LCV-stained ridge detail to appear even darker, providing good contrast for photography.

#### **Storage/Disposal**

LCV kits stored at room temperature will remain useful for a year or more. Once the kit has been prepared, the solution will remain useful for 3-6 months if kept in a dark bottle and refrigerated.

Pre-mixed LCV solutions can be used until a quality control test no longer yields the expected results.

Excess LCV solution can be disposed of down the drain with excess water.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 51 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

**Acid Yellow 7 - Chemical**

Caution: not recommended to be  
applied by spraying

**Description**

Acid yellow 7 is a protein stain that results in a yellow fluorescent coloration. It is used to enhance the detail in faint prints in blood and will not develop areas of latent prints that contain only the normal constituents of latent print residue. Due to its fluorescence, it is particularly useful on dark backgrounds. Acid yellow 7 should only be used on non-porous surfaces and can work well even if the item has been treated with cyanoacrylate fuming or LCV. Fixing of blood impressions with SSA should occur prior to development with Acid Yellow 7.

**Reagent****Developer**

2g Acid yellow 7  
100ml acetic acid  
500ml ethanol  
1400ml distilled water

Acid yellow 7 is added to the acetic acid.

This solution is combined with the ethanol.

Distilled water is added.

The solution is placed onto a magnetic stirrer and stirred for at least 30 minutes.

**Rinse**

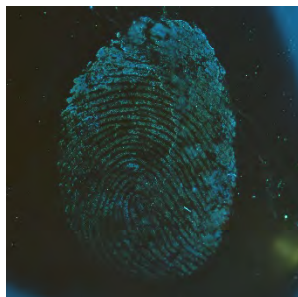
100ml acetic acid  
500ml ethanol  
1400ml distilled water

Chemicals are combined as above.

The developer and rinse solutions are prepared in the Crime Laboratory.

**Method****Control Print**

A test print is processed at the first use of the day to ensure that the desired reaction is being obtained. Ridge detail should be visible under the ALS at various wavelengths with yellow or orange barrier filters, as seen here:



#### Application

Items are processed in a fume hood or well-ventilated area.

Blood impressions are fixed onto the evidence surface with 5-Sulfosalicylic acid fixer solution.

Application can be performed by the immersing, toweling, cascading, and pooling methods (see reagent application techniques for a description of these methods).

The solution should be in contact with the impression in blood for approximately 5 to 10 minutes.

Excess Acid yellow 7 is washed from the surface using the rinse solution. The rinse solution may need to be applied several times in order to reduce the background staining and achieve the greatest contrast.

The surface is then allowed to dry.

Low contrast prints may be improved by retreatment with Acid yellow 7. The above procedure is followed but the fixing stage is omitted.

#### Visualization

The item/surface is examined for ridge detail with an ALS under blue to blue-green light (400-490nm) while using a yellow or orange barrier filter.

Any prints that are suitable for capture are photographed.

#### **Storage/Disposal**

Acid Yellow 7 developer and rinse can be stored in a clear glass bottle for 6 months or until a quality control test no longer yields the expected results.

Excess Acid Yellow 7 developer and rinse solutions must be disposed of down the drain with excess water.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 53 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

#### 4.6 ADHESIVE SURFACES

Items comprised of adhesive surfaces are frequently encountered in the laboratory as well as in the field. Special reagents exist to target latent print residues on such surfaces. These reagents, to include previously mentioned reagents like rhodamine, can be applied to the adhesive side of items such as tape, labels, stamps, etc.

##### General Considerations

##### Methods of adhesive release

There are various methods available to Criminalists for releasing an adhesive surface from another surface. These methods include freezing with Liquid Nitrogen, soaking with Un-du, applying heat with a blow dryer or other heat source, and manual separation. Liquid Nitrogen is recommended for use on strong adhesives such as duct tape, while Un-du is recommended for use on weaker adhesives, such as masking tape. Precaution should be exercised when choosing an adhesive release method and a quality control test with a similar tape type should be performed before application in casework. Cyanoacrylate fuming of any non-adhesive, non-porous surfaces should take place before (and possibly after) the use of an adhesive release method.

##### Additional testing

Prior to processing adhesive surfaces, Criminalists should be sure that there are no requests for additional testing (example: DNA, trace, etc.). If such requests have been made, the Criminalist should consult with the customer and the Crime Laboratory before proceeding.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 54 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

**Wetwop - Chemical****Description**

Wetwop is a pre-mixed liquid used to develop latent prints on adhesive surfaces. It is particularly effective on the adhesive side of tape; however, it can also be used on latex and Styrofoam surfaces.

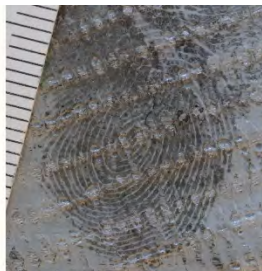
Note: Latent prints may be recovered from the non-sticky side of tape. Thus, tape should be processed with cyanoacrylate fuming prior to processing the adhesive side of tape, so that latent prints are preserved.

**Reagent**

Wetwop is available in a pre-mixed solution (White or Black).

**Method****Control Print**

A test print is processed at the time of use to ensure that the desired reaction is being obtained. If possible, the test print should be placed on a similar type of tape. Wetwop is available in white or black. Ridge detail should appear to be white or black in color depending on the choice of the Wetwop. Black can be seen here:

**Application**

Adhesive surfaces are separated using one of the previously described methods. The Wetwop container is well shaken, and a small amount of the reagent is poured into a secondary container. Using a brush, Wetwop is painted onto the adhesive side of the surface being examined. The mixture is left on the adhesive surface for approximately 15 seconds. Wetwop solution is rinsed off with running tap water or by gently agitating the item in a bowl of water. If additional contrast is needed, the above steps are repeated.

**Visualization**

Any prints that are suitable for capture are photographed.

**Storage/Disposal**

Wetwop pre-mixed solution has an indefinite shelf life. The working solution should be disposed of after each use, with excess water, down the drain.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 55 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

#### **4.7 POST PROCESSING PROCEDURES**

At the conclusion of processing items in the laboratory, case identifying information should be added to the surface of the item, if space and surface type allows, using indelible ink. Information should include the incident number, lab case number, the date of repackaging, the Criminalist's initials, and the item's number.

Items should be placed into a compatible sized heat-sealed bag, with the Criminalist's initials and the date written across both sealed ends. The case identifying information listed above is added to the heat-sealed bag as well as a caution statement if hazardous chemicals have been applied.

The heat-sealed bag(s) along with any original proximal packaging are then placed into the item's original outer packaging. Evidence tape is applied to the open end, and the Criminalist's initials and the date are recorded across the seal. Packaging tape is then used to cover the evidence tape and any unsecured openings of the package. If an item is processed with hazardous chemicals, a caution sticker will be applied to the outermost packaging in a visible location.

#### **Special Circumstances**

##### ***Firearm Related Evidence***

Any portion of a firearm needed for an operability examination by the Firearms Analysis Unit should be placed back into the original outer packaging without being placed in a heat-sealed bag. Cartridges and cartridge cases (if processed) do not need to be individually marked with case identifying information. They can be placed back into their original packaging for resubmittal to the Firearms Analysis Unit. If there is no request for processing of the cartridges or cartridge cases, they will remain within their original packaging.

##### ***Biohazards***

Items posing a biological hazard should be marked as such by placing a biohazard warning sticker on the outermost packaging in a visible location. If there is a question concerning how best to repackage a contaminated item, the Crime Laboratory should be consulted.

##### ***Adhesive Surfaces***

When repackaging any adhesive surfaces, it is generally recommended to use acetate sheet protectors as the proximal packaging before placing the item into a heat-sealed bag. If adequate acetate sheet protectors are unavailable, a heat-sealed bag can be used in their place.

##### ***Lifts***

Hinge, gel, and casting lifts do not require packaging in a heat-sealed bag and can be placed directly into envelopes or another suitable container.

#### **4.8 MIDEO**

Processing examinations will be recorded in Mideo and generated through the system. The processing worksheet is a required worksheet and will be saved to the system upon completion. In the event that Mideo is not functioning, hardcopy worksheets may be utilized. The hardcopy worksheets can be found on the quality drive.

All required field sets must be completed. A representative image of the evidence will be uploaded to Mideo.

Photo logs will not be required. Simplified metadata descriptions will be added to items and latent prints in the SAN.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 56 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	



#### 4.9 MAINTENANCE PROGRAM

The Unit does not designate any equipment as critical. The equipment is serviced on an as needed basis. The hoods are inspected annually with the scheduling assistance of the Crime Laboratory. This program of maintenance is updated and recorded in the LPU equipment database by members of the Unit. Additionally, a Criminalist is designated as the Equipment Database Manager with a second Criminalist as a back-up. All equipment is reviewed as part of an annual equipment database maintenance check.

#### 4.10 CONFLICTS & WORKFLOW

Conflicts can arise where a reviewing Criminalist may have a differing conclusion than the original Criminalist. This may occur during the actual processing of the items or upon review of the case record. The reviewing Criminalist may determine there is additional ridge detail on an item that is suitable for capture. The original Criminalist has the opportunity to re-examine the item and may agree with the reviewer upon additional examination.

The following steps should be taken to ensure that these conflicts are resolved effectively and expediently:

- The conflicting Criminalists should discuss the issue and attempt to resolve the matter to all relevant parties' agreement.
- If the Criminalists reach a resolution, a notification via email will be made to a Criminalist IV/Director of the conflict.
- If the Criminalists cannot reach a resolution, the discussions should include the Director of Quality, the Director, and/or a Criminalist IV. An independent Criminalist not already associated with the case will be consulted and the two Criminalists in agreement will sign off on the case.
- When a decision is reached, it must be clearly communicated to all relevant parties involved.

Documentation is required in all situations.

Mideo will track all conclusion changes in the system. A Criminalist IV and/or the Director will be notified.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 57 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

## **5. CRIME SCENE**

The LPU offers its service to process crime scenes and/or vehicles on an as needed basis. All Criminalists must have the proper education, training, and experience before being placed on the Crime Scene on-call list. Since each crime scene is considered unique, Criminalists should use their overall education, training, and experience when deciding how to best process any crime scene.

### **5.1 Callout Guidelines**

The crime scene list contains contact information for the LPU Criminalists (I – IV). The Criminalist at the top of the list will remain there for a period of one week. After the one-week period that Criminalist will move to the bottom. It is the responsibility of the Criminalist on top of the list to make arrangements with another Criminalist if he/she is unavailable during that time period. The Director will always be placed at the bottom of the list when all other Criminalists are unavailable for a crime scene callout or in cases where there is an emergency in the laboratory during off hours. The list will be sent to the Operations Division, the Crime Scene Response Unit, and the Homicide Unit as updated. It is the responsibility of all Criminalists to know which Criminalist is currently on call.

Whenever possible, two qualified Criminalists should respond to crime scenes. Three Criminalists may respond to a scene if one of the Criminalists is in the training program. Depending on the nature and size of the scene, additional personnel may respond at the discretion of the responding Criminalists. Once Operations calls out a Criminalist to respond to a scene, that Criminalist is responsible for calling out additional Criminalists. The Criminalist receiving a call from Operations is not required to go down the list in order to find a second qualified Criminalist to assist in processing the scene. The activity log may be utilized to determine the frequency of response by all Criminalists. A rotation for response is the goal to ensure that all Criminalists are given the opportunity to assist at a scene. If a Criminalist who is not on top of the list receives a call from Operations, that Criminalist should ask Operations if he/she called the on-call person. If a Criminalist receives a call out request directly from a customer, it is the responsibility of that Criminalist to call the Criminalist on the top of the list. The Criminalist receiving the call on off hours should remind the investigator to call Operations in the future.

Notification will be made to the Director/designee regarding the following:

- When a response to a scene is requested and response is made
- Names or initials of Criminalists responding
- When scene is completed

### **5.2 Vehicles**

The unit is assigned vehicles for responding to scenes. The vehicles should be operated in a safe manner. All Criminalists are responsible for stocking the vehicles with the proper supplies and monitoring the fuel levels.

### **5.3 Notification and Request for Services**

Requests for crime scene processing services may come from the Operations Division, directly from the customer, or from the Crime Scene Response Unit. If a Criminalist is contacted by the Operations Division, he/she should contact the customer directly to ensure the proper supplies and equipment are brought to the scene.

Common questions to ask the investigator prior to departing for the scene include, but are not limited to:

- Is it an indoor or outdoor scene?
- What type of incident is it?
- Is the body on scene?
- What types of evidence are we looking for?
- Does the scene appear to be cleaned?
- Do we need to chemically enhance any possible bloody prints?

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 58 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

- Do we need to bring the alternate light source?
- Are there any other special considerations?

#### **5.4 Crime Scene Documentation**

The crime scene notes (templates located on the quality drive) can be supplemented with photographs, sketches, and/or videos. Crime scene notes begin the moment the Criminalist receives the request to respond to the scene. All crime scene documentation shall be written in permanent ink, with the exception of extreme weather conditions such as heavy rain and/or subfreezing temperatures. Each page of notes and/or rough sketches shall be marked with the incident number, case number, date, the note taker's handwritten initials, and page number. Crime scene worksheets are available and should be utilized for documentation of the scene.

General information/observation includes, but is not limited to, the following:

- Date and time of notification
- Location of the incident
- Date and time of arrival
- Weather (if applicable)
- Personnel present that are interacting with the forensic units at the scene
- General observations
- Both negative and positive results of examinations/searches

The Evidence Log includes, but is not limited to, the following information/observations:

- Cone number (if applicable)
- Evidence letter or identifier
- Initials of collector(s)
- Time of collection and date (if not same as start date)
- Brief description of the item
- Location from where the item was collected

In instances where no evidence is collected and/or no processing was conducted at the scene, a case record will be generated for the notes and when necessary, a report may be created. When processing is completed, a report will be generated.

Notes will be entered into the LIMS crime scene panels under the i#. Handwritten notes will be added to the case record.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 59 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

## 6. COMPARISON

### 6.1 LATENT PRINT FUNDAMENTALS

Latent print examinations involve the discovery, development, enhancement, documentation, and preservation of residue impressions deposited by contact of friction ridge skin with an object and the comparison of such impressions to the exemplar reproduction of friction ridge skin known to belong to a specific individual. "Latent prints" is a generic term of general acceptance but may refer to any of the following:

- Latent, Patent, and Plastic Impressions
- Fingerprints, Palm prints, and Plantar prints
- Chance Impressions and prints of unknown origin

The purpose of latent print examination is to determine the origin of the preserved impression while operating within an established and accepted protocol. Friction ridge impression examinations are conducted by Criminalists using the Analysis, Comparison, Evaluation, and Verification (ACE-V) methodology, which includes both qualitative and quantitative aspects. ACE is not generally applied as a strictly linear process because it may include a return to any previous phase. Application of ACE includes observations, measurements, assessments, decision making, and documentation, which are enabled by the education, training, skill, and experience of the Criminalist.

The examination of friction ridge impressions and the resulting conclusions are based on ridge flow/patterns/shape (level 1); ridge paths, the location, direction, and spatial relationships of minutiae (level 2); and ridge/pore structure (level 3). The analysis phase leads to the determination of either suitable or not suitable (no value) for identification purposes. The comparison phase is a side-by-side comparison of friction ridge impressions. The evaluation phase leads to the following conclusions: *identification, exclusion, or inconclusive*.

#### Foundation for Friction Ridge Examination

##### Skin

The morphology of friction ridge skin is unique and the arrangement of friction ridges is persistent barring trauma to the basal layer of the epidermis. An impression of the unique details of friction ridge skin can be transferred during contact with a surface. An impression that contains suitable quality and quantity of friction ridge detail can be identified to, or excluded from, a source. Impressions may display features of varying quality (clarity of ridge features) and specificity (weighted values and rarity).

##### Criminalist

The Criminalist gains expertise in the analysis and comparison of friction ridge impressions through training and experience. Casework involves analyzing and comparing latent print impressions with known impressions from the relevant population. Suitability is the Criminalist's determination that the quality and quantity of the friction ridge impression is adequate and contains unique details such that the source could be identified. Macro and micro features are utilized through the analysis and comparison process.

#### Levels and Use of Friction Ridge Skin Detail for Examination

##### Level One Detail – Macro

Overall ridge flow/shape

General morphology (example: overall size)

Can be used for pattern interpretation

Can be used to determine anatomical source (example: finger/palm/foot/toe) and orientation

Can be used to exclude in high quality impressions

Cannot be used alone to identify

##### Level Two Detail – (Micro)

Individual ridge path

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 60 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

Presence of minutiae (example: ridge ending, bifurcation, dot)  
Absence of minutiae (example: continuous ridge, open field)  
Compound minutiae (example: enclosures, cross-overs, spurs, opposing bifurcations)  
Obscured ridge path feature (example: when a single ridge flows into a visually obscured area and 2 ridges emerge)  
Ridge path morphology (example: length of a ridge, angle of bifurcation opening)  
Used in conjunction with level one detail to identify or exclude

Level Three Detail – (Micro)

Structure/condition of individual ridges  
Shape of the ridges and pores  
Relative pore position  
Other specific friction skin morphology (example: ridge breaks, etc.)  
May be used in conjunction with level one and/or level two detail to identify or exclude

Additional Features – (Macro and Micro)

Other features associated with friction ridge skin (example: presence of incipient ridges, creases, wrinkles, scars, warts, paper cuts, blisters, etc.)  
May be permanent or temporary  
May exist as level one, two and three detail  
May be used in conjunction with friction ridge detail to identify or exclude

**Criteria for Identification**

SWGFAST – Standards for Examining Friction Ridge Impressions and Resulting Conclusions (Document #10) states the following:

“The use of a fixed number of friction ridge features as a threshold for the establishment of an identification is not scientifically supported.”

**Sufficiency for Conclusions**

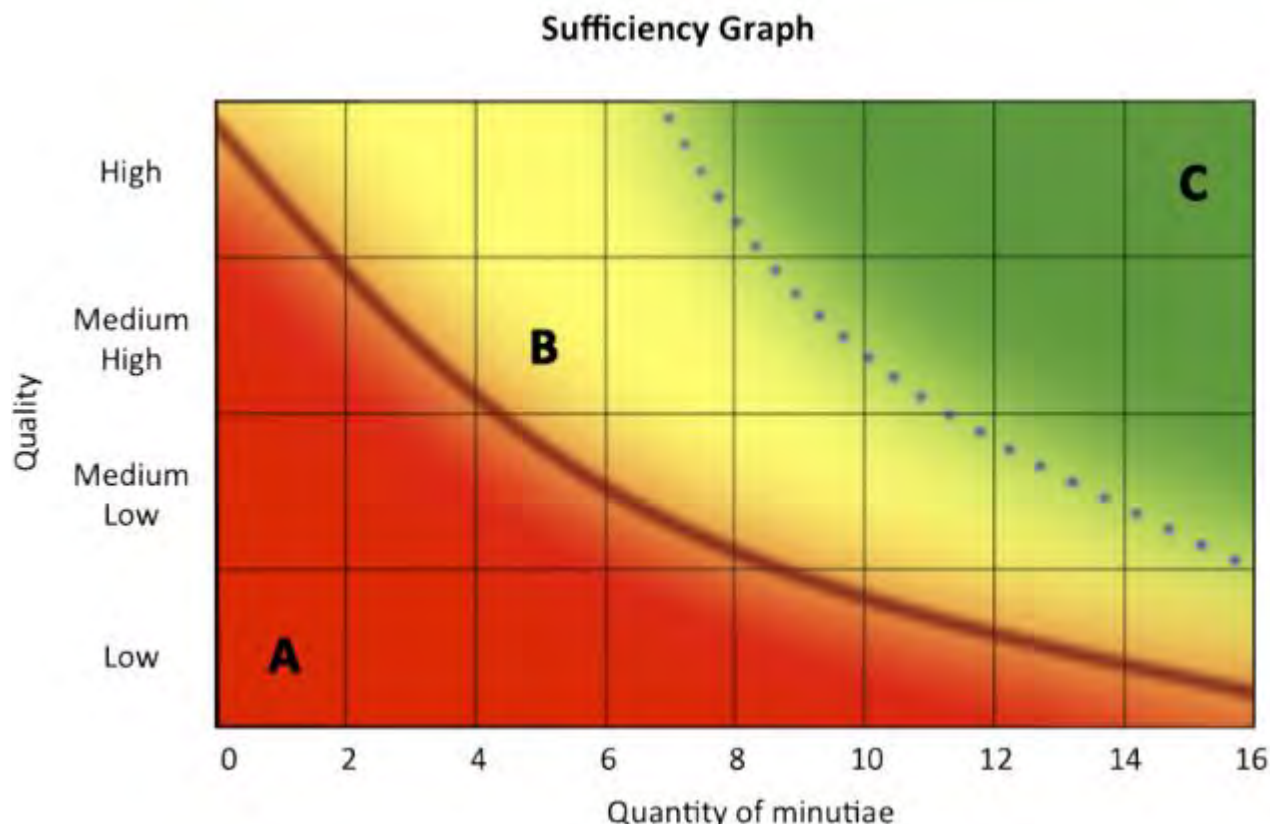
Sufficiency is a subjective interpretation of the quality and quantity of the objective data observed in the impression. As the quality of an impression increases, the need for quantity of friction ridge features decreases, as well as the inverse.

**Quality** is the assessment of the clarity of ridge features. Generally, as quality increases so does the discernibility and reliability of the ridge features. Quality may not necessarily be consistent throughout the impression.

The level of quality determines the degree of tolerances that will be used during the comparison process. High quality will lead to low tolerances and conversely low quality will require high tolerances.

**Quantity** is the number of ridge endings, bifurcations, and dots (minutiae) in contiguous ridges, determined without any reference to known impressions. Level 2 detail encompasses more than minutia counts (including the ridge path, areas with open fields, and selectivity of minutiae).

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 61 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	



The sufficiency graph depicted serves as a guideline only. Each latent print is unique and may not fall within the prescribed areas of the graph. In the above figure, the solid curve in the graph defines the lower limit of the sufficiency of friction ridge details below which, in the area marked **A**, an identification decision may not be clearly supported. The dotted curve indicates the boundary between levels of complexity (complex versus non-complex). In the area marked **B**, the examination is considered complex, and an identification may be supported. In the area marked **C**, the examination is considered non-complex, and an identification may be clearly supported.

## 6.2 COMPARISON CASE STRATEGIES

### Procedure I

An identification of one latent print in the case or one latent print per item to one or more listed subjects can be provided to the customer before completing analysis on all latent prints. In some cases, analysis of the remaining prints may not be performed.

### Procedure II

The Customer has reasonable cause to request that more or all latent prints in the case be compared against the subject(s). The Criminalist will complete the examination for trial upon request from the Customer. Re-lifts or additional photographs of the same latent print do not have to be compared provided the original lifts or photographs are suitable for identification purposes and compared. If the probative location cannot be determined, the Criminalist may examine all suitable latent prints. To conclude that no identifications exist, all of the suitable latent prints in the case shall be compared to each subject, provided that appropriate exemplar prints are available.

### Additional Considerations

The LPU will not make additional comparisons to any latent prints that have been previously documented and reported as identifications when the originating Criminalist and/or verifier are available for testimony. Any request

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 62 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	



made to compare identified latent prints to a new set of known impressions/major case impressions will be denied. This request will be re-directed to the CSRU as a ten print to ten print comparison. Communication regarding this request will be documented in case correspondence.

Ten print to ten print/post mortem comparisons and/or AFIS search requests of ten prints/post mortems, must first be directed to the CSRU. The LPU may be able to assist with these comparisons and/or AFIS searches when requested by the CSRU or the Homicide Unit.

### **6.3 METHOD OF FRICTION RIDGE EXAMINATION (ACE-V)**

The ACE-V methodology of friction ridge impression examination utilizes a qualitative and quantitative assessment of Level 1, Level 2, Level 3 details, and additional features. The ACE-V methodology is applied to examinations and comparisons of friction ridge impressions (example: latent to known, known to known, etc.).

#### **Analysis (A)**

Analysis is the assessment of a friction ridge impression to determine suitability for identification. Friction ridge impressions lacking value for identification are not further compared. Factors considered to determine suitability include the following:

- Quality (clarity) and Quantity of detail
- Level One Detail
- Level Two Detail
- Level Three Detail
- Additional Features
- Pattern Classification
- Anatomical Source
  - Finger (abduction/adduction of digits)
  - Palm (hand flexion)
  - Foot
- Possible Simultaneity
- Factors influencing quality include but are not limited to:
  - Residue/matrix
  - Deposition (pressure, shearing stress, or torque)
  - Surface/substrate (angle of contact)
  - Environment
  - Development medium
  - Preservation method
  - Condition of the friction skin (adolescent growth, aging, injury or disease)

As stated in the Quality Manual (Section 7.2.1.1.2), all test methods that involve the comparison of an unknown to a known require the evaluation of the unknown latent(s) to identify characteristics suitable for comparison prior to comparison to one or more known exemplar(s). Analytical images (which could be just the grayscale image) will be created and saved to the SAN. Criminalists may utilize a variety of colored markings to memorialize the features depicted in the latent print that supports their determination of suitability for identification.

#### **Comparison (C)**

Comparison is the direct or side-by-side observation of friction ridge detail to determine whether the detail in two impressions is in agreement based upon similarity, sequence and spatial relationship.

Criminalists compare impressions in a recurring process to evaluate disagreement or agreement. Comparison begins by determining if level 1 details are within tolerance. If so, a target group of level 2 and/or level 3 features is selected from the unknown impression and searched for in the known impression. Alternative target groups may be selected and compared. If similarities are found, additional adjacent features are compared and

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 63 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

assessed. A culmination of the agreements or disagreements observed between the impressions initiates the evaluation phase.

At times, a Criminalist may compare latent prints that have limited quality and/or quantity of information. This may include complex latents with low specificity of features and/or significant distortion. A Criminalist may encounter identifications that pose more of a challenge to reach a conclusion. Such an identification may require:

- The presence of an unusual combination of level two detail, a rare ridge characteristic, scarring, level three detail, or equivalent.

**AND/OR**

- The concurrence of **two** other qualified Criminalists based upon direct or side by side comparison of the latent print and the exemplar print. Prior approval by the Criminalist IV/Director must be obtained for consultation with a qualified latent print analyst outside of the Unit.

Comparison images with annotations depicting the detail supporting the evaluation will be saved to the SAN.

### **Exemplar Prints**

Exemplar prints are of an individual associated with a known or claimed identity and deliberately recorded electronically, by ink, or by another medium (also referred to as “known” prints). Exemplar prints are not considered evidence and copies/representations are retained (with the exception of inked elimination prints) within the case record as documentation. Contemporaneous exemplars should be utilized when available in the case.

Major case impressions and post-mortem impressions utilized in comparisons are scanned and/or photographed and uploaded to the SAN. Inked exemplar prints that are stored in the unit are considered originals. If exemplar prints are submitted as an evidentiary item number, the item will be transferred into LIMS as a safekeeping item and the barcode will be covered.

Exemplar ten prints are typically printed by the following means:

- Massachusetts State Police Database (MORPHO State)
- Repository for Integrated Criminalistic Imaging (RICI)
- Personnel ID System (PICS)
- Federal Bureau of Investigation Database (MORPHO Federal)

Exemplar prints may be received in the form of:

- Inked Ten Prints/Elimination Prints
- Digital/Livescan Files
- Post-mortem Prints
- Major case impressions

Exemplar prints submitted to the unit for comparison purposes may be submitted back to the originating agency/customer/major case files with a copy of the exemplar prints retained in the case record. Original elimination prints may be retained in the case record.

Criminalists conduct quality checks of exemplar prints provided to ensure:

- Electronic capture errors are not present in Livescan files

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 64 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	



- Rolled vs. Flats are in agreement
- Right vs. Left are documented in the correct order/designation/labeled card
- Demographic information is present (minimum of a name)
- MA SID number and/or a CR # is documented (if applicable)
- Arrest date (if applicable)
- Additional exemplars received bearing the same name has consistent ridge detail depicted in previous cards obtained

### **Evaluation (E)**

Once the examination progresses from the comparison phase into the evaluation phase, it is determined whether or not the information is sufficient to form one of the three conclusions or return to the analysis phase and reassess suitability.

Evaluation is the formulation of a conclusion based upon analysis and comparison of friction ridge impressions. Conclusions that can be reached are:

#### Identification

An identification is the determination that two friction ridge impressions originated from the same source because there is sufficient quality and quantity of corresponding information such that the examiner would not expect to see the same arrangement of features repeated in another source.

#### Exclusion

Exclusion is the determination that two friction ridge impressions originated from different sources because there is sufficient quality and quantity of non-corresponding information.

When the impressions are determined to be high quality with unambiguous features (plain impression depicting clear level 1 detail), an exclusion is warranted. For example, when the unknown impression is an arch pattern and the specific known impression under consideration is a whorl pattern (see images below).



Images courtesy of SWGFAST – Standards for Examining Friction Ridge Impressions and Resulting Conclusions (Document #10)

There are exceptions to excluding on level 1 alone. Instances where, due to an accident, disease or intentional disfigurement, fingerprint patterns or ridge flow may change by taking on the appearance of a different pattern or ridge configuration. Examiners coming to exclusions based on Level 1 detail must be aware of these phenomena and account for their influence as part of the decision-making process.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 65 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	



Inked Print

Scarred Print

Images courtesy of the Fingerprint Interest Group

For all other latent print impressions, a Criminalist will come to the decision of exclusion only after the following criteria are met:

- That all necessary anatomical regions are clearly recorded for comparison within the exemplar prints.
- Level one and level two detail must be used in conjunction to reach an exclusion decision.
  - **Level one:** A core and/or delta is ideal. Major creases, a vestige, funnel area, or any distinctive ridge flow that anchors the anatomical location of the latent print.
  - Shape of the latent print, ridge flow, creases, position on the evidentiary item, and neighboring ridge detail can all assist the Criminalist in determining the anatomical region.
  - **Level two:** Target a group of level two ridge events with a specific spatial relationship to the level one feature. Do not dismiss open field areas that also have a specific spatial relationship to the level one feature.
  - A tolerance should be set for anatomical region and distal orientation when conducting an analysis of the above listed detail. A Criminalist should take into consideration that the latent print is a different orientation or that there is a variation in appearance of the level one and two detail.
  - Anatomical uncertainty may arise even when you have distinct detail present in the latent print. The Criminalist must search every possible anatomical region in every possible orientation and ensure that each is tracked within the analytical images and/or case notes.
  - Criminalists should consider the substrate the print was recovered from in regard to correct orientation (example: adhesive surfaces where the impression could be mirrored).
- The Criminalist will use more than one target group of level two detail before reaching a conclusion of exclusion.
  - **Target groups:** These features are relatively unique, selective, and easy to spot (example: enclosures, short ridges, over-unders, ridges facing opposite directions, etc.)
  - The first target group may not be captured in the exemplars and/or the Criminalist may miss seeing the initial target group. When there are differences at multiple target groups, the sufficiency for exclusion will be supported.

Exclusions can be made by a physical comparison (as noted above) or deduced when an impression is identified to another individual. When an exclusion is deduced, it is simply referring to the sample group that was considered.

#### Inconclusive

Inconclusive evaluation can result when a Criminalist is unable to identify or exclude the source of an impression due to the areas of the known exemplar prints having incompletely recorded ridge detail or the ridge detail is not suitable to allow for a complete comparison. In this instance, the impression needs to be reexamined using clear and complete known exemplar prints.

Inconclusive evaluation can result when a Criminalist has completed an exhaustive search of the latent print impression and the known exemplars, and the latent print impression is neither identified nor excluded as originating from the same source. An inconclusive conclusion will be made when all of the above listed exclusion criteria cannot be met.

#### Inconclusive with similarities - Investigative Information

Inconclusive evaluation can result when a Criminalist has completed a comparison with a specific finger or palm and similarities are observed but no identification can be effected. This information is being reported out as potential investigative information only; the evidentiary value may be limited.

When an inconclusive with similarities conclusion has been reached, the latent and known comparison images will be saved for the case record and will include "SIM" in the title. Comparison decisions made prior to the inconclusive with similarities decision will be included in the report. If additional subjects were not compared, that will be reflected in the report.

#### ***Verification (V)***

Verification is the independent application of the ACE process utilized by a subsequent examiner to either support or refute the conclusions of the original examiner.

A verification will be conducted on all reported identifications, exclusions, and inconclusive with similarities conclusions. Verifiers are held to the same level of responsibility as the original Criminalist on the case. It is the verifier's responsibility to ensure that the original Criminalist followed all procedures, did enough testing, and reached the best conclusion for the data given. Verifiers do not try to confirm the conclusion but instead attempt to falsify the original Criminalist's evaluations.

The verifier's images will be the supporting documentation for the conclusion reached.

The verifier may be made aware of the verification via email. This email acts as a notification only and is not considered a part of the case record. A request may be received by the verifying Criminalist to conduct a 100% verification on all latents.

#### Latent to Known Comparisons

Verifications may be conducted on any conclusions (example: inconclusive, not suitable for identification purposes). A verification consists of the verifying Criminalist having access to the known exemplar(s), latent print(s), and conclusions of the original Criminalist. The verification process in no way inhibits the verifier's independent analysis, comparison, and evaluation.

The latent and known image(s) needed for the verification process can be accessed through the SAN. Any known impression cards not uploaded to the SAN at the time of verification will be provided in physical form to the verifier. A verification folder will be created on the SAN by the verifying Criminalist containing annotated images produced by the verifying Criminalist. This folder will be named by using the verifier's initials and the word 'verification' (example: AA verification, KM verification). These images will be locked and included in discovery packets.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 67 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

Post-Mortem Impressions/Ten Print to Ten Print Verifications (Requests from Homicide/CSRU)

A verification process will be conducted on conclusions of identification and exclusion with post-mortem impressions and ten print impressions. A representation of both ten print cards will be retained as a part of the case record. Comparison images created by the original Criminalist may be retained in an analytical folder found on the SAN.

Verifications will follow the same image workflow as stated above.

**Double Verification**Latent to Known Comparisons

Double verifications may be conducted on single latent print identifications. These may include those generated by AFIS, when the latent print has limited quality/quantity of information, or both. These verifications will be conducted by two different Criminalists. Double verifications can be requested for any conclusion at the discretion of the originating Criminalist.

Double verifications on identifications will follow the same image workflow as stated for open verifications.

**Blind Verification**Latent to Known Comparisons

Blind verifications will be utilized for conflict resolution and may be completed on any type of conclusion(s). These may include single latent print identifications to include those generated by AFIS, when the latent print has limited quality, quantity of information or both. In a blind verification, the Director/Criminalist IV (not involved with the case) will assign the verification and provide the latent print(s) and known exemplar(s). The original Criminalist's conclusion(s) and supporting documentation will not be provided.

The Director/Criminalist IV will create a folder on the SAN for the verifying Criminalist which will contain the latent print(s) and known exemplar(s) without case information included. The verifying Criminalist will save analytical images in the same manner as stated above in a 'blind verification' folder. The images will be utilized to document their conclusion(s) without accessing any case information until the examination has been completed.

If a discrepancy between the evaluations of the original and verifying Criminalist(s) is found during the verification process and no agreement is made see Section 6.5.

**Consultations**

Criminalists are encouraged to foster a culture of openness and discussion regarding the comparison of latent prints. Most discussions regarding latent print comparisons do not rise to the level of consultation and will not need to be documented as part of the case record.

Consultations may be performed in certain situations, including the following:

- assess the suitability of a specific latent print(s) for comparison
- assess the suitability for an AFIS search
- evaluate a specific latent with a known impression

Consultation requests are made after the original Criminalist has recorded their preliminary observations (annotations on images) and findings (suitability/conclusions). These observations and findings shall not be provided to the consulting Criminalist.

When the consulting Criminalist contributes to a decision being made by the original Criminalist, it will be documented in the case record. Documentation may include, but is not limited to the following:

- specific latent print(s) reviewed

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 68 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

- the topic and result of the consultation
- date(s) of consultation and consulting Criminalist identifier
- consulting Criminalist images

The consulting Criminalist will NOT be the verifier or the arbitrary (3<sup>rd</sup>) Criminalist in the event that no agreement is reached.

### **Evaluation Change**

Review of conclusions may lead to the verifier producing a differing conclusion than the original Criminalist (e. g. insufficient ridge detail for identification vs. sufficient ridge detail for identification, identification vs. inconclusive, or exclusion vs. inconclusive). The original Criminalist has the opportunity to re-analyze the latent and may agree with the verifier upon the additional analysis.

A Criminalist IV and/or the Director will be notified. If no agreement is reached see Section 6.5.

### **Additional Names for Comparison**

When a customer requests multiple rounds of names for comparison purposes the Criminalist can inquire the purpose of the comparison with a particular individual. The Criminalist can notify the customer that the print(s) has/have been searched through the AFIS and no further comparisons will be completed with subjects that have previous arrests/cards in the system unless there is additional investigative information.

## **6.4 MIDEO**

Comparison examinations will be recorded in Mideo and notes will be generated through the system. The comparison worksheets that can be generated are the Analysis Case Notes, Comparison Case Notes, Conclusion Summary, and AFIS Case Notes. These worksheets are determined by the work performed in the case and will be saved to the system upon completion.

All required field sets must be completed. The comparison Criminalist will create a latent print icon for each latent print in the assignment. One grayscale image per latent print will be uploaded to Mideo, replacing the generic latent icon. All other images will remain on the SAN. The comparison Criminalist will create an exemplar icon for each individual that is being compared. The images of the knowns will remain on the SAN.

Mideo case notes will reflect evaluation changes and non-consensus decisions.

In the event that Mideo is not functioning, hardcopy worksheets may be utilized. The hardcopy worksheets can be found on the quality drive. When the hardcopy Comparison ACE Worksheet is completed a check mark will indicate "yes" to the question posed. A dash mark or blank box will indicate "no" to the question posed. "N/A" may be used when the question posed is 'not applicable'. When a check mark is indicated for the inconclusive question posed, the "other area" and/or the "comment" section of the worksheet will support the inconclusive evaluation made by the Criminalist.

## **6.5 CONFLICTS AND WORKFLOWS**

Conflicts can arise when there is an inconsistent conclusion between two or more Criminalists upon completion of ACE-V.

The following steps should be taken to ensure conflicts are resolved effectively and expediently:

- The conflicting Criminalists should meet and discuss the issue in an attempt to resolve the matter. .
- If the Criminalists reach a resolution, a notification via email will be made to a Criminalist IV/Director of the conflict.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 69 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	



- If the Criminalists cannot reach a resolution, the discussions should include the Director of Quality, the Director, and/or a Criminalist IV. A blind verification by an independent Criminalist not already associated with the case will be conducted on the impression(s) causing the conflict. If a differing decision is reached by the independent Criminalist, a consensus panel will be created by the Director of Quality, the Director, and/or Criminalist IV.
- When a decision is reached, it must be clearly communicated to all relevant parties involved.

Documentation is required in all situations.

### **Erroneous Identification**

An erroneous identification is the incorrect determination that two areas of friction ridge impressions originated from the same source. An erroneous identification typically includes the following elements:

- The Criminalist documented the identification by recording the name from the exemplar prints and the friction ridge area in their case notes.
- The comparison was submitted to a second Criminalist for verification.
- The second Criminalist determined the latent print and known impression were **NOT** made by the same source and the error is not administrative.
- Consensus decision is not reached between the Criminalist and the Verifier.

Verification of an erroneous identification is equal to having effected the original erroneous identification. All mitigating and aggravating circumstances will be taken into account in determining appropriate corrective action.

### **Erroneous Identification Workflow**

A Criminalist and/or a qualified Latent Print Analyst(s) from an outside source will complete a blind verification and reach a conclusion. A quality review meeting shall be conducted by the Director of Quality, the Director, and/or a Criminalist IV and will determine if a consensus panel will need to be formed and/or what recommended corrective action(s) may be implemented.

A consensus panel may be comprised of an odd number of Criminalists not associated with the case. Each panel member will conduct their own independent blind verification within a reasonable timeframe. The panel will hold a meeting after the independent verifications are completed. The purpose of the meeting is to come to a consensus opinion that is agreed upon by all, documented, and relayed to the Director of Quality, Director and/or a Criminalist IV.

An additional quality review meeting may be necessary after the consensus opinion to finalize recommended corrective action(s).

If the Criminalist is certified by the International Association for Identification (IAI), he/she will notify the Association of the incident.

### **Erroneous Exclusion**

An erroneous exclusion is the incorrect determination that two areas of friction ridge impressions did not originate from the same source. An erroneous exclusion typically includes the following elements:

- A Criminalist compared a suitable latent print to exemplar prints and excluded the donor as the source of the impression.
- The verification by another Criminalist established an identification with exemplar set(s) of the same individual.
- Consensus decision is not reached between the Criminalist and the Verifier.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 70 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

**Erroneous Exclusion Workflow**

A Criminalist and/or a qualified Latent Print Analyst(s) from an outside source will complete a blind verification and reach a conclusion. A quality review meeting shall be conducted by the Director of Quality, the Director, and/or a Criminalist IV and will determine if a consensus panel will need to be formed and/or what recommended corrective action(s) may be implemented.

The same workflow and additional meetings described above for the consensus panel may be implemented for an erroneous exclusion decision that remains in conflict.

**Non-Consensus Decisions**

A non-consensus decision is a determination or conclusion reached by a Criminalist at any step of the examination process that cannot be assessed as an error, but conflicts with the consultant or verifier of that decision. For example, whether or not the examination of a latent and known from the same source should result in an identification or inconclusive decision cannot be defined in terms of an error but only with respect to a consensus.

Non-consensus determination of suitability is when a Criminalist's determination of suitability does not concur with the consultant or verifier.

Non-consensus inconclusive is when a Criminalist reaches a decision of inconclusive that conflicts with the consultant or verifier's conclusion of identification or exclusion.

**Non-Consensus Decision Workflow**

When a disagreement occurs, the original Criminalist and verifier must first meet in an attempt to come to a resolution. If a single conclusion cannot be reached for the latent(s) in question, a Criminalist IV/Director will be notified of the original and verifying examiners' conclusions within two working days after the meeting. A blind analysis of the latent print(s) in question and the known impression(s), if applicable, will be conducted by a qualified examiner and supporting analysis/comparison images will be completed.

When no agreement can be made after the blind analysis, a quality review meeting may be conducted by the Director of Quality, the Director, and/or a Criminalist IV and will determine if a consensus panel will need to be formed and/or what recommended corrective action(s) may be implemented.

The same workflow and additional meetings described above for the consensus panel may be implemented for non-consensus decisions that remain in conflict.

**Double Verification Non-Consensus Workflow**

When a latent print impression is sent for a double verification, both verifiers must be in agreement in order to report out the conclusion. When the original examiner and one verifier are in agreement, but the additional verifier delivers a non-consensus decision, a meeting will take place with all parties in an attempt to come to a resolution. If a single conclusion cannot be reached for the latent in question by all three Criminalists, a Criminalist IV/Director will be notified within two working days after the meeting. A blind analysis of the latent print in question and the known impression will be conducted by a qualified examiner and supporting analysis/comparison images will be completed. When a majority consensus cannot be made after the blind analysis, a quality review meeting may be conducted by the Director of Quality, the Director, and/or a Criminalist IV and will determine if a consensus panel will need to be formed and/or what recommended corrective action(s) may be implemented.

The same workflow and additional meetings described above for the consensus panel may be implemented for decisions that remain in conflict.

When all three Criminalists are in non-consensus with differing conclusions, a meeting will take place with all parties in an attempt to come to a resolution. If a single conclusion cannot be reached for the latent in question by all three

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 71 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

Criminalists, a Criminalist IV/Director will be notified within two working days after the meeting. No additional analysis or meetings will be required, and the most conservative conclusion will be reported.

### **Conflict Resolution Documentation**

When an agreement is made after the blind analysis, a separate report will be completed by one of the two examiners that are in agreement for the latent(s) for which there was a conflict. The second Criminalist will then complete the technical and administrative review.

The qualified Criminalist does not need to analyze/verify remaining latent(s) in the case for which there was no conflicting decisions between the originating examiner and the originating verifier. The original Criminalist and originating verifier will complete an additional report for the latents in agreement.

Tracking non-consensus decisions provides a means to quantify whether examiners are being overly cautious or aggressive in their decisions.

## **6.6 AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM (AFIS)**

The Automated Fingerprint Identification System (AFIS) is a tool used to search unknown latent prints, found at crime scenes or recovered from evidentiary items, against a database of known fingerprints of individuals. The database provides access to known print records for comparison purposes.

Only trained and authorized personnel will be given access to the AFIS databases which are password protected. The list of qualified personnel is maintained in the Quality records.

The BPD LPU AFIS Section provides the following services:

- Priority on lift cases without a suspect.
- Review of previously worked open homicide cases to determine whether additional AFIS searches can be completed.
- Troubleshooting AFIS database problems encountered.
- Assignment of any cold cases.
- Assistance with AFIS searches requested from crime scenes and/or for Criminalists.
- Compiling AFIS statistics.
- Training of the AFIS databases & services.
- Assist with identifications of unknown bodies and individuals.
- Completing FBI reverse searches.
- Assist in training new Criminalists on all aspects of AFIS.

### Criteria for Searches

AFIS may be utilized by the Criminalist to search latent prints when one or more of the following criteria is met:

- No suspect(s) information is available
- Elimination exemplar prints are provided, and no identifications are made
- A request is made by the Customer
- Criminalist discretion

A Criminalist (original or verifier) may also utilize AFIS to assist in a closed search of a latent print(s) with a subject or multiple subjects. When a verifier performs a closed search, the following should be completed:

- Creation of a case in the database to allow for the closed search
- A "V" will be added at the end of the case number when the verifier is performing a closed search
- All information will be entered to create the case with the verifiers own calibrated image

The Criminalist shall have the authorization to perform or not perform database searches on a case-by-case basis taking into consideration the facts of the case and the factors listed below.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 72 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	



A friction ridge impression is suitable for a search when any of the following are present:

- A minimum of 6 clear and unique level two details or higher
- A core and/or delta, or recognizable palm area
- Clarity of detail (may include orientation)

Exigent circumstances may allow for searching of suitable friction ridge impressions prior to complete analysis of all friction ridge impressions in a case.

Latent print images that will be searched, must be calibrated to be 1:1. Descriptions, with pictures, are available in the AFIS workflow guide detailing two techniques for calibrating images for entry into AFIS, and can be utilized as a reference.

#### Local AFIS Database (AFIX) Considerations

AFIX Tracker database retains all Boston Police Department arrests and is maintained by the Crime Scene Response Unit. Records uploaded to AFIX Tracker are also added to the MORPHO state database. The LPU prefers searching in the MORPHO state database due to the higher number of identifications made through this system. AFIX Tracker is only used minimally at the discretion of the Criminalist.

The AFIX database retains all the search criteria listed above as well as the candidate list(s) generated. This information will be maintained by the database for retrieval if needed. The reference manual for the AFIX database can be found on the SAN.

#### State and Federal Databases (MORPHO) Considerations

The State MORPHO database retains Massachusetts criminal and civilian records and is maintained by the Massachusetts State Police. The State MORPHO AFIS system allows the LPU to gain access to the Federal Database. The Federal database retains US criminal and civilian records and is maintained by the Federal Bureau of Investigation.

Latent prints searched can be added to the unsolved latent database at the Criminalists discretion. The candidate list(s) generated should be captured and stored on the SAN.

Detailed procedures for MorphoTrak can be found in the AFIS workflow guide to include entry of latent prints and obtaining exemplar cards. The reference manual for the MORPHO database can be found on the SAN.

#### Documentation

Local (AFIX), State (MORPHO), and Federal (IAFIS) searches will be documented with the date searched. Unique search numbers may be added for each latent searched in the system. A calibrated/cropped latent image for AFIS databases may be stored on the SAN in the appropriate incident number folder.

#### Notifications

A report of results will be completed for all searches against the database. AFIS searches where no hit has been made will not fall under the verification process. In some circumstances, upon verification of a hit performed by a trained and qualified Criminalist, a verbal or written notification of the results can be disseminated to the Customer prior to the final report. This will be documented in the case record.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 73 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

## 7. STORAGE AREA NETWORK (SAN)/DIGITAL IMAGING

### 7.1 STORAGE AREA NETWORK (SAN)

The SAN will be comprised of folders created for incident numbers related to requests. Sub-folders are dependent on the case and work product produced. The following are possible sub-folders that may exist:

Documents – could be created upon initial contact regarding a case. Contact logs could be created within this folder. An AFIS folder may be created if needed for the case.

Overalls – storage for documentation photographs.

Virtual Folders – storage for all latent print images (except for photos taken of latent lifts).

Latent lifts – storage for overalls and latent images from lifts.

CD images – storage for images submitted on a CD.

Analysis – storage for Criminalist work product.

Verification/Blind Verification – storage for Verifier's work product.

Completed reports, examination checklists, and case correspondence will be saved in LIMS under the incident number. The SAN is maintained and routinely backed-up by the Information Systems Group (ISG).

### 7.2 GENERAL DIGITAL IMAGE CAPTURE

Items of evidence and friction ridge impressions should be documented through photography. Images of friction ridge impressions are captured when, in the opinion of the Criminalist, they may have sufficient ridge detail for comparison purposes.

In the course of latent print processing, other forms of evidence may be required to be photographed. The Criminalist should contact the appropriate unit to capture said evidence.

Each Criminalist is responsible for the capture, transfer, storage, retrieval, archiving and documentation of digital photographs taken in their assigned cases. Image capture devices should be capable of rendering an accurate representation of the item of evidence.

#### Quality Assurance

Prior to use for casework, the Criminalist should check the digital equipment settings for proper performance. All capture equipment operation manuals will be maintained in the unit and should be readily available.

Images should be reviewed to check for the quality of capture prior to the completion/packaging of the evidence. Original images will be stored and maintained in an unaltered state in their native format. No digital image shall be deleted once it has been captured. Note: All images that are locked are automatically opened as copies. No changes are made to original images and copies of the photos are always made. All images are captured in JPEG format.

#### Camera Capture

##### Overall Images

Overall images are primarily used for documentation purposes and are not considered evidence. Criminalists may use overall images to document item packaging as well as unique characteristics of items (i.e., serial numbers).

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 74 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

### Latent Print Images

Latent Print images are examination quality photographs and are considered evidence. It is recommended to take a location photo of the item with the latent prints labeled in order to document their position and orientation.

### Latent Lift Images

Overalls and/or latent prints present on lifts should be photographed. These images are not considered evidence. The lifts are tracked as evidence and the photos are duplications of the ridge detail present.

### **Scanner Capture**

The flatbed scanner may be used for the capturing of known prints. The Criminalist should use the following settings when scanning:

- JPEG format
- Examination images: Minimum 1000ppi / recommended 1200ppi
- Documentation images: Minimum 300ppi

### **7.3 IMAGE DOWNLOAD**

Adobe Bridge Downloader or direct transfer from a photo card may be used to download images. Images are downloaded to the SAN in the appropriate incident number folder. All photo uploads should be completed as soon as possible after processing is completed for the case(s). In the event that downloading is not immediate, refer to the Forensic Division Evidence Manual section 15: Evidence Handling and Storage .

### Metadata

The following metadata will be applied to all images using Adobe Bridge.

- Title: Incident Number
- Keywords: Case Number
- Description: Description of what the image represents
  - Nanometers (nm)/filter should be added here or in notes when latent prints are recovered
- Author: Criminalist
- Copyright: Latent Print Unit (or equivalent)

### **7.4 IMAGE PROCESSING**

The aim of any digital enhancement is to improve the visualization (quality) of the image without adding or removing features that were not present when the image was captured.

The LPU uses Adobe Photoshop for processing, analysis, and enhancement of digital images. Basic image processing techniques can be performed for both overall images and latent print images. These techniques could include but are not limited to the following: brightness and contrast, levels, dodging and burning, resizing, cropping, inversion, rotation, conversion to grayscale, white balance, image sharpening and blurring, and the Clear-ID extension. Adobe Photoshop History Log tracks the images processing techniques performed by the Criminalist and should always be active.

### **7.5 WORKFLOW FOR DIGITAL IMAGES**

#### **Format the Memory Card**

It is recommended to format the memory card in the digital camera before each use. No formatting should be completed until all previous pictures have been saved to the SAN.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 75 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

### Recommended Camera Settings

Overall photographs: Aperture priority and F>8 (for higher depth of clarity)

Latent Prints (Evidence): Manual mode and F>16 (higher depth of clarity)

### Photographing Latent Evidence

Every attempt will be made to fill the frame with the impression and take photos as close to a 90-degree angle as possible. Photographic and lighting techniques are used to maximize the quality of ridge detail captured. A scale (minimum 1cm) will be incorporated in the image as a reference for measurement.

#### *Special Circumstances:*

1. Curved or Irregular Surfaces
  - a. Scale should be kept flat where the ridge detail is in focus (highest level of the latent)
    - i. If the latent cannot be captured at 90 degrees a photo with an L shaped or ABFO scale can be taken
  - b. Multiple photos of the ridge detail can be taken by rotating the item on the same plane
  - c. If an item is rotated an overlay of the ridge detail should be in focus
2. Transparent Surfaces
  - a. If it is known what side of the item the ridge detail is located, a photograph should be taken from the same side
  - b. If it is unknown what side of the item the ridge detail is located, a note will be made on which side the ridge detail was photographed from and that the ridge detail may be horizontally flipped

### Using Digital Images for ACE-V

When conducting ACE-V the following images may be created:

Processed images (grayscale): Latent images processed in Photoshop and/or with the Clear-ID extension

Analysis images: Latent images that contain analysis annotations and are created before comparison images

Comparison images: Images that contain annotations that were made when conducting a comparison between a latent and known exemplar

Known images: Exemplar impressions without annotations used with latent prints for comparison

## 8. CASE RECORD AND REPORTS

### Case Records

Case records are defined as the examination documentation, whether handwritten, typed, printed, or digital/electronic, maintained by the Criminalist during the analysis of the submitted items of evidence. For any examination, documentation will be completed in a manner that adequately describes the details of the examination. Documentation of the case records could include the following:

#### Processing/Crime Scene:

- Information pertaining to each item examined for latent prints will be documented in Mideo or the LPU Crime Scene worksheets.
- A description of each piece of evidence, the condition (if relevant), and how it was sealed.
- Type of examination conducted; chemical, physical, or visual and/or any combination.
- All latent prints developed/recovered will be described as to which item it was recovered from.
- If practical, a diagram and/or photograph of the item and location of the latent print will be recorded in the case record.
- The quality control test will be documented in Mideo.
- Results of examination; latent prints recovered and specific item number.
- Notes pages will be numbered.
- Abbreviations included in casework notes should be defined or conform to those included in section 12, if not commonly accepted within the discipline of friction ridge analysis.

#### Comparison:

- Number of latent prints evaluated or recovered per item and/or lift.
- From where the latents were obtained (items and/or lifts).
- Number of AFISable latent prints, specific latent prints searched through the specific AFIS system, and the date of search.
- Name of individual(s) being compared, including an identifier, if applicable, (DOB, FBI #, SID #, BPD-CR #, Booking #, etc.).
- Results of examination (example: identification, exclusion or inconclusive).
- Representation of all latent prints with suitable quality/quantity for identification purposes and exemplar prints.
- Notes pages will be numbered.
- Abbreviations included in casework notes should be defined or conform to those included in section 12, if not commonly accepted within the discipline of friction ridge analysis.

### Reports

The report will be considered finalized after the technical and administrative reviews have been completed. The finalized report date will indicate the completion of testing for the items detailed. The report should address the following information:

- Incident #, Case #, District/Unit/Agency, Date of report
- Type of Crime
- Location of Crime (Crime Scene Processing Reports only)
- Methods Utilized and Activities initiated
- Disposition of the evidence
- Signature(s) of author(s) and signature of reviewer

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 77 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

## Processing Reports

### Evidence Description

The following should be included in the report when describing latent print evidence:

- Description of item(s) being examined
- Item identifier (LIMS #)

### Opinions, Results, and Interpretations

The following information may be included in the results section of the report on a case-by-case basis:

- Latent prints recovered from the item(s)
- No latent prints recovered from the item(s)
- Non-ridge detail impressions recovered from item(s)
- Item(s) not conducive to the recovery of latent prints
- Additional item(s) generated

The written report shall indicate if any items received were not processed, so the requesting customer may ask that any additional work be done.

## Comparison Reports

### Evidence Description

The following information should be among the description included in the report when describing latent print evidence:

- Lifts and/or latent prints being examined
- Number/letter assigned to lift(s) and/or latent print(s)
- Location/evidence the lifts and/or latent prints were recovered from

### Description of Exemplar Prints

- Type of exemplar (TP/PP/MCI's)
- Include an identifier, if applicable, (DOB, FBI #, SID #, BPD CR #, Booking #, etc.)

### Opinion, Results, and Interpretations

The following information may be included in the results section of the report on a case-by-case basis:

- Latent prints suitable for identification purposes
- Latent prints not suitable for identification purposes
- Separately designated areas that could reflect one continuous impression
- One designated area that could reflect two or more distinct impressions
- Possible AFIS quality impressions
- Possible palm or foot impressions
- Negative ridge detail

The completed report shall indicate if **suitable latent prints remain unexamined**, so that the requesting customer may ask that any additional work be done.

### Conclusions

The results of the examination and appropriate conclusions are to be stated in the report. The following conclusions may be used:

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 78 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

**Identification**

*Include the following information:*

- The known impression(s) identified
- The latent number(s)/letter(s)
- Which finger/palm/foot was identified
- Where the latent(s) was/were found

**Exclusion**

*Include the following information:*

- The known impression(s) excluded
- The latent number(s)/letter(s)

**Inconclusive**

*Include the following information:*

- The known impression(s) cannot be identified or excluded
- The latent number(s)/letter(s)

When a comparison result is deemed "Inconclusive", a reason must be documented. Examples of a reason include, but are not limited to:

- The exemplar prints had areas of ridge detail not suitable and/or not recorded at all.
- The information within the latent and the available exemplar prints can neither be identified nor excluded after an exhaustive search.
- A thorough conclusion was made after a comparison of the latent print and known impression.

**Not Suitable for identification purposes**

*Include the following information:*

- The latent number(s)/letter(s) that do not have suitable ridge detail for identification purposes.

**Report Release**

Signed reports are retained in LIMS and a copy of the completed report is made available to the customer(s). The Unit may provide the District Attorney's Office with a copy of an analysis report upon request by the Assistant District Attorney assigned to the case.

**Additional Considerations**

Examination results are limited to conclusions accepted within the latent print discipline.

The absence of impressions on any surface does not indicate lack of contact or deliberate destruction of transferred residues.

No current scientific method exists which permits a determination of the time interval between deposit and development by examination of a latent print impression.

No current scientific method exists which permits a determination of the age, race, or gender of a person from an analysis of a latent print impression.

Suitability determination is a human endeavor. Variances in a Criminalist's conclusions of suitability may occur due to normal human factors.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 79 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

Examinations or comparisons are equally dependent upon the quality of the latent and known impressions.

Within each category of exemplar prints is a full range of quality from clear, legible reproductions to smeared, indistinct or incomplete transfers of friction ridge formations.

While the experience of any Criminalist may provide an intuitive reaction which leads to an opinion about the above, unknown factors, the vast realm of exception, and the lack of scientific demonstration prohibit any reporting of such indications.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 80 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	



## **9. CASE REVIEW**

A technical and administrative review of every case will be performed. This activity will be maintained in the case record. The administrative and technical reviewer may be the same person and may sign the report as a reviewer.

When the original and reviewing Criminalists are not available for testimony and a third Criminalist will be offering testimony for the case, a technical and administrative review will be conducted by the third Criminalist. The review form will be maintained as noted above.

### ***Technical Review***

A technical review of a case is a review of examination documentation, data and other documents which form the basis for a conclusion.

If a discrepancy is found by the technical reviewer, the originating Criminalist will be notified. Regardless of whether or not an agreement is reached, a Criminalist IV or Director will be notified.

### ***Administrative Review***

An administrative review of a case consists of checking format, grammar, spelling, sentence and paragraph construction, and overall readability. The reviewer also confirms that all other administrative and examination records are uniquely identified with the case number and/or i/CC#.

The reviewing Criminalist will notify the originating Criminalist of any corrections.

### **Additional Considerations**

Various points to be considered while reviewing case records include:

- Have all reasonable questions in the evidence examination been addressed?
- Are there any additional questions, which may be pertinent and should be answered?
- Are all technical documents of a permanent nature and free of obliterations and erasures?
- The reviewer may view actual evidence if they believe it is necessary to complete this review.

### **Worksheet & Report Changes**

Any changes made to notes post-technical and administrative review will be tracked in Mideo and may be captured in LIMS within case correspondence.

Amended reports will indicate, at the beginning, the reason behind a change and the correction will be highlighted within the report.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 81 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

## 10. DISCOVERY REQUESTS

### Requests

All requests received for discovery material must be from the customer, Investigator, and/or District Attorney's Office. The discovery request should include the CC #/I # and the name of the requestor. The originating Criminalist(s) should be notified of the request. The Unit requests at least 30 days' notice to fulfill all discovery requests. If a request is received in less than the 30 days due to court compliance, a fulfillment date is required. The Unit will make every effort to meet the date specified, however it is dependent on the case and current priorities of the Unit.

When requests are made for documentation beyond the case record (reports, notes, images, etc.), a Criminalist IV/Director will be notified of the request. It may be necessary to forward such request(s) to the Legal Department prior to release of the information.

The Unit is limited in providing the ranked list of candidate's names generated by the AFIS database(s) per the Massachusetts CORI law. Criminal record information cannot be released. Requests for AFIS candidate list(s) with names must be forwarded to the Legal Department.

### Packet

All folders stored on the SAN under an Incident # will be copied and added to a CD/DVD for a discovery request. All documentation within LIMS, the case file and/or case record will be added to the CD/DVD for a discovery request to include the Mideo finalized case notes and chain of custody logs for all items submitted to the LPU. Copies of all the images are to be included with the CD/DVD. A discovery release form will be completed for the packet. A date and signature of the individual receiving the packet will be captured on the release form. A copy will be provided with the packet and the original will be added to the case record.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 82 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

## 11. TESTIMONY

Testimony is a responsibility associated with all the positions within the unit. Personnel are frequently summoned to testify in district, municipal, superior, and federal courts. All members of the unit will do their best to accommodate testimony where a summons had not been issued.

Personnel responding to court should be dressed appropriately. They will not only be representing themselves but the unit and department. Additional personnel attending to observe testimony are authorized to appear in typical unit attire.

Testimony for processing and comparison cases will be based on the case record maintained by the unit. Criminalists testifying in processing cases should familiarize themselves with the most recent unit statistics regarding latent print recovery from firearms. The statistics can be found on the LPU SAN.

Criminalists testifying in comparison cases will not testify to a zero error rate, 100% certainty, or the 'exclusion of all others'. Testimony is an opinion based on the work product that supports the conclusions reported.

Criminalists are permitted to bring original case files to court. In the event an original document is requested as an exhibit and a scanned copy is not already on the SAN, a request for a copy should be made and added to the case file prior to departure from court.

ID: LPU-SOP	Approval Date: 6-3-2022	Revision # 2022.0 - Effective date: 6-13-2022	Page 83 of 88
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

## 12. ABBREVIATIONS & TERMS

Abbreviation/Term	Definition
→	Moving to next processing step (processing worksheets)
/	Results (processing/comparison worksheets)
^	Add above
A	Arch or Analysis: the assessment of a friction ridge impression to determine suitability for identification
AB	Amido Black
ADA	Assistant District Attorney
AFIS	Automated Fingerprint Identification System
ALS	Alternate Light Source
ANAB	ANSI-ASQ National Accreditation Board
ANSI	American National Standards Institute, owner of ANAB
AR	Accreditation Requirements (AR3125)
ASB	Academy Standards Board
ASCLD	American Society of Crime Laboratory Directors
ASCLD/LAB	American Society of Crime Laboratory Directors/Laboratory Accreditation Board
ASQ	American Society for Quality
ASTM International	American Society for Testing and Materials
AX	Ardrox
AY	Acid Yellow
BFS	Bureau of Field Services
BIS	Bureau of Investigative Services
BPD	Boston Police Department
BRIC	Boston Regional Intelligence Center
C, comp.	Comparison: the direct or side-by-side observation of friction ridge detail to determine whether the detail in two impressions is in agreement based upon similarity, sequence and spatial relationship
CC#	Central Complaint Number
Chemically	Processing methods to include, but not limited to, superglue fuming, dye staining, and/or blood enhancements
CJIS	Criminal Justice Information Services Division
CLU	Crime Laboratory Unit
CPR	Subject Photo Request (FBI)
Crim	Criminalist
CR#	Criminal Record number
CSRU	Crime Scene Response Unit
D	Digital
DCU	Drug Control Unit
DFO	1,8 Diazfluoren-9-one
DOA	Date of Arrest, referencing ten print cards
E	Evaluation: the formulation of a conclusion based upon analysis and comparison of friction ridge impressions
ECU	Evidence Control Unit
Elim	Elimination Prints
ET	Evidence Tracker
EVI	Evidence number in RMS

Excl, EX	Exclusion, Exclude
EXH	Exhaustive comparison
Exp.	Expires
Ext.	Exterior
FA, F/A	Firearm
FAS	Firearms Analysis Section
FAU	Firearms Analysis Unit
Federal	Federal IAFIS
FG/FD	Forensic Group/Forensic Division
FP	Finger Print
FSSB	Forensic Science Standards Board
FWD	Item forwarded
H	Hit (Mideo)
HR	Hungarian Red
I#	Incident number
IAI	International Association for Identification
IAFIS	Integrated Automated Fingerprint Identification System
IAPE	International Association for Property and Evidence
ID, Id, IDENT	Identification
IDF	Iodine Fuming
IDU	Identification Unit
IEC	International Electrotechnical Commission (ISO/IEC)
ILAC	International Laboratory Accreditation Cooperation
INC, Inc	Inconclusive
IND	1,2-Indanedione
Init.	Initials
Int.	Interior
IRD	Insufficient ridge detail
IRQ	Image Request Submission (FBI)
ISG	Information Services Group
ISO	International Organization for Standardization (ISO/IEC)
KP	Known prints
L	Loop/Left
L#	Latent lift latent number
L1	Level one
L2	Level two
L3	Level three
LAT #	Latent Print Section/Unit Case Number
LCV	Leucocrystal violet
LFFS	Latent Fingerprint Feature Search (FBI)
LFIS	Latent Fingerprint Image Search (FBI)
LI	Left Index
LIMS	Laboratory Information Management System

LL	Left Little
LM	Left Middle
Local	Local AFIX database
LOV	Latent of value
LP	Left Palm
LPS	Latent Print Section
LPU	Latent Print Unit
LR	Left Ring
LT	Left Thumb
Mag	Magnetic
MCI	Major Case Impressions
Msg	Message (Mideo)
MSP	Massachusetts State Police
MSPCL	Massachusetts State Police Crime Laboratory
MVC	Mason Vactron Chamber
NAS	National Academy of Science
NCFS	National Commission on Forensic Science (Expired 4-23-17)
NC	Not compared – Mideo
NEDIAI	New England Division of the International Association for Identification
NEG RD	Negative Ridge Detail
NH	No Hit (Mideo)
NIN, Nin	Ninhydrin
NIN-HT	Ninhydrin for Heat Transfer paper
NIST	National Institute of Standards And Technology
NR	No Reaction
NRC	National Research Council
NS	Not suitable
NSC	Not Sufficient for Capture; Not Suitable for Capture
OBTN	Occasion Based Tracking Number
OSAC's	Organization for Scientific Area Committees
P	Processing
Pass	Passenger
PC	Polycyano
PCAST	The President's Council of Advisors on Science and Technology
PCU	Physical Comparison Unit
P#	Processing latent number
PHL	Photo Lab
Physically	Processing methods to include, but not limited to, various types of fingerprint powders
PICS	Personnel Identification System
PM	Post mortem impressions
POW	Powders
PP	Palm prints
ppi	Pixels per inch

Prev.	Previous/previously
PT	Proficiency Testing
Q/Q	Quantity/Quality
QA	Quality Assurance
QC	Quality Control
R	Right
RD	Ridge Detail
Reg	Regular/Regular powder
RH6G	Rhodamine 6G
RBS	Reddish Brown Stain
rec'd, rec	Received
Rep	Representative
Rev'd	Reviewed
RI	Right Index
RICI	Repository for Integrated Criminalistic Imaging System
RL	Right Little
RM	Right Middle
RO	Release to Officer
RP	Right Palm
RPT	Report
RR	Right Ring
RT	Right Thumb
S	Search (AFIS)/Suitable
SAN	Latent Print Unit Storage Area Network
SAU, SA	Sexual Assault Unit/ Sexual Assault
SCDAO	Suffolk County District Attorney's Office
SDO	Standards Development Organization
SID#	State Identification Number
SIM	Inconclusive with similarities
SG	Super Glue
SN/S#	Serial Number
SPR	Small Particle Reagent
SSA	5-Sulfosalicylic Acid
State	State MORPHO database
Suff.	Sufficient
SWGFAST	Scientific Working Group on Friction Ridge Analysis, Study, and Technology
TLI	Ten print to Latent Inquiry
TCN#	Transaction Control Number
TCR#	Transaction Control Reference
TP	Ten Prints
ULD	Unsolved Latent Delete Request (FBI)
ULM	Unsolved Latent Match (FBI)
ULW	Universal Latent Workstation

V/Ver	Verification: The independent application of the ACE process is utilized by a subsequent examiner to either support or refute the conclusions of the original examiner
VF/v.folder	Virtual folder
Vis, vis	Visual
Visually	Examination with various types of light
VMD	Vacuum Metal Deposition
W	Whorl
WW	Wetwop
x, X	Times/ Crime Scene Report





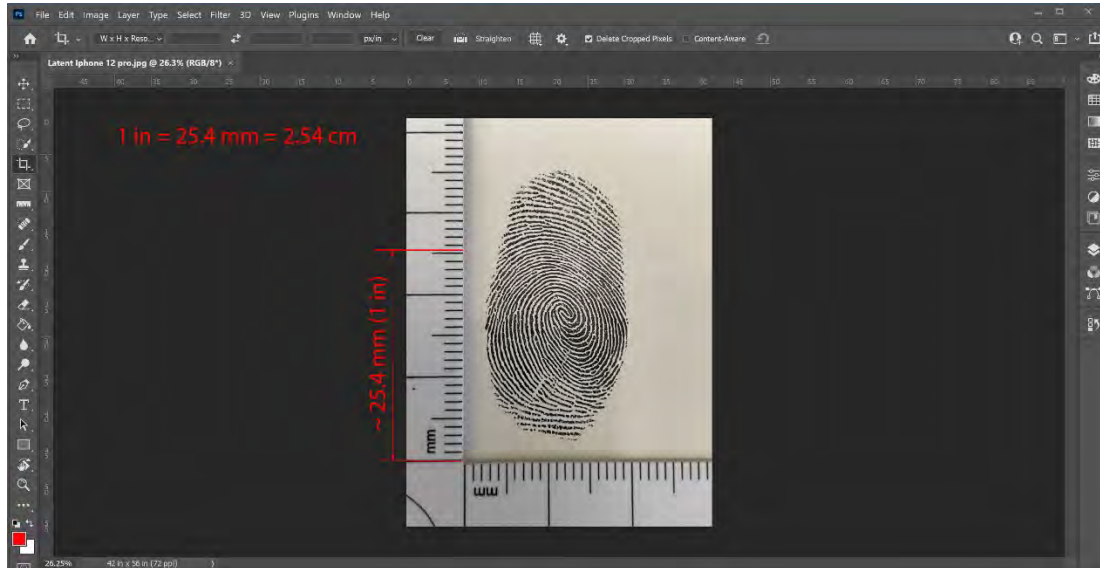
## **AFIS Workflow Guide**

This document will provide workflow guidance for using the Automated Fingerprint Identification System (AFIS).

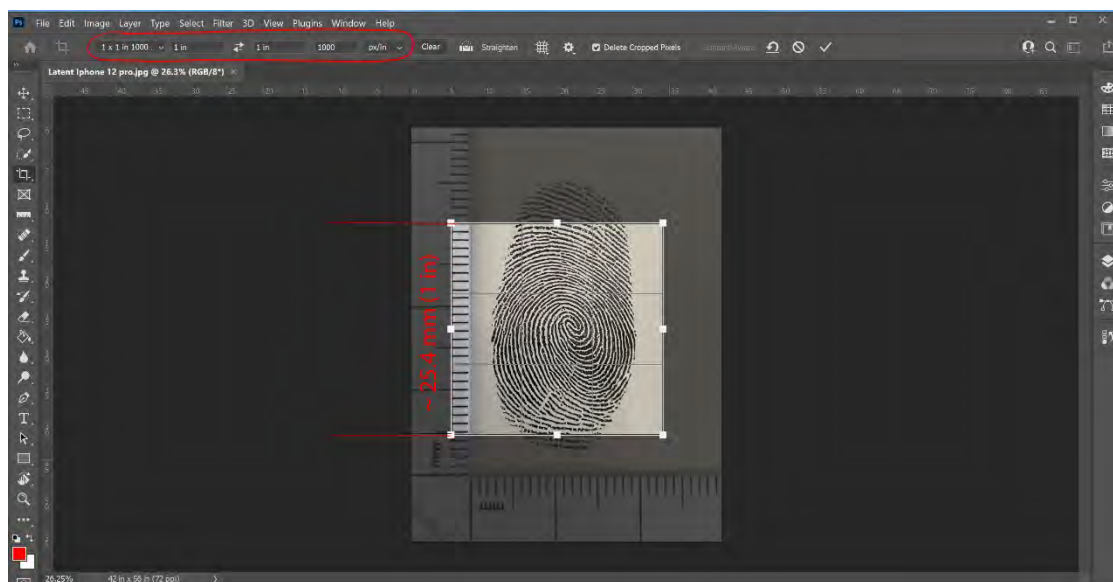
## **CALIBRATION**

Latent print images that are launched for searches in AFIS must be calibrated 1:1. Criminalists may follow, but are not limited to, the two techniques outlined below:

### *Technique One*



- If you have a latent image with a scale showing at least one inch (25.4 mm or 2.54 cm), you can crop it, with the crop tool, in one step using the preset (1 in x 1 in x 1000ppi); . your image is now ready for AFIS. If the scale is less than one inch, then go to Technique Two.



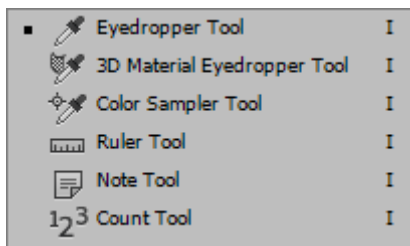
*\*This method can be used for palm prints using a crop preset (2 in x 2 in x 1000ppi) if the scale has at least 2 inches (50.8 mm or 5.08 cm).*

ID: LPU-AFIS	Approval Date: 5/2/2022	Revision # 2022.0 - Effective date: 5/2/2022	Page 2 of 19
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

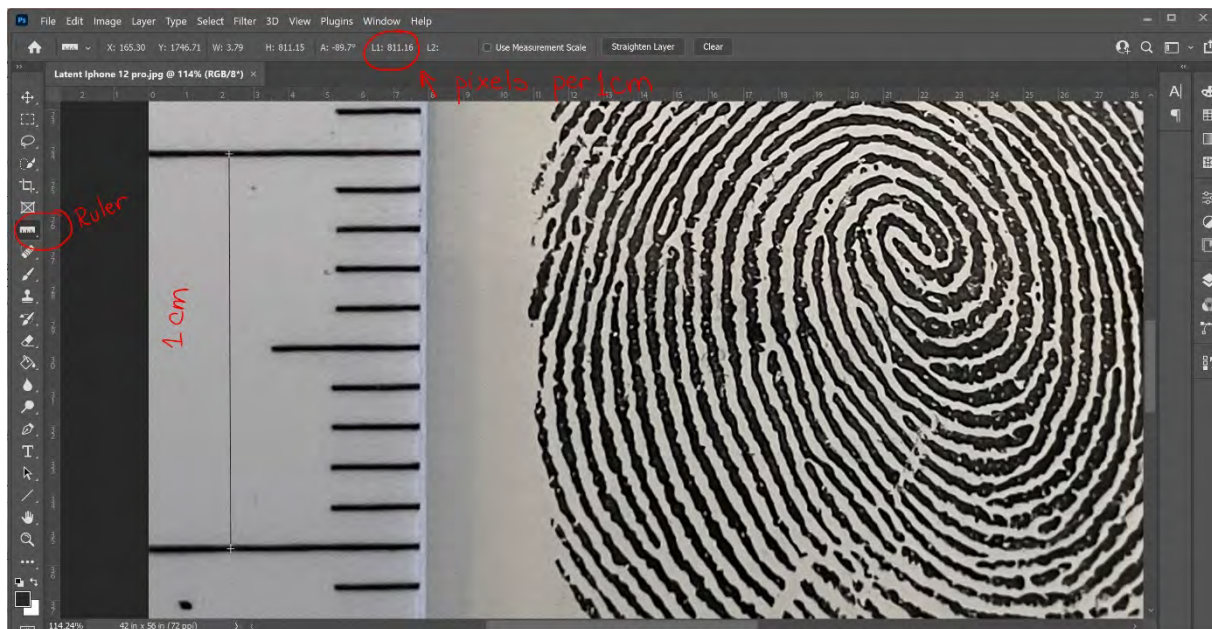
## Technique Two



- On the left side tool bar there is an eye dropper tool; click on this tool and a menu will pop up:



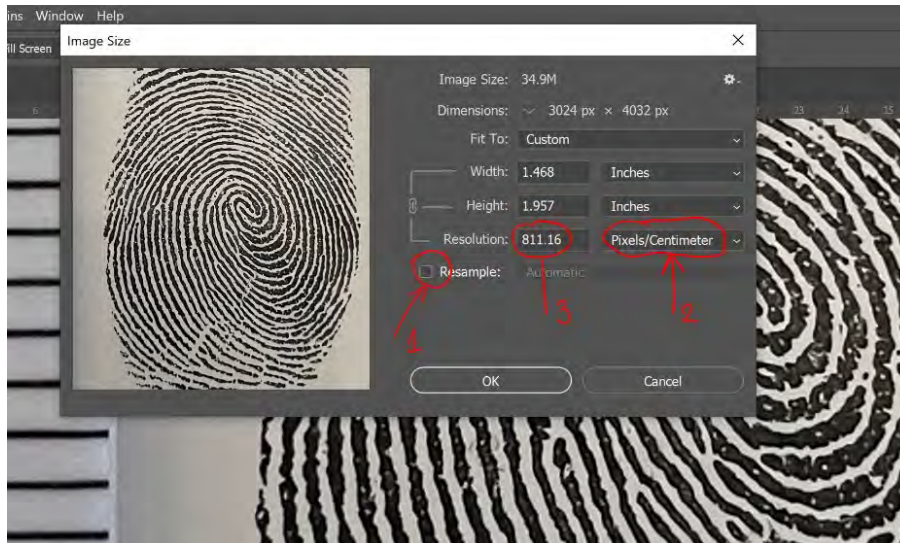
- Select the ruler tool. Measure out 1 cm. A number will appear on the top tool bar "L1" value showing the number of pixels per one centimeter (cm).



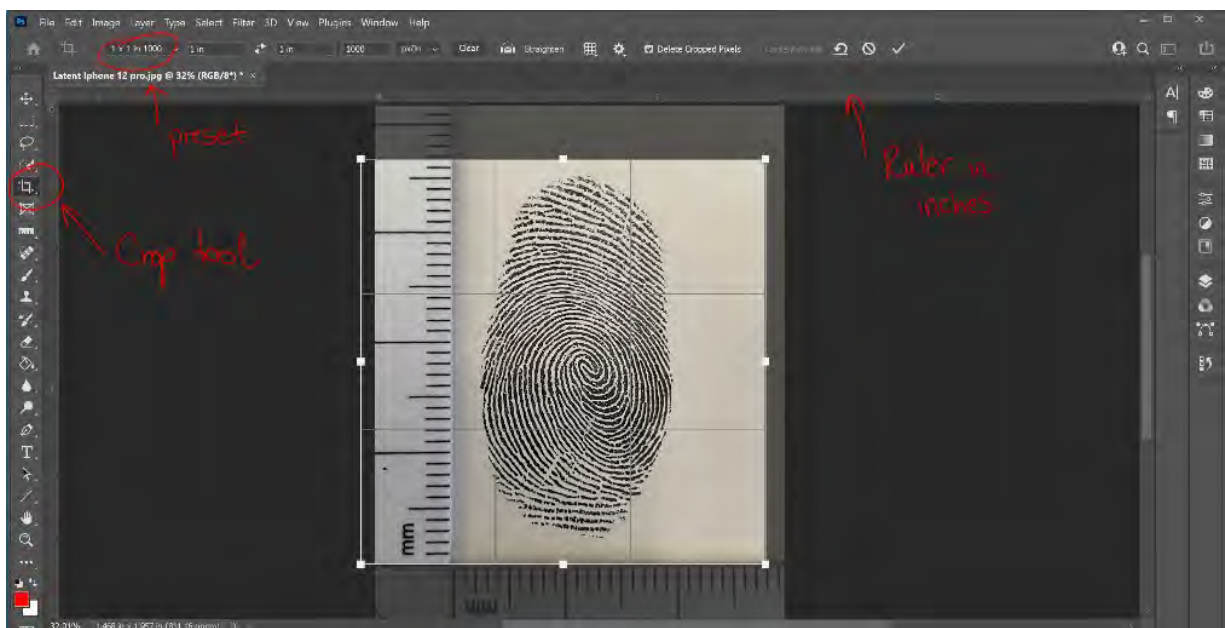


## Technique Two Continued

- Copy the number listed, in the example this number is 811.16. On the top of the tool bar in Photoshop click on Image, then on Image Size. The following box will appear:

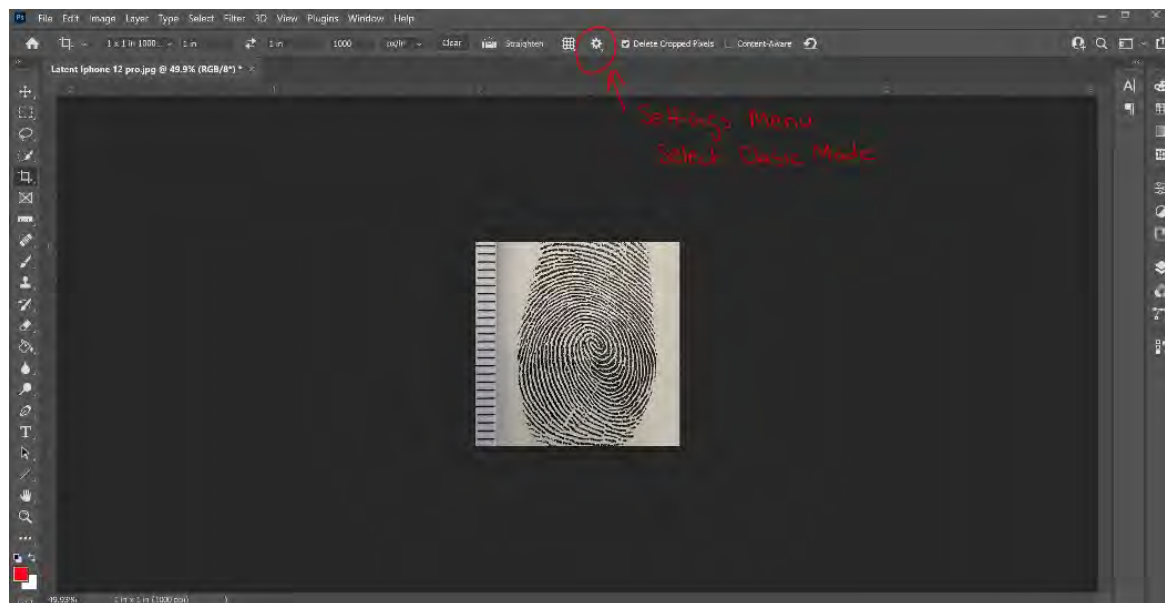


1. Make sure the resample image is NOT checked.
2. Change resolution box to Pixels/centimeter.
3. Place number (L1 value) into the box and Hit "OK".



- A preset of 1 in. W x 1 in. H x 1000 ppi can be set.
- On the left side tool bar there is a crop tool. Use the preset listed above and a grid will appear over the latent image.

- Make sure the ruler appears at the top of your workspace and is showing inches (you can check the ruler by right clicking on the ruler). The box can then be measured to 1:1 by dragging the small gray boxes using the ruler.
- Move the entire crop box (be sure the setting is set for Classic Mode to fit over the ridge detail you would like captured for AFIS entry). Crop that area. You should see the image decrease in size as shown below:

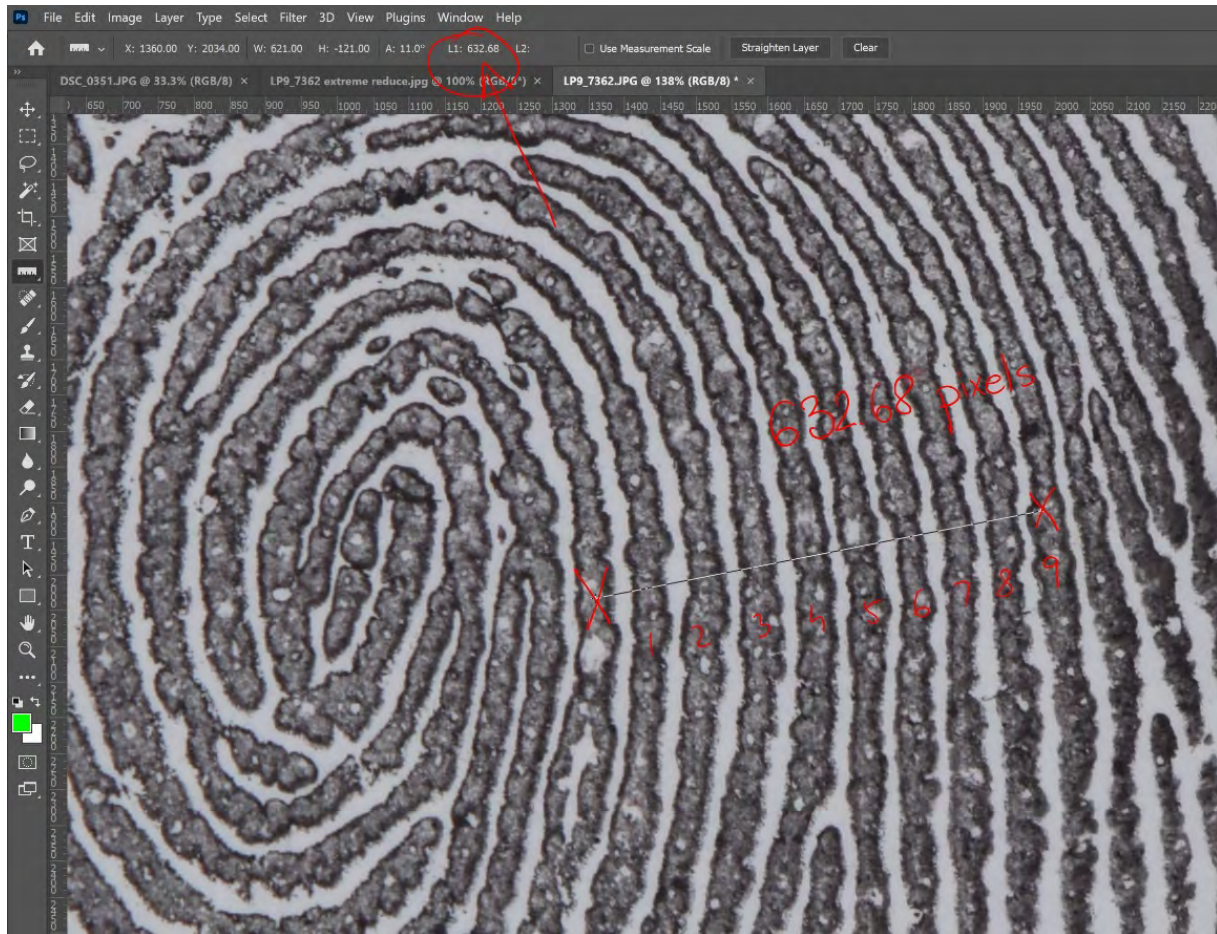


- Save the image at this time. You can always print the image to verify the calibration with a ruler before entry into AFIS.

## Calibrating in Photoshop (No scale)

1. Open an image in Photoshop
2. Put the ruler tool in pixels as measurement
3. Measure out approximately 9 ridges (as perpendicular as possible) by selecting the ruler from the tool bar in an area with no compressed or extended ridges. See image below:

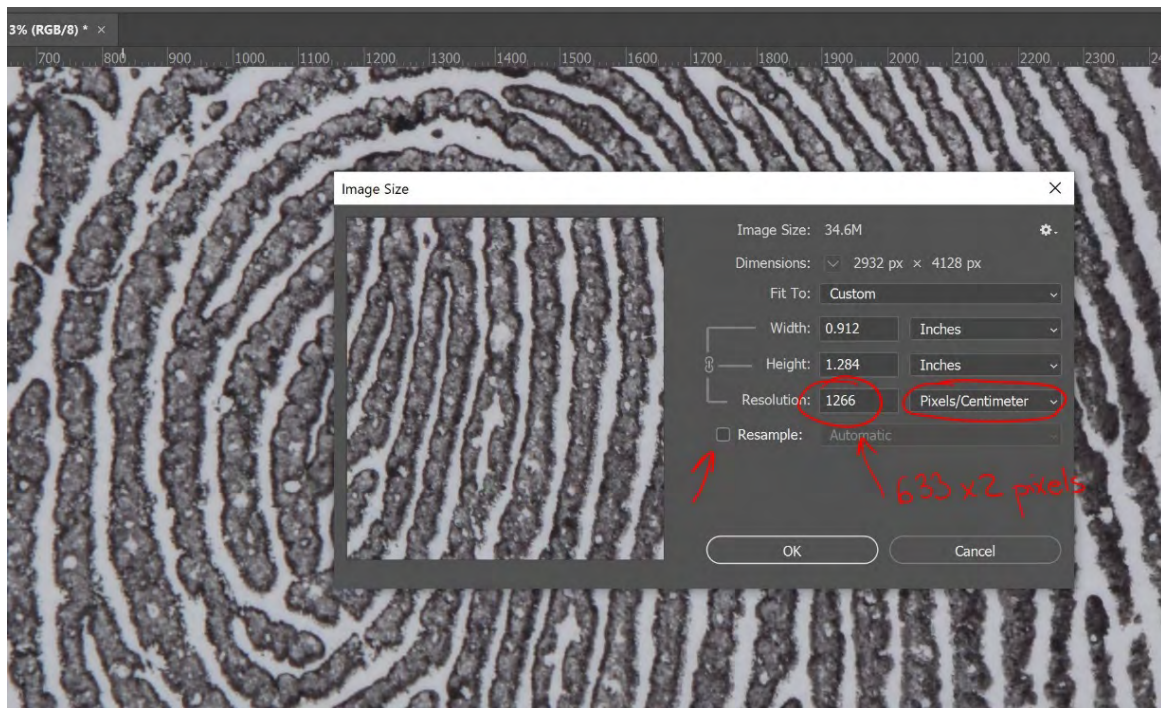
ID: LPU-AFIS	Approval Date: 5/2/2022	Revision # 2022.0 - Effective date: 5/2/2022	Page 5 of 19
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	



4. Example above: 9 ridges = ~633 pixels (L1 value) = ~0.5 cm so  $633 \times 2 = 1266$  Pixels equal ~1 cm

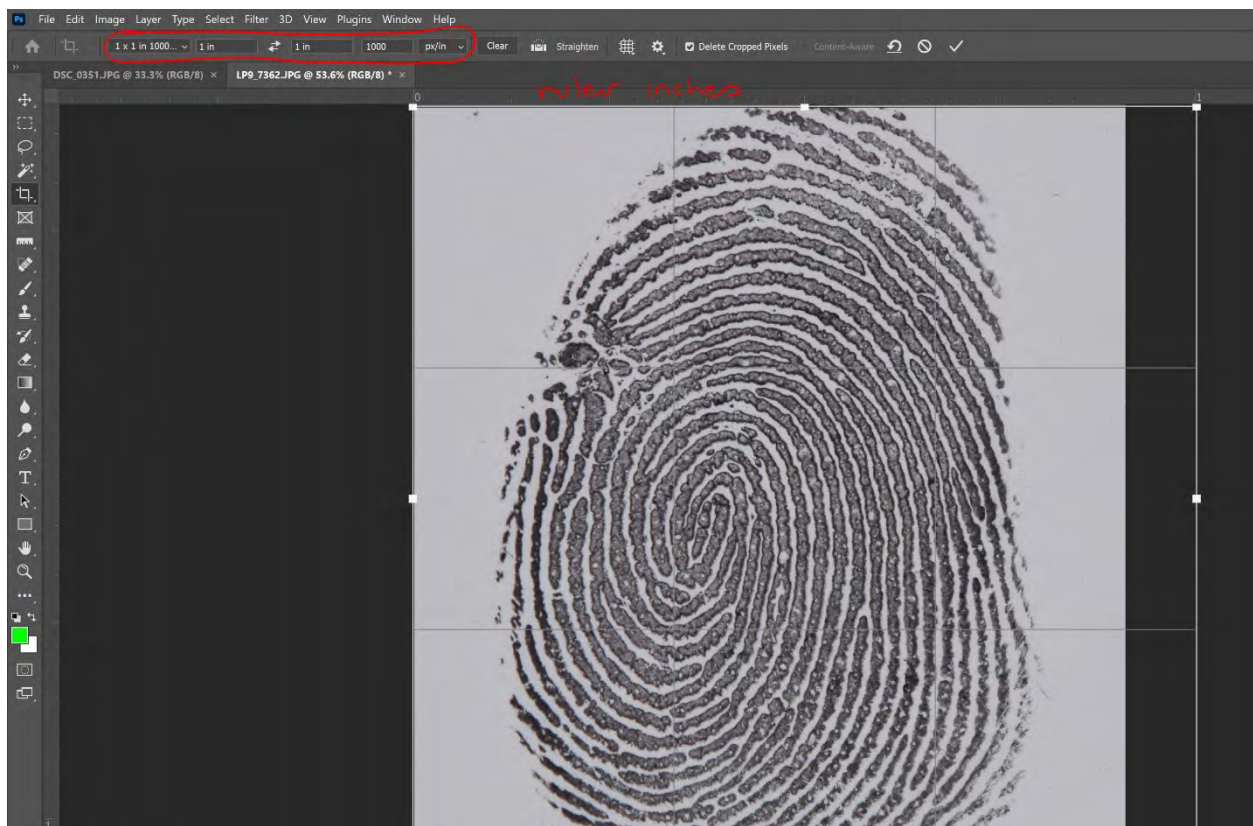
5. Image size: select Pixels/Centimeter and enter 1266. Leave Resample box unchecked.





6. Change ruler to inches

7. Use preset 1 in x 1 in x 1000ppi and adjust the box to the correct size on the ruler.



The image is an approximate calibration, and it can be increased or decreased in size with +/- 10% to perform additional searches if needed.

To increase the size 10%, add 126 pixels to 1266 resulting in 1392 pixels that need to be added in the image size to calibrate

To decrease the size 10%, subtract 126 pixels from 1266 resulting in 1140 pixels that need to be subtracted in the image size to calibrate.

## **AFIX Tracker (Local)**

When utilized at the Criminalist's discretion, the following steps are completed:

1. Open the AFIX tracker app from AFIX6 or AFIX7 computers
2. Click on the Crime Scene tab and select "Pull # of last records 20" then click OK
3. Select the last empty row and start filling the info of the case in starting with "Case Number"
4. Click on the "Latents" tab and then on the "Image Wizard" tab on the next window
5. Select "Latent Image File" from the pop-up window; change Import scale to 1000ppi and click Next
6. Select "Default Latent" from the description and click Next
7. Browse for your calibrated latent, select it and click Next
8. From the "Tools" bar select "Smart Extraction"
9. Click on the green check mark on the bottom
10. Select "Search Wizard" from the top bar
11. Local search will be selected by default. Click Next
12. Select the databases that will be searched (ten prints, palm prints, unsolved latents, and the number or returned candidates) and click Finish
13. To check the results, select "Search Results"
14. Check all candidates and mark the decision on each one by right clicking on the name

## **MORPHO (State & Federal)**

### *Passwords*

Morpho passwords are required to be changed every 3 months and can only be changed on the main terminal. Reminders can be set on calendars 2-3 days prior to expiration to ensure you are not locked out of the system. If you become locked out prior to changing your password, you will need to call the Morpho technician assigned at the MA State Police.

Once your password has been updated, the additional Morpho terminals will each need to be updated to allow all applications to open.

### ***Shortcut to the SAN (server) on Morpho (Mass State computer)***

When the Morpho system is rebooted or the password is changed, the possibility exists that the shortcut to the LPU-SAN server could be deleted. Follow the instructions below to reconnect and add the shortcut to the desktop:

ID: LPU-AFIS	Approval Date: 5/2/2022	Revision # 2022.0 - Effective date: 5/2/2022	Page 8 of 19
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	



1. Ensure your password has not expired. If it has expired the following steps may not work.
2. Delete any LPU-SAN server's shortcuts for Morpho.
3. Double click on the computer icon and if there is any mapping of the server in the Network Location, right click on it and then click "Disconnect."
4. Create a new connection by mapping the LPU-SAN server. Right click on the computer icon and select "Map network drive." Select X: from Drive window. Instead of using the Browse function, type the following into the address bar: **\\10.25.16.75\Latent Print Unit** and click finish.
5. A new window should appear asking for username and password. *If this window does not appear then your password has expired and will have to be updated.*
6. Username is **Boston\_police\Your ID** and your own password for windows.
7. Access should be granted to the LPU-SAN server at this point.
8. Creation of a shortcut to the LPU-SAN server can be completed on your desktop.

### *Signing into Morpho Trak:*

Username: [BOS and ID#]

Password: [Upper case, lower case, #]

**Menu Bar** (vertical) on right side of screen ⇨ "Latent"

**Latent Expert** – create case/search latents

**Database Maintenance** – print ten print cards / delete latents from unsolved State Database

**Home Page** – status screen/responses

### **LATENT EXPERT**

Click on "Add" icon to add a case

Add a case panel:

CASE PREFIX: "Boston PD"

CASE NUMBER: [13XXXX without hyphen]

LATENT CASE AGENCY: "Boston PD"

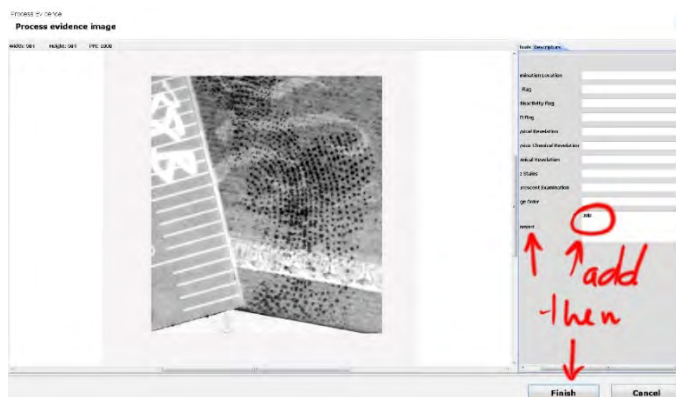
DATE OF CASE: date of incident

CRIME TYPE: select from drop down list

CASE IDENTIFIER: Last name, First name (no space after comma)

Click on the "Add new evidence from file" icon (try to limit to a max 30 latents per case to reduce lag time). If there are more than 30 latents you can create a new case with same name (ex. 219999a, 219999b, 219999c)

- Latent image opens ⇨ add latent name into description (1A) ⇨ "FINISH"
- Options to rotate and make additional adjustments to an image, but if previously done in Photoshop, go straight to "FINISH"



A new screen will open



↳ Add latent (4<sup>th</sup> box in top row)  
- Size box & double click

red=finger purple=palm

A new screen will open



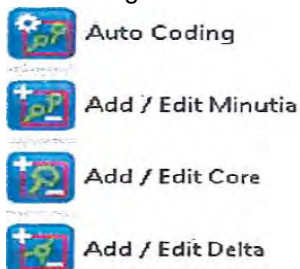
↳ "Create Area"

red=encoding will be outside of selected area  
green=encoding will be inside the selected area

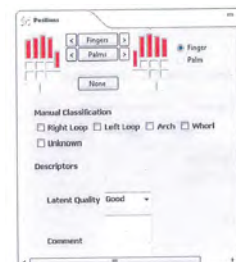
This step is optional. Use it only when you need a specific area to be encoded. (ex. Distortion, multiple impressions, etc.)



↳ Commonly used options for editing minutiae:



Additional tools are available for encoding



Positions Area

When Encoding and Positions Areas are complete ⇨ "SEARCHES" (double click)

A new screen will open

ADD TO LATENT DATABASE: "YES" is automatically selected or can select "NO"

ORIENTATION RANGE: "VERTICAL" (~ 45 degree rotation both ways) is automatically selected or can select "ANY" (full 360 degree)

- ☒ Person (LT/TP – LP/PP) – this will search State ten print and palm print cards
- ☒ FBI LFFS (searches done after State has no hits)

ID: LPU-AFIS	Approval Date: 5/2/2022	Revision # 2022.0 - Effective date: 5/2/2022	Page 10 of 19
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

- ☒ Choose the latent(s) you want to search

↳ "SUBMIT"

**Note:** IF the latent is a joint, the search should be done in the FBI database. State Morpho does not search the joints and upper palms.

### Searching "Copy a Latent With Encodings"

Latent Expert ⇒ select your case

- ↳ Click on circle next to "Case Latents" ⇒ select latent to search (e.g. 001-01-01)
  - Select "Copy Latent with Encodings" on left side menu
    - A message window will pop up ⇒ select "OK"
  - Create an additional copy and open latent
    - Can now change parameters (fingers, palms, pattern type)
    - Can add/delete encodings
- ↳ double click "Searches"
  - The copied latent should appear (e.g. 001-02-01)

*Follow the directions directly above to search latent in State and/or Federal database(s)*

### HOME PAGE

FILTER RESULTS

ID: "BOS"

USER: "ID#"

Conclusions: 1. IDENT 2. NON IDENT 3. NO DECISION

Make sure to save the candidate list by saving SEARCH RPT to the appropriate AFIS folder on the server.

The report must be saved after checking off at least one conclusion and before closing screen.

After entering in conclusions ⇒ "SAVE"

**\*\*If there is a possible IDENT, it is easier to print or save the card from the HOME PAGE\*\***

### Printing the ten print card with the possible hit:

Right click on SID# ⇒ "View Case" (DATABASE MAINTENANCE screen will open)

Click on "Print Tenprint" (vertical menu bar on left side of screen)

CARD FORM...: [change to "StateCriminal.fmt"](#)

### Saving the ten print card as a PDF:

PRINTER: [PDF writer](#)

- ↳ "Print" (automatically saves to "Pdf" folder on server)
  - Rename and move to examiner folder

### Saving a finger/palm as a JPG image (recommended):

- Right click on the comparison screen or double click on finger image on the ten print screen.
- Right click ⇒ Export image ⇒ Rename ⇒ Save to appropriate file
  - ↳ Open in Photoshop
    - Change image size to 2500ppi
    - Resample must be on to make the resolution approx. the same in latent and known.

### **DATABASE MAINTENANCE**

RECORD TYPE: Criminal

Enter in any of the following information to search for a card:

SID/CID: MAXXXXXXXX (8 digit #)

LAST NAME

FIRST NAME

↳ "Search"

Under **Tenprint Search Results** ⇒ select the criminal record ⇒ "Open" \*\*Opens the COMPOSITE\*\*

- select the card you want from the drop-down list
- follow directions under **HOME PAGE** to save as a PDF

**Printing Civilian/Applicant cards** (Searchable only by AFIS Section criminalists, available based on request for the remaining examiners)

RECORD TYPE: Applicant

Enter in any of the following information to search for card:

SID/CID: MACXXXXXXX (7 digit #)

\*Searches can be done based on demographic info, for the applicants as well.

### **Saving the ten print card as a PDF:**

PRINTER: PDF writer

↳ "Print" (automatically saves to "Pdf" folder on server)

- Select State Applicant card
- Rename and move to examiner folder

### **FBI ten print cards**

Menu Bar ⇒ "Latent" ⇒ IRQ-CPR

*"IRQ Display" and "Type-2 Descriptors" tabs should be selected*

Enter in the following information:

FBI Number: XXX...

↳ Click on OK

Attention Indicator: **NAME OF CRIMINALIST (ex. SMITH,JOHN)**

↳ Click on Submit

Open Database Maintenance

*Find Tenprint tab" should be selected*

Enter FBI # (scroll down the page) ⇒ click on "Search"

↳ select the card you want

↳ double click your selection or click on "open"

A new screen will open displaying the ten prints

Follow directions under Home page to print and/or save as PDF

- CARD FORM...: **change to "FBI Criminal.fmt"**

If no name is printed on the FBI card, copy the Transaction Control Reference value (numbers and letters) from the Transaction Data tab,

Find: FBI-PWEK3W9TX-32345043 Record Type: FBI

Incident ID : FBI-PWEK3W9TX-32345043

Transaction Data

Type of Transaction: ULMT

Date: 09152021

Transaction Priority:

Destination Agency Identifier: MA0131100

Originating Agency Identifier: WVIAFIS0Z

Transaction Control Number: E202125800000297367

Transaction Control Reference: MTVNS0120210915961071

and paste it into the Transaction Control Number field and search it again. If the card was printed in MA, a SID# MAC# will appear with the name. See below image:

Find Tenprint Find Latent

Date (mmddccyy):

Date Printed (mmddccyy):

Transaction Control Number: MTVNS0120210915961071

Transaction Control Reference:

FBI Civil Record Number:

Valid entries are alphanumeric and special characters 1 to 40 in length.

Tenprint Search Results

ID	Last Name	First Name	Date of Birth	Record Type	FBI Number
FBI-PWEK3W9TX-32345045				FBI	PWEK3W9TX
FBI-PWEK3W9TX-32345043				FBI	PWEK3W9TX
FBI-PWEK3W9TX-32345044				FBI	PWEK3W9TX
FBI-PWEK3W9TX-32345048				FBI	PWEK3W9TX
MAC 1281133	TORRES	DONAS	12091968	APPLICANT	PWEK3W9TX

If there are no results after the search, contact the FBI for the name. See Request Exemplars from CJIS.

### Delete latents from Unsolved State Database (when latent was ID manually, or an FBI Hit):

Follow these steps:

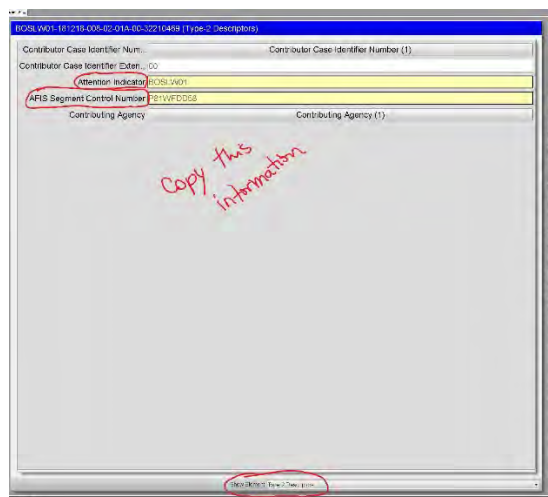
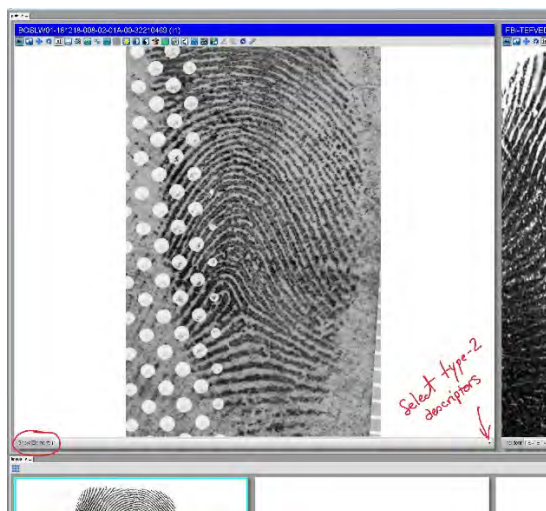
1. Open Database Maintenance.
2. Select "Find Latent" from tabs.
3. Scroll down the window until you see "Latent Case Number."

4. Type the case name "BOSLW01-13XXXX."
5. All latents added into the unsolved database will be listed.
6. Click on the latent that you want to delete.
7. In the left bar there is a "Delete Latent" button. Click on it.
8. Confirm the deletion.
9. Exit window.

**Delete latents from Unsolved Federal Database (only on reverse FBI Hits – AFIS section):**  
Follow these steps:

1. Open ULM Home page and select your search. Select Type-2 Descriptors from the Show Element drop list window (bottom of image).
2. Copy the information from all 5 fields (red circles).

Here is how to get the information from the FBI reverse ULM search (Home page).





3. Open IRQ-CPR app.

4. Select "ULD display" and Type-2 Descriptors from tabs.

5. Fill the following 5 criteria into the empty fields from the Type-2 Descriptor information of FBI reverse search found on ULM -Home page.

- Attention indicator
- AFIS Segment Control Number
- Contributor Case Identifier Number
  - Contributor Case Prefix
  - Contributor Case Identifier
- Contributor Agency
  - CRI1

4. Click submit.

5. Exit window.

6. In your home page, for a successful deletion, you should see your request with an "f-uldr" in "State" tab. If "f-errl" is displayed there was an error in the deletion process.

To check the error "f-errl" double click on it. At the bottom of the window the error message is displayed.

### Closed Searches:

Go to Case

Click on latent to be searched

- Make sure box is highlighted

Copy latent with encodings

Searches

- Do not add to database
- Known/unknown orientation

Have to click Person AND Closed

- Scroll down in box
- Click Add and enter SID# (If multiple SID#'s, have to click Add each time)
- Optional if you want to save the list with multiple SID#s:
  - o Click Export, rename (list knowns) and save to AFIS folder
  - o For additional closed searches you can import the saved list instead of typing all SID#s again

Check latent NOT SEARCHED and then click SUBMIT

Go to Home Page

## **COLD CASE SEARCHES**

The AFIS section has the ability to research unsolved homicide cases that had been previously worked by the LPU and determine if additional searches should be completed in the state and/or federal databases. The AFIS section may assess the latents for various additional and/or new searches (AFIS quality, 360 degree search, additional encodings, additional databases, etc.)

If additional searches are completed, the following procedure should be utilized:

1. If searches were previously conducted, search for and open the case in MORPHO. If no latents were previously searched, create a new case in MORPHO.
2. Open the latent print that will be searched (example: 001-01-01A).
3. Determine if new encoding or search criteria is needed.
4. Open up the search page by double clicking on "search".
5. Select if the latent print will be added to the unsolved database.
6. Select the orientation of the latent print.
7. Enter how many candidates to return (minimum of 3).
8. If searching the state database, check the "Person to Person" box. If searching the federal database, check the "LFFS" box.
9. Select the latent print(s) to be searched.
10. Click on Submit.
11. For pre interface cases, create a milestone in Mideo "New AFIS searches" and fill in the required information
12. Generate worksheets of the searches (AFIS page only) for a search that results in "no hit."
13. Generate all required worksheets if a search results in a "hit."

When a member of the AFIS section determines that a latent is AFISable, and that decision differs from the originating Criminalist, notification will be made with the original Criminalist prior to any searches being conducted.

ID: LPU-AFIS	Approval Date: 5/2/2022	Revision # 2022.0 - Effective date: 5/2/2022	Page 16 of 19
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	



If searches do not generate a “hit,” members of the AFIS section will complete an AFIS no hit search report and have the report reviewed. The AFIS team member will issue the report to the customer as well as alert the original Criminalist that additional searches were completed with “no hit”.

If a “hit” is generated with a candidate, the member of the AFIS section will complete the comparison, generate the notes, and final report. If available, the original Criminalist should be the verifier. When the original Criminalist is unavailable or the AFIS team member is the original Criminalist, an alternate Criminalist will be sent the request for verification. The analytical image of the latent will be the encoded image saved within Morpho.

If a disagreement occurs, the non-consensus decision protocol will be followed.

## **REVERSE SEARCHES**

A reverse search is when a newly entered known impression “hits” to an unsolved latent print image that was added at the time of its search and not identified. The AFIS team have the ability to review the federal reverse searches for BPD cases. Negative reverse searches do not require case note documentation and/or a report.

When a “hit” is made in a reverse search, notification is made to the original examiner on the case.

## **Workflow for reverse FBI hits through MORPHO**

1. Open Home page.
2. In ID field type “BOS”.
3. IN TOT field type “ULM”.

4. A list with all reverse FBI hits will be listed.

Id	Date	User	Hold Op	TOT	RFP	Priority
BOSLW01-140937-001-01-01B-00	3/22/19 11:40 AM	fbi		ULM		6
BOSLW01-160636-002-03-01B	8/18/16 2:50 PM	boe132454		LFPB		7
BOSLW01-160629-001-01-01C-00	1/16/19 9:06 AM	fbi		ULM		6
BOSLW01-160629-001-02-01C-00	1/16/19 9:06 AM	fbi		ULM		6
BOSLW01-160629-001-02-01C-00	4/6/19 11:24 AM	fbi		ULM		6
BOSLW01-160629-001-02-01C-00	3/22/19 3:56 PM	fbi		ULM		6
BOSLW01-160629-001-02-01C-00	2/26/20 1:46 PM	fbi		ULM		6
BOSLW01-160754-001-01-01B-00	2/13/19 7:06 PM	fbi		ULM		6
BOSLW01-160754-001-01-01B-00	2/20/19 12:23 PM	fbi		ULM		6
BOSLW01-160754-001-01-01B-00	4/20/19 4:56 PM	fbi		ULM		6
BOSLW01-160754-001-01-01B-00	9/6/19 6:33 PM	fbi		ULM		6
BOSLW01-160754-001-01-01B-00	1/04/20 10:27 AM	fbi		ULM		6
BOSLW01-160754-001-01-01B-00	7/31/20 11:07 PM	fbi		ULM		6
BOSLW01-160926-008-01-01C-00	2/11/20 6:01 PM	fbi		ULM		6
BOSLW01-161654-002-01-01B-00	1/2/19 11:02 AM	fbi		ULM		6
BOSLW01-162187-001-01-01B-00	11/17/19 9:17 PM	fbi		ULM		6
BOSLW01-162187-001-01-01D-00	11/17/19 9:14 PM	fbi		ULM		6
BOSLW01-162187-003-01-01B-00	11/17/19 9:33 PM	fbi		ULM		6
BOSLW01-162187-006-01-01B-00	11/17/19 6:13 PM	fbi		ULM		6
BOSLW01-162187-006-01-01B-00	11/17/19 6:56 PM	fbi		ULM		6
BOSLW01-162187-007-01-01B-00	11/17/19 7:26 PM	fbi		ULM		6
BOSLW01-162187-008-01-01B-00	11/17/19 7:44 PM	fbi		ULM		6
BOSLW01-162349-001-01-01B-00	9/24/20 10:44 AM	fbi		ULM		6
BOSLW01-162349-002-01-01B-00	9/24/20 10:44 AM	fbi		ULM		6
BOSLW01-162466-001-01-01B-00	11/7/19 1:32 AM	fbi		ULM		6
BOSLW01-162466-001-01-01B-00	5/11/20 11:45 AM	fbi		ULM		6
BOSLW01-170232-001-01-01B-00	3/27/19 4:59 AM	fbi		ULM		6
BOSLW01-170363-006-01-01B-00	12/10/19 1:50 PM	fbi		ULM		6
BOSLW01-170846-002-01-01B-00	6/20/19 11:41 PM	fbi		ULM		6
BOSLW01-170846-002-01-01B-00	6/26/19 6:15 AM	fbi		ULM		6
BOSLW01-170909-007-03-01A-00	8/23/19 1:37 PM	fbi		ULM		6
BOSLW01-171334-003-02-01A-00	9/11/19 5:04 PM	fbi		ULM		6
BOSLW01-171334-010-02-01A-00	9/11/19 5:04 PM	fbi		ULM		6
BOSLW01-171334-010-02-01A-00	11/20/19 12:25 PM	fbi		ULM		6
BOSLW01-171334-017-02-01A-00	9/11/19 5:04 PM	fbi		ULM		6
BOSLW01-171647-001-02-01A-00	2/18/20 10:01 PM	fbi		ULM		6
BOSLW01-181218-008-02-01A-00	12/24/19 3:55 AM	fbi		ULM		6
BOSLW01-182251-006-01-01C-00	9/28/19 9:40 PM	fbi		ULM		6

- Click on first record that has "f-lvtp1" listed in the State column and check the results if is an ID or not (records listed "f-lvtpa" were already addressed).
- If the reverse result is **not a hit**, select "Non-ident" and click "Save". Add the info into the LPU stats Reverse State/FBI Hits (no additional steps are needed).
- If it is a HIT, check the case number and see if the latent was already IDed or not. If it was previously IDed select "Ident" and click save. Add the info into the LPU stats Reverse State/FBI Hits.
- If it was not originally IDed, need to request using "IRQ-CPR" by typing in the FBI# (9-digit number), attention indicator: Name and then send an email notification to the original analyst with the latent and the Known FBI information.  
See below example:

"Good morning/afternoon Analyst,

A candidate was generated by the Federal Integrated Automated Fingerprint Identification System after a ten-print inquiry and latent# (case#, i#) added to the unsolved federal database:

Search BOSLW01-20999-001-01-01B (latent #)  
COLBERT, Chelsea FBI# 32PCEHLNK (RI)

Please let me know if there is any further information needed to complete your analysis.

Thanks"

- Add the info into the LPU stats Reverse State/FBI Hits.
- Follow the steps to delete the latent from the **Unsolved Federal Database (ULD)**.

## **Requesting Exemplar from CJIS**

Request for a ten print exemplar card only found in the FBI database can be made by calling the CJIS Special Processing Center (304-625-5584, [spc@leo.gov](mailto:spc@leo.gov)), which is open 24/7, to ensure the individual is in the database and then finalize the request by emailing.

Request for a palm print exemplar card only found in the FBI database can be made by calling the Palm Print Services and Analysis Team (304-625-2849, [palm\\_prints@fbi.gov](mailto:palm_prints@fbi.gov)) which is open 24/7, to ensure the individual is in the database and then finalize the request by emailing.

## **AFIS Request Form**

An AFIS request form is available on the SAN under Latent Prints Uncontrolled Documents for use by the Latent Print Unit personnel to request assistance from the AFIS section. This form requests information, including but not limited to, case information, latent numbers, previously searched, which databases, and comments. After filling out the form, LPU personnel can email the AFIS team members with the attached request form. The AFIS team will conduct requested work, fill out Mideo information, and generate reports as needed.

## **REVERSE NOTIFICATIONS (TLI HITS) SENT FROM MSP**

The AFIS team should do comparison images of any possible TLI notifications received via email by the MSP. Should the result be "No Hit" a consultation will be performed by another AFIS team member. If any non-consensus decisions are reached the AFIS section will follow the Non-Consensus Decisions from the LPU SOP. When a consensus decision is made, the comparison images generated by the AFIS team are **not** required to be saved and the LPU stats Reverse State/FBI hits Google sheet will be updated.

If the notification is an **Identification** email the information to the original criminalist and delete the latent from the state unsolved latent database.

"Good morning/afternoon Analyst,

A candidate was generated by the MSP Identification System after a ten-print inquiry and latent# (case#, i#) added to the unsolved state database:

Search BOSLW01-20999-001-01-01B (latent #)  
COLBERT, Chelsea SID# MA999999999 (RI)

Please let me know if there is any further information needed to complete your analysis.

Thanks"

ID: LPU-AFIS	Approval Date: 5/2/2022	Revision # 2022.0 - Effective date: 5/2/2022	Page 19 of 19
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	



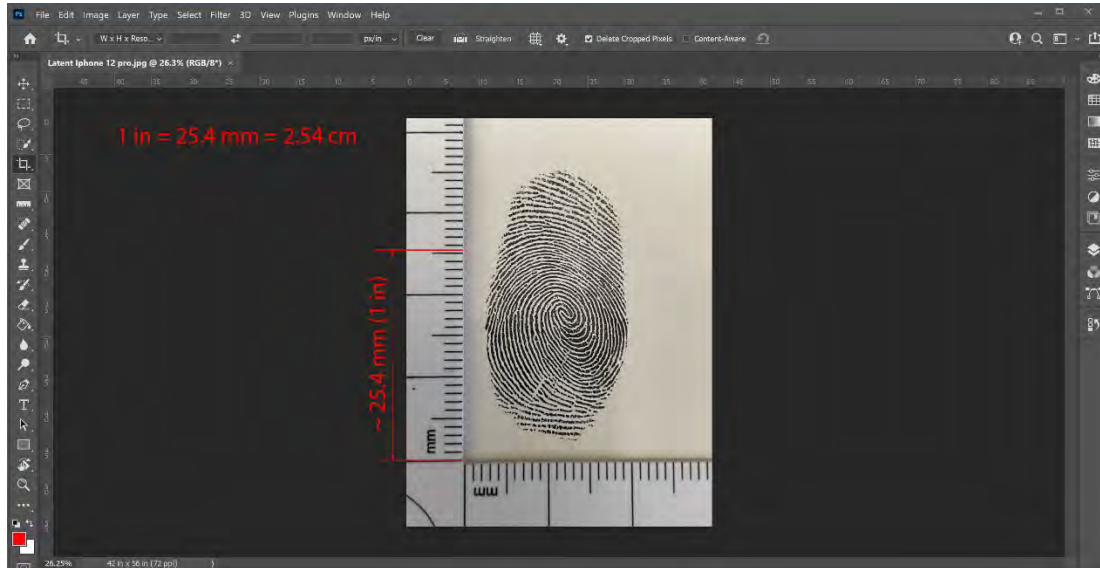
## **AFIS Workflow Guide**

This document will provide workflow guidance for using the Automated Fingerprint Identification System (AFIS).

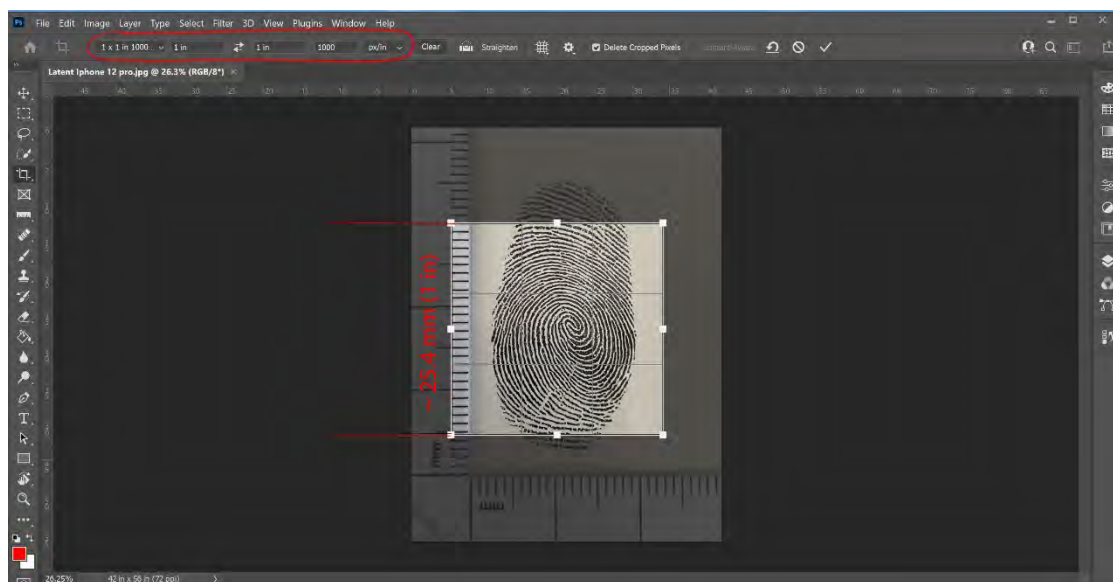
## **CALIBRATION**

Latent print images that are launched for searches in AFIS must be calibrated 1:1. Criminalists may follow, but are not limited to, the two techniques outlined below:

### *Technique One*



- If you have a latent image with a scale showing at least one inch (25.4 mm or 2.54 cm), you can crop it, with the crop tool, in one step using the preset (1 in x 1 in x 1000ppi); . your image is now ready for AFIS. If the scale is less than one inch, then go to Technique Two.

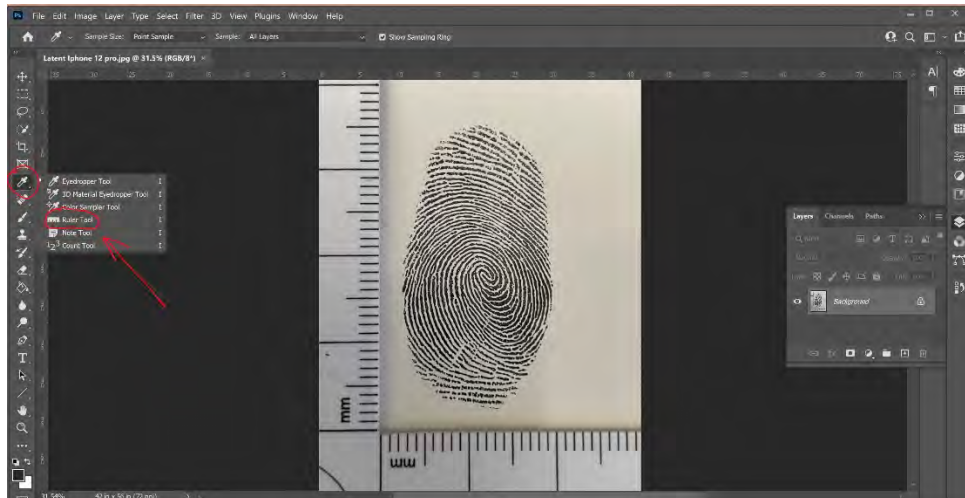


*\*This method can be used for palm prints using a crop preset (2 in x 2 in x 1000ppi) if the scale has at least 2 inches (50.8 mm or 5.08 cm).*

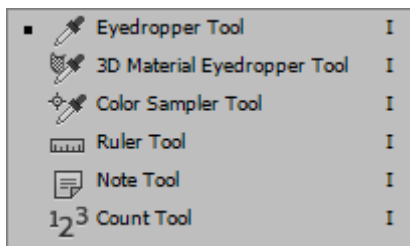
ID: LPU-AFIS	Approval Date: 5/2/2022	Revision # 2022.0 - Effective date: 5/2/2022	Page 2 of 19
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	



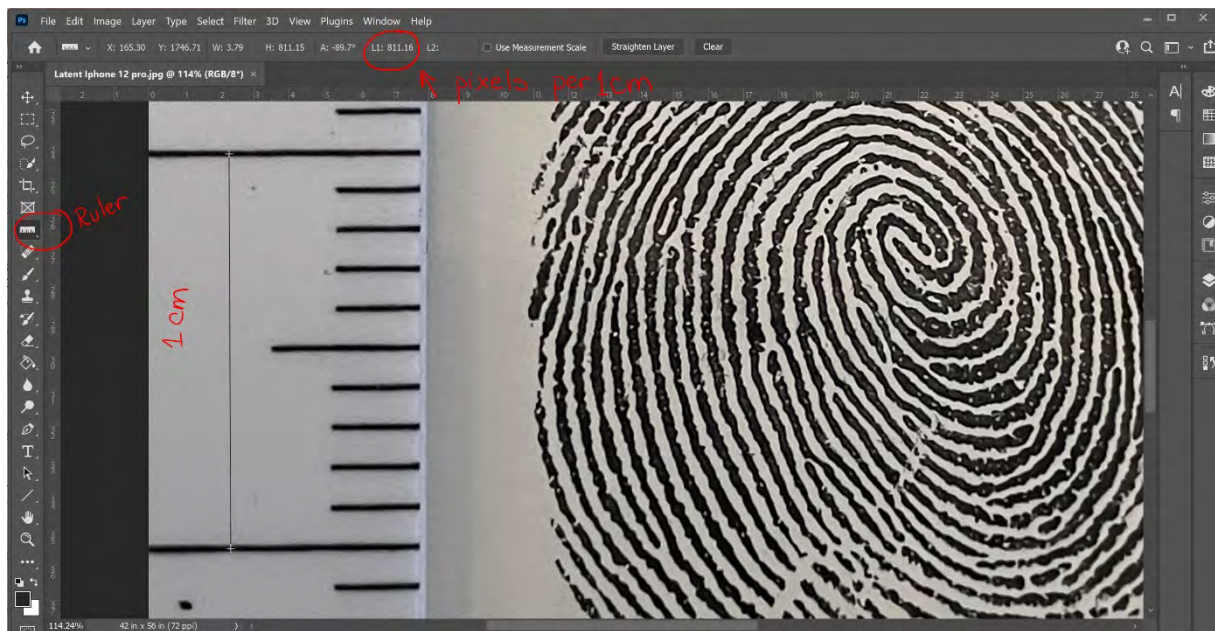
## Technique Two



- On the left side tool bar there is an eye dropper tool; click on this tool and a menu will pop up:

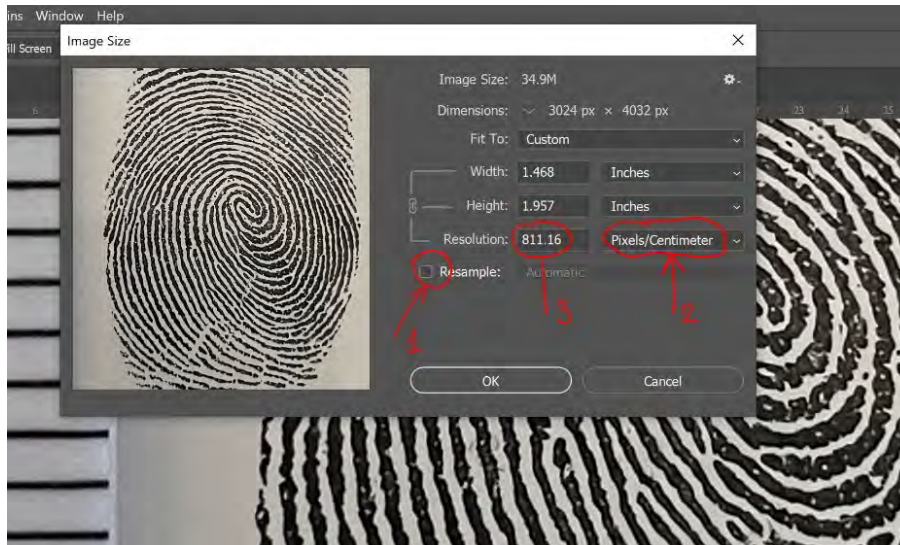


- Select the ruler tool. Measure out 1 cm. A number will appear on the top tool bar “L1” value showing the number of pixels per one centimeter (cm).

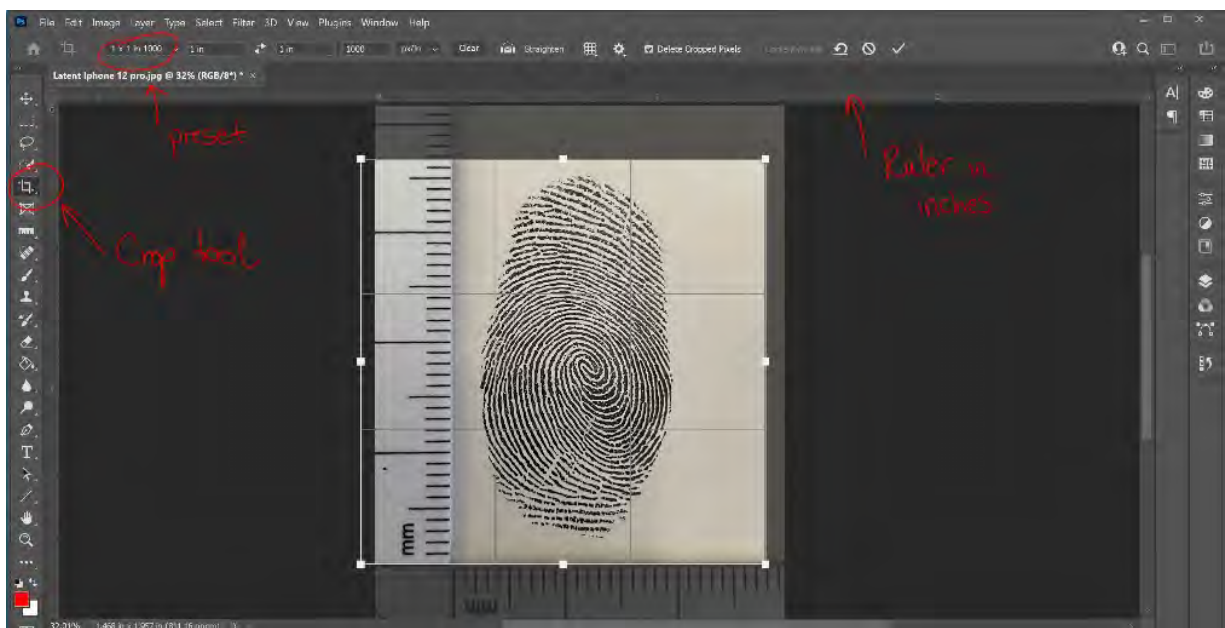


### Technique Two Continued

- Copy the number listed, in the example this number is 811.16. On the top of the tool bar in Photoshop click on Image, then on Image Size. The following box will appear:

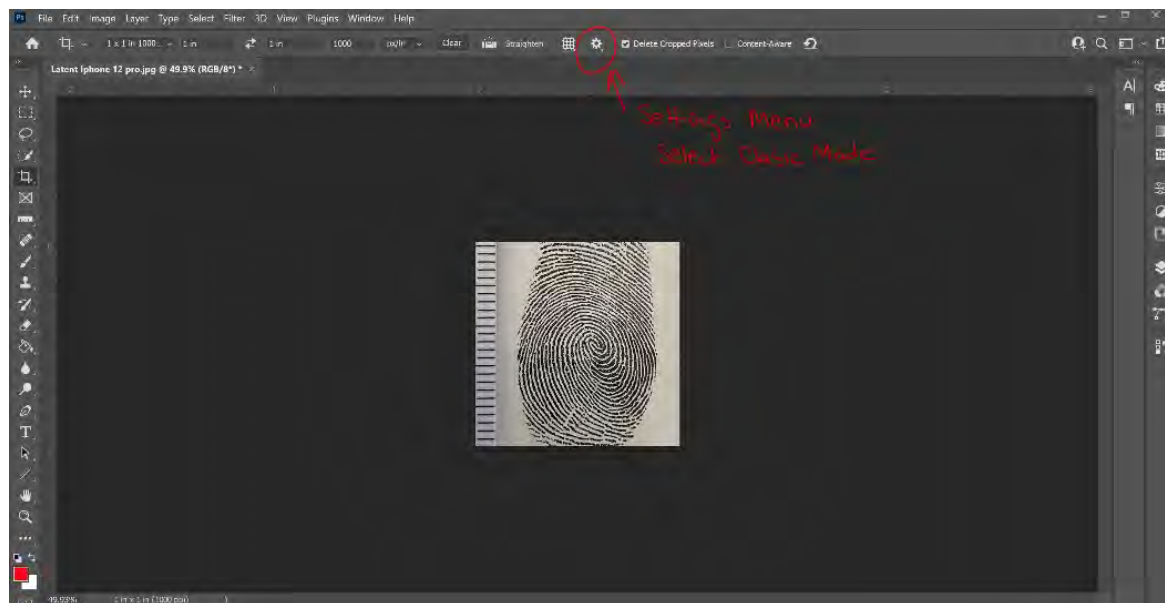


1. Make sure the resample image is NOT checked.
2. Change resolution box to Pixels/Centimeter.
3. Place number (L1 value) into the box and Hit "OK".



- A preset of 1 in. W x 1 in. H x 1000 ppi can be set.
- On the left side tool bar there is a crop tool. Use the preset listed above and a grid will appear over the latent image.

- Make sure the ruler appears at the top of your workspace and is showing inches (you can check the ruler by right clicking on the ruler). The box can then be measured to 1:1 by dragging the small gray boxes using the ruler.
- Move the entire crop box (be sure the setting is set for Classic Mode to fit over the ridge detail you would like captured for AFIS entry). Crop that area. You should see the image decrease in size as shown below:

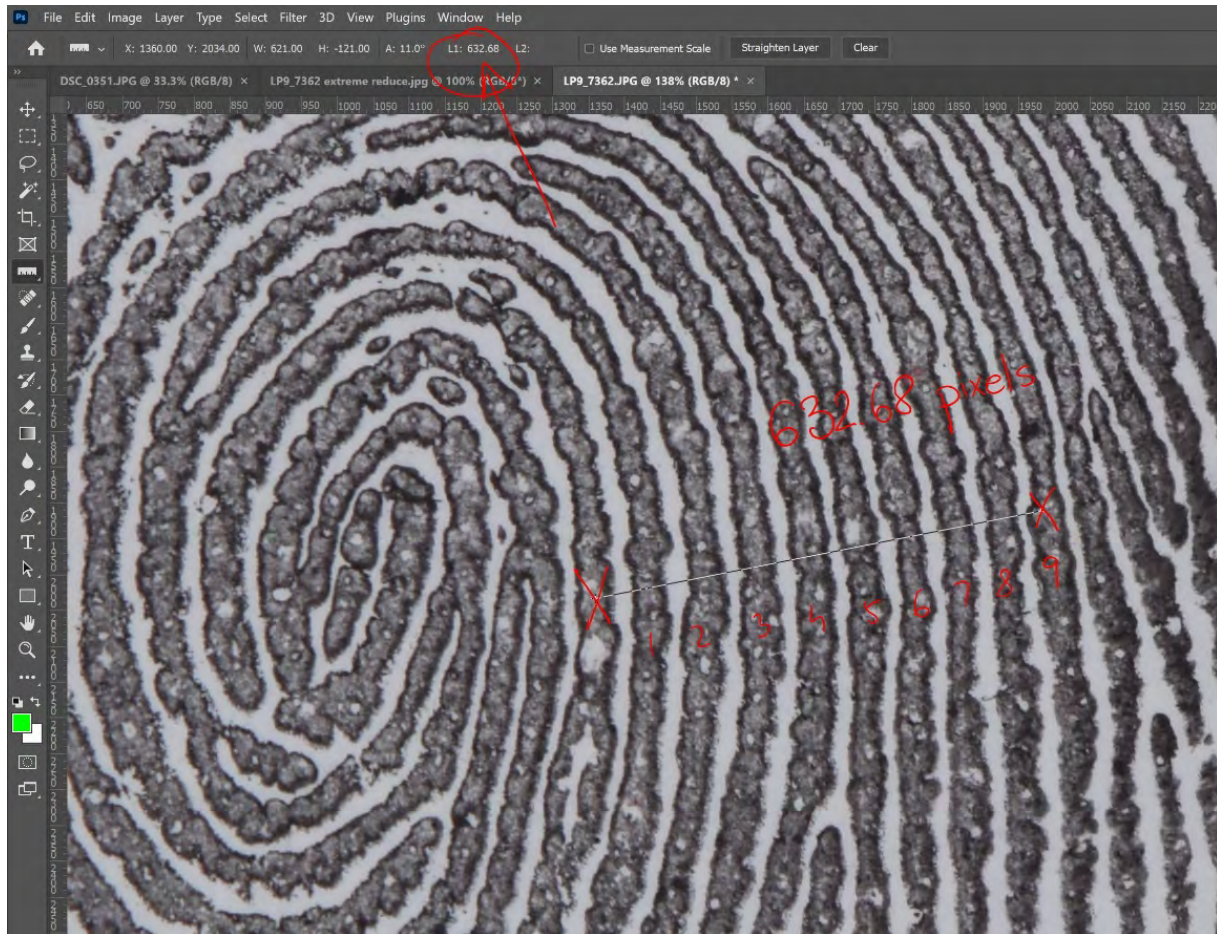


- Save the image at this time. You can always print the image to verify the calibration with a ruler before entry into AFIS.

## Calibrating in Photoshop (No scale)

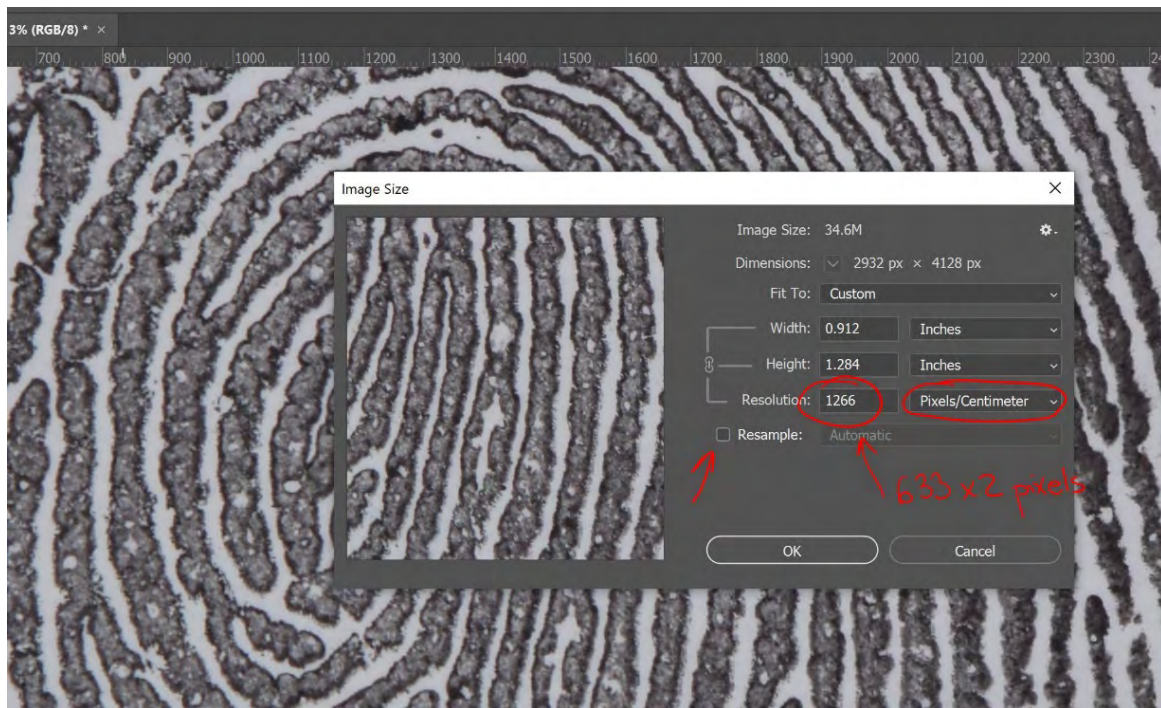
1. Open an image in Photoshop
2. Put the ruler tool in pixels as measurement
3. Measure out approximately 9 ridges (as perpendicular as possible) by selecting the ruler from the tool bar in an area with no compressed or extended ridges. See image below:





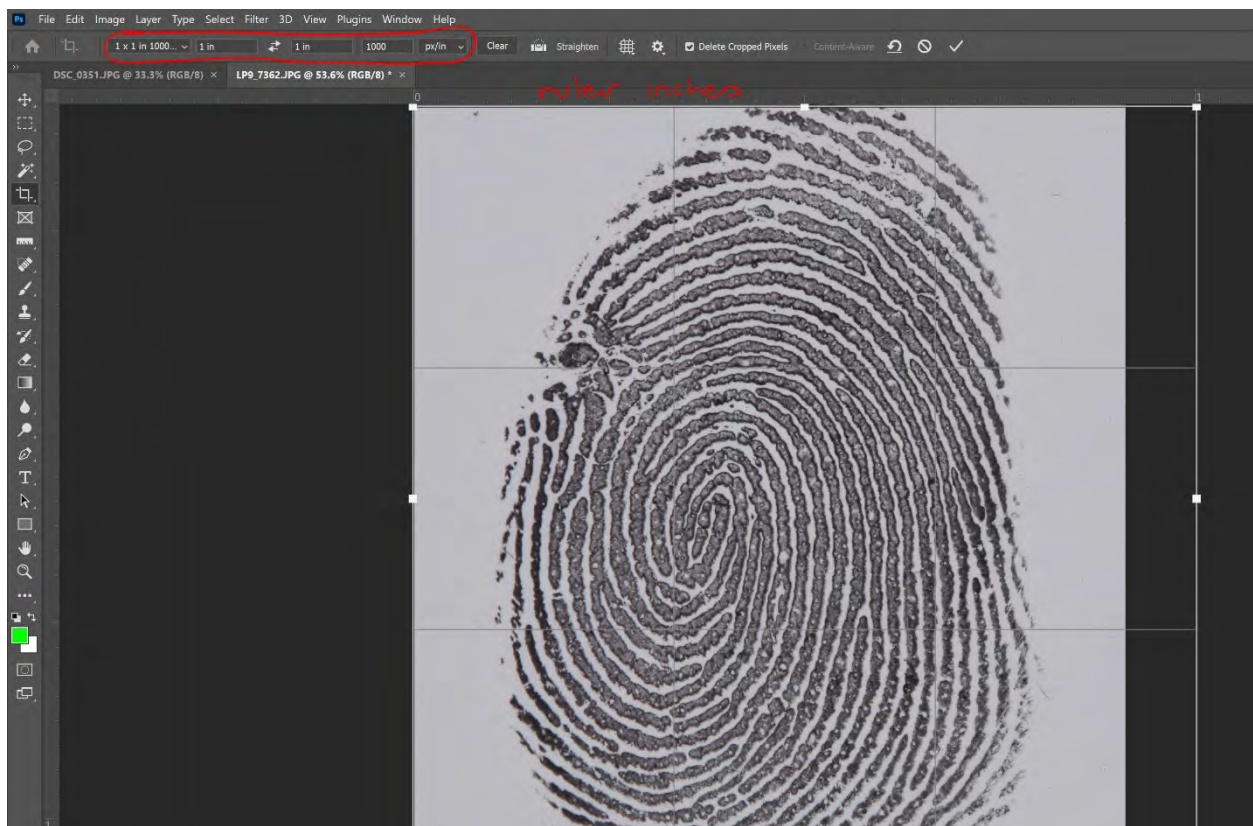
4. Example above: 9 ridges = ~633 pixels (L1 value) = ~0.5 cm so  $633 \times 2 = 1266$  Pixels equal ~1 cm

5. Image size: select Pixels/Centimeter and enter 1266. Leave Resample box unchecked.



6. Change ruler to inches

7. Use preset 1 in x 1 in x 1000ppi and adjust the box to the correct size on the ruler.





The image is an approximate calibration, and it can be increased or decreased in size with +/- 10% to perform additional searches if needed.

To increase the size 10%, add 126 pixels to 1266 resulting in 1392 pixels that need to be added in the image size to calibrate

To decrease the size 10%, subtract 126 pixels from 1266 resulting in 1140 pixels that need to be subtracted in the image size to calibrate.

## **AFIX Tracker (Local)**

When utilized at the Criminalist's discretion, the following steps are completed:

1. Open the AFIX tracker app from AFIX6 or AFIX7 computers
2. Click on the Crime Scene tab and select "Pull # of last records 20" then click OK
3. Select the last empty row and start filling the info of the case in starting with "Case Number"
4. Click on the "Latents" tab and then on the "Image Wizard" tab on the next window
5. Select "Latent Image File" from the pop-up window; change Import scale to 1000ppi and click Next
6. Select "Default Latent" from the description and click Next
7. Browse for your calibrated latent, select it and click Next
8. From the "Tools" bar select "Smart Extraction"
9. Click on the green check mark on the bottom
10. Select "Search Wizard" from the top bar
11. Local search will be selected by default. Click Next
12. Select the databases that will be searched (ten prints, palm prints, unsolved latents, and the number or returned candidates) and click Finish
13. To check the results, select "Search Results"
14. Check all candidates and mark the decision on each one by right clicking on the name

## **MORPHO (State & Federal)**

### *Passwords*

Morpho passwords are required to be changed every 3 months and can only be changed on the main terminal. Reminders can be set on calendars 2-3 days prior to expiration to ensure you are not locked out of the system. If you become locked out prior to changing your password, you will need to call the Morpho technician assigned at the MA State Police.

Once your password has been updated, the additional Morpho terminals will each need to be updated to allow all applications to open.

### ***Shortcut to the SAN (server) on Morpho (Mass State computer)***

When the Morpho system is rebooted or the password is changed, the possibility exists that the shortcut to the LPU-SAN server could be deleted. Follow the instructions below to reconnect and add the shortcut to the desktop:

ID: LPU-AFIS	Approval Date: 5/2/2022	Revision # 2022.0 - Effective date: 5/2/2022	Page 8 of 19
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

1. Ensure your password has not expired. If it has expired the following steps may not work.
2. Delete any LPU-SAN server's shortcuts for Morpho.
3. Double click on the computer icon and if there is any mapping of the server in the Network Location, right click on it and then click "Disconnect."
4. Create a new connection by mapping the LPU-SAN server. Right click on the computer icon and select "Map network drive." Select X: from Drive window. Instead of using the Browse function, type the following into the address bar: **\\10.25.16.75\Latent Print Unit** and click finish.
5. A new window should appear asking for username and password. *If this window does not appear then your password has expired and will have to be updated.*
6. Username is **Boston\_police\Your ID** and your own password for windows.
7. Access should be granted to the LPU-SAN server at this point.
8. Creation of a shortcut to the LPU-SAN server can be completed on your desktop.

### *Signing into Morpho Trak:*

Username: [BOS and ID#]

Password: [Upper case, lower case, #]

**Menu Bar** (vertical) on right side of screen ⇨ "Latent"

**Latent Expert** – create case/search latents

**Database Maintenance** – print ten print cards / delete latents from unsolved State Database

**Home Page** – status screen/responses

### **LATENT EXPERT**

Click on "Add" icon to add a case

Add a case panel:

CASE PREFIX: "Boston PD"

CASE NUMBER: [13XXXX without hyphen]

LATENT CASE AGENCY: "Boston PD"

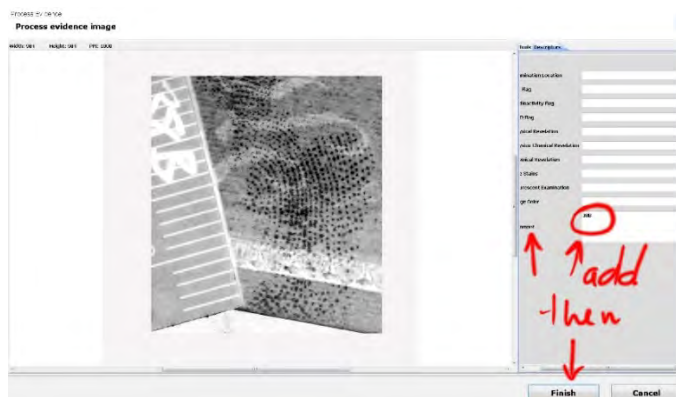
DATE OF CASE: date of incident

CRIME TYPE: select from drop down list

CASE IDENTIFIER: Last name, First name (no space after comma)

Click on the "Add new evidence from file" icon (try to limit to a max 30 latents per case to reduce lag time). If there are more than 30 latents you can create a new case with same name (ex. 219999a, 219999b, 219999c)

- Latent image opens ⇨ add latent name into description (1A) ⇨ "FINISH"
- Options to rotate and make additional adjustments to an image, but if previously done in Photoshop, go straight to "FINISH"



A new screen will open



↳ Add latent (4<sup>th</sup> box in top row)  
- Size box & double click

red=finger purple=palm

A new screen will open



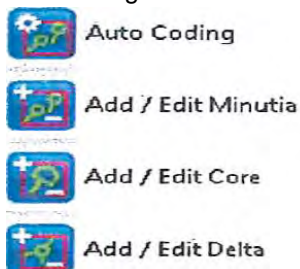
↳ "Create Area"

red=encoding will be outside of selected area  
green=encoding will be inside the selected area

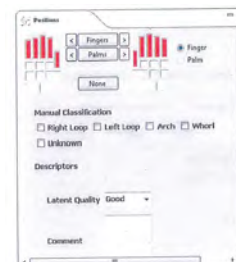
This step is optional. Use it only when you need a specific area to be encoded. (ex. Distortion, multiple impressions, etc.)



↳ Commonly used options for editing minutiae:



Additional tools are available for encoding



Positions Area

When Encoding and Positions Areas are complete ⇨ "SEARCHES" (double click)

A new screen will open

ADD TO LATENT DATABASE: "YES" is automatically selected or can select "NO"

ORIENTATION RANGE: "VERTICAL" (~ 45 degree rotation both ways) is automatically selected or can select "ANY" (full 360 degree)

- ☒ Person (LT/TP – LP/PP) – this will search State ten print and palm print cards
- ☒ FBI LFFS (searches done after State has no hits)

ID: LPU-AFIS	Approval Date: 5/2/2022	Revision # 2022.0 - Effective date: 5/2/2022	Page 10 of 19
Approval Authority: Director of Latent Print Unit		ALL PRINTED COPIES ARE UNCONTROLLED	

- ☒ Choose the latent(s) you want to search

↳ "SUBMIT"

**Note:** IF the latent is a joint, the search should be done in the FBI database. State Morpho does not search the joints and upper palms.

### Searching "Copy a Latent With Encodings"

Latent Expert ⇒ select your case

↳ Click on circle next to "Case Latents" ⇒ select latent to search (e.g. 001-01-01)

- Select "Copy Latent with Encodings" on left side menu
  - A message window will pop up ⇒ select "OK"

- Create an additional copy and open latent

- Can now change parameters (fingers, palms, pattern type)
- Can add/delete encodings

↳ double click "Searches"

- The copied latent should appear (e.g. 001-02-01)

*Follow the directions directly above to search latent in State and/or Federal database(s)*

### HOME PAGE

FILTER RESULTS

ID: "BOS"

USER: "ID#"

Conclusions: 1. IDENT 2. NON IDENT 3. NO DECISION

Make sure to save the candidate list by saving SEARCH RPT to the appropriate AFIS folder on the server.

The report must be saved after checking off at least one conclusion and before closing screen.

After entering in conclusions ⇒ "SAVE"

**\*\*If there is a possible IDENT, it is easier to print or save the card from the HOME PAGE\*\***

### Printing the ten print card with the possible hit:

Right click on SID# ⇒ "View Case" (DATABASE MAINTENANCE screen will open)

Click on "Print Tenprint" (vertical menu bar on left side of screen)

CARD FORM...: [change to "StateCriminal.fmt"](#)

### Saving the ten print card as a PDF:

PRINTER: [PDF writer](#)

↳ "Print" (automatically saves to "Pdf" folder on server)

- Rename and move to examiner folder

### Saving a finger/palm as a JPG image (recommended):

- Right click on the comparison screen or double click on finger image on the ten print screen.
- Right click ⇒ Export image ⇒ Rename ⇒ Save to appropriate file
  - ↳ Open in Photoshop
    - Change image size to 2500ppi
    - Resample must be on to make the resolution approx. the same in latent and known.

### **DATABASE MAINTENANCE**

RECORD TYPE: Criminal

Enter in any of the following information to search for a card:

SID/CID: MAXXXXXXXX (8 digit #)

LAST NAME

FIRST NAME

↳ "Search"

Under **Tenprint Search Results** ⇒ select the criminal record ⇒ "Open" \*\*Opens the COMPOSITE\*\*

- select the card you want from the drop-down list
- follow directions under **HOME PAGE** to save as a PDF

**Printing Civilian/Applicant cards** (Searchable only by AFIS Section criminalists, available based on request for the remaining examiners)

RECORD TYPE: Applicant

Enter in any of the following information to search for card:

SID/CID: MACXXXXXXX (7 digit #)

\*Searches can be done based on demographic info, for the applicants as well.

### **Saving the ten print card as a PDF:**

PRINTER: PDF writer

↳ "Print" (automatically saves to "Pdf" folder on server)

- Select State Applicant card
- Rename and move to examiner folder

### **FBI ten print cards**

Menu Bar ⇒ "Latent" ⇒ IRQ-CPR

*"IRQ Display" and "Type-2 Descriptors" tabs should be selected*

Enter in the following information:

FBI Number: XXX...

↳ Click on OK

Attention Indicator: **NAME OF CRIMINALIST (ex. SMITH,JOHN)**

↳ Click on Submit

Open Database Maintenance

*Find Tenprint tab" should be selected*

Enter FBI # (scroll down the page) ⇒ click on "Search"

↳ select the card you want

↳ double click your selection or click on "open"

A new screen will open displaying the ten prints

Follow directions under Home page to print and/or save as PDF

- CARD FORM...: **change to "FBI Criminal.fmt"**

If no name is printed on the FBI card, copy the Transaction Control Reference value (numbers and letters) from the Transaction Data tab,

Find: FBI-PWEK3W9TX-32345043 Record Type: FBI

Incident ID : FBI-PWEK3W9TX-32345043

Transaction Data

Type of Transaction: ULMT

Date: 09152021

Transaction Priority:

Destination Agency Identifier: MA0131100

Originating Agency Identifier: WVIAFIS0Z

Transaction Control Number: E202125800000297367

Transaction Control Reference: MTVNS0120210915961071

and paste it into the Transaction Control Number field and search it again. If the card was printed in MA, a SID# MAC# will appear with the name. See below image:

Find Tenprint Find Latent

Date (mmddccyy):

Date Printed (mmddccyy):

Transaction Control Number: MTVNS0120210915961071

Transaction Control Reference:

FBI Civil Record Number:

Valid entries are alphanumeric and special characters 1 to 40 in length.

Tenprint Search Results

ID	Last Name	First Name	Date of Birth	Record Type	FBI Number
FBI-PWEK3W9TX-32345045				FBI	PWEK3W9TX
FBI-PWEK3W9TX-32345043				FBI	PWEK3W9TX
FBI-PWEK3W9TX-32345044				FBI	PWEK3W9TX
FBI-PWEK3W9TX-32345048				FBI	PWEK3W9TX
MAC 1281133	TORRES	DONAS	12091968	APPLICANT	PWEK3W9TX

If there are no results after the search, contact the FBI for the name. See Request Exemplars from CJIS.

### Delete latents from Unsolved State Database (when latent was ID manually, or an FBI Hit):

Follow these steps:

1. Open Database Maintenance.
2. Select "Find Latent" from tabs.
3. Scroll down the window until you see "Latent Case Number."

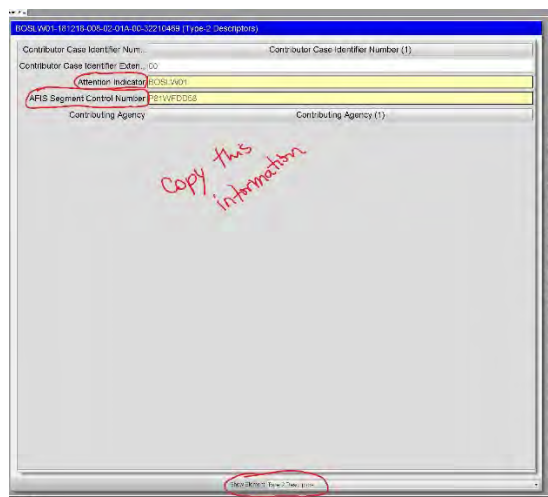
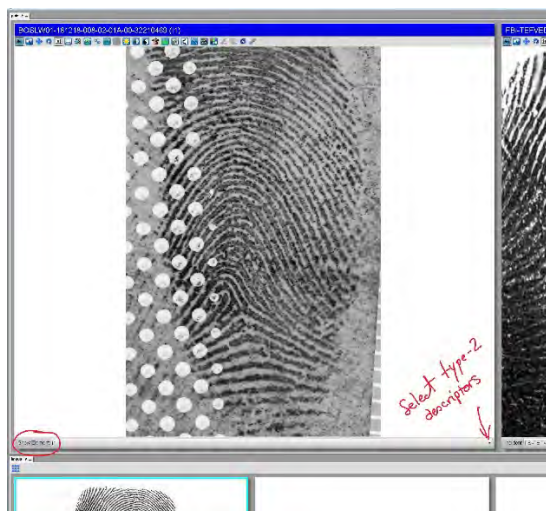


4. Type the case name "BOSLW01-13XXXX."
5. All latents added into the unsolved database will be listed.
6. Click on the latent that you want to delete.
7. In the left bar there is a "Delete Latent" button. Click on it.
8. Confirm the deletion.
9. Exit window.

**Delete latents from Unsolved Federal Database (only on reverse FBI Hits – AFIS section):**  
Follow these steps:

1. Open ULM Home page and select your search. Select Type-2 Descriptors from the Show Element drop list window (bottom of image).
2. Copy the information from all 5 fields (red circles).

Here is how to get the information from the FBI reverse ULM search (Home page).



3. Open IRQ-CPR app.

4. Select "ULD display" and Type-2 Descriptors from tabs.

5. Fill the following 5 criteria into the empty fields from the Type-2 Descriptor information of FBI reverse search found on ULM -Home page.

- a. Attention indicator
- b. AFIS Segment Control Number
- c. Contributor Case Identifier Number
  - Contributor Case Prefix
  - Contributor Case Identifier
- d. Contributor Agency
  - CRI1

4. Click submit.

5. Exit window.

6. In your home page, for a successful deletion, you should see your request with an "f-uldr" in "State" tab. If "f-errl" is displayed there was an error in the deletion process.

To check the error "f-errl" double click on it. At the bottom of the window the error message is displayed.

### Closed Searches:

Go to Case

Click on latent to be searched

- Make sure box is highlighted

ID: LPU-AFIS	Approval Date: 5/2/2022	Revision # 2022.0 - Effective date: 5/2/2022	Page 15 of 19
Approval Authority: Director of Latent Print Unit		ALL PRINTED COPIES ARE UNCONTROLLED	

Copy latent with encodings

Searches

- Do not add to database
- Known/unknown orientation

Have to click Person AND Closed

- Scroll down in box
- Click Add and enter SID# (If multiple SID#'s, have to click Add each time)
- Optional if you want to save the list with multiple SID#s:
  - o Click Export, rename (list knowns) and save to AFIS folder
  - o For additional closed searches you can import the saved list instead of typing all SID#s again

Check latent NOT SEARCHED and then click SUBMIT

Go to Home Page

## **COLD CASE SEARCHES**

The AFIS section has the ability to research unsolved homicide cases that had been previously worked by the LPU and determine if additional searches should be completed in the state and/or federal databases. The AFIS section may assess the latents for various additional and/or new searches (AFIS quality, 360 degree search, additional encodings, additional databases, etc.)

If additional searches are completed, the following procedure should be utilized:

1. If searches were previously conducted, search for and open the case in MORPHO. If no latents were previously searched, create a new case in MORPHO.
2. Open the latent print that will be searched (example: 001-01-01A).
3. Determine if new encoding or search criteria is needed.
4. Open up the search page by double clicking on "search".
5. Select if the latent print will be added to the unsolved database.
6. Select the orientation of the latent print.
7. Enter how many candidates to return (minimum of 3).
8. If searching the state database, check the "Person to Person" box. If searching the federal database, check the "LFFS" box.
9. Select the latent print(s) to be searched.
10. Click on Submit.
11. For pre interface cases, create a milestone in Mideo "New AFIS searches" and fill in the required information
12. Generate worksheets of the searches (AFIS page only) for a search that results in "no hit."
13. Generate all required worksheets if a search results in a "hit."

When a member of the AFIS section determines that a latent is AFISable, and that decision differs from the originating Criminalist, notification will be made with the original Criminalist prior to any searches being conducted.

ID: LPU-AFIS	Approval Date: 5/2/2022	Revision # 2022.0 - Effective date: 5/2/2022	Page 16 of 19
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

If searches do not generate a “hit,” members of the AFIS section will complete an AFIS no hit search report and have the report reviewed. The AFIS team member will issue the report to the customer as well as alert the original Criminalist that additional searches were completed with “no hit”.

If a “hit” is generated with a candidate, the member of the AFIS section will complete the comparison, generate the notes, and final report. If available, the original Criminalist should be the verifier. When the original Criminalist is unavailable or the AFIS team member is the original Criminalist, an alternate Criminalist will be sent the request for verification. The analytical image of the latent will be the encoded image saved within Morpho.

If a disagreement occurs, the non-consensus decision protocol will be followed.

## **REVERSE SEARCHES**

A reverse search is when a newly entered known impression “hits” to an unsolved latent print image that was added at the time of its search and not identified. The AFIS team have the ability to review the federal reverse searches for BPD cases. Negative reverse searches do not require case note documentation and/or a report.

When a “hit” is made in a reverse search, notification is made to the original examiner on the case.

## **Workflow for reverse FBI hits through MORPHO**

1. Open Home page.
2. In ID field type “BOS”.
3. IN TOT field type “ULM”.

4. A list with all reverse FBI hits will be listed.

Id	Date	User	Hold Op	TOT	RFP	Priority
BOSLW01-140937-001-01-01B-00	3/22/19 11:40 AM	fbi	ULM			6
BOSLW01-160636-002-03-01B	8/18/16 2:50 PM	boe132454	LFPB			7
BOSLW01-160629-001-01-01C-00	1/16/19 9:06 AM	fbi	ULM			6
BOSLW01-160629-001-02-01C-00	1/16/19 9:06 AM	fbi	ULM			6
BOSLW01-160629-001-02-01C-00	4/6/19 11:24 AM	fbi	ULM			6
BOSLW01-160629-001-02-01C-00	3/22/19 3:56 PM	fbi	ULM			6
BOSLW01-160629-001-02-01C-00	2/26/20 1:46 PM	fbi	ULM			6
BOSLW01-160754-001-01-01B-00	2/13/19 7:06 PM	fbi	ULM			6
BOSLW01-160754-001-01-01B-00	2/20/19 12:23 PM	fbi	ULM			6
BOSLW01-160754-001-01-01B-00	4/20/19 4:56 PM	fbi	ULM			6
BOSLW01-160754-001-01-01B-00	9/6/19 6:33 PM	fbi	ULM			6
BOSLW01-160754-001-01-01B-00	1/04/20 10:27 AM	fbi	ULM			6
BOSLW01-160754-001-01-01B-00	7/31/20 11:07 PM	fbi	ULM			6
BOSLW01-160926-008-01-01C-00	2/11/20 6:01 PM	fbi	ULM			6
BOSLW01-161654-002-01-01B-00	1/2/19 11:02 AM	fbi	ULM			6
BOSLW01-162187-001-01-01B-00	11/17/19 9:17 PM	fbi	ULM			6
BOSLW01-162187-001-01-01D-00	11/17/19 9:14 PM	fbi	ULM			6
BOSLW01-162187-003-01-01B-00	11/17/19 9:33 PM	fbi	ULM			6
BOSLW01-162187-006-01-01B-00	11/17/19 6:13 PM	fbi	ULM			6
BOSLW01-162187-006-01-01B-00	11/17/19 6:56 PM	fbi	ULM			6
BOSLW01-162187-007-01-01B-00	11/17/19 7:26 PM	fbi	ULM			6
BOSLW01-162187-008-01-01B-00	11/17/19 7:44 PM	fbi	ULM			6
BOSLW01-162349-001-01-01B-00	9/24/20 10:44 AM	fbi	ULM			6
BOSLW01-162349-002-01-01B-00	9/24/20 10:44 AM	fbi	ULM			6
BOSLW01-162466-001-01-01B-00	11/7/19 1:32 AM	fbi	ULM			6
BOSLW01-162466-001-01-01B-00	5/11/20 11:45 AM	fbi	ULM			6
BOSLW01-170232-001-01-01B-00	3/27/19 4:59 AM	fbi	ULM			6
BOSLW01-170363-006-01-01B-00	12/10/19 1:50 PM	fbi	ULM			6
BOSLW01-170846-002-01-01B-00	6/20/19 11:41 PM	fbi	ULM			6
BOSLW01-170846-002-01-01B-00	6/26/19 6:15 AM	fbi	ULM			6
BOSLW01-170909-007-03-01A-00	8/23/19 1:37 PM	fbi	ULM			6
BOSLW01-171334-003-02-01A-00	9/11/19 5:04 PM	fbi	ULM			6
BOSLW01-171334-010-02-01A-00	9/11/19 5:04 PM	fbi	ULM			6
BOSLW01-171334-010-02-01A-00	11/20/19 12:25 PM	fbi	ULM			6
BOSLW01-171334-017-02-01A-00	9/11/19 5:04 PM	fbi	ULM			6
BOSLW01-171647-001-02-01A-00	2/18/20 10:01 PM	fbi	ULM			6
BOSLW01-181218-008-02-01A-00	12/24/19 3:55 AM	fbi	ULM			6
BOSLW01-182251-006-01-01C-00	9/29/19 9:40 PM	fbi	ULM			6

- Click on first record that has "f-lvtp1" listed in the State column and check the results if is an ID or not (records listed "f-lvtpa" were already addressed).
- If the reverse result is **not a hit**, select "Non-ident" and click "Save". Add the info into the LPU stats Reverse State/FBI Hits (no additional steps are needed).
- If it is a HIT, check the case number and see if the latent was already IDed or not. If it was previously IDed select "Ident" and click save. Add the info into the LPU stats Reverse State/FBI Hits.
- If it was not originally IDed, need to request using "IRQ-CPR" by typing in the FBI# (9-digit number), attention indicator: Name and then send an email notification to the original analyst with the latent and the Known FBI information.  
See below example:

"Good morning/afternoon Analyst,

A candidate was generated by the Federal Integrated Automated Fingerprint Identification System after a ten-print inquiry and latent# (case#, i#) added to the unsolved federal database:

Search BOSLW01-20999-001-01-01B (latent #)  
COLBERT, Chelsea FBI# 32PCEHLNK (RI)

Please let me know if there is any further information needed to complete your analysis.

Thanks"

- Add the info into the LPU stats Reverse State/FBI Hits.
- Follow the steps to delete the latent from the **Unsolved Federal Database (ULD)**.

## Requesting Exemplar from CJIS

Request for a ten print exemplar card only found in the FBI database can be made by calling the CJIS Special Processing Center (304-625-5584, [spc@leo.gov](mailto:spc@leo.gov)), which is open 24/7, to ensure the individual is in the database and then finalize the request by emailing.

Request for a palm print exemplar card only found in the FBI database can be made by calling the Palm Print Services and Analysis Team (304-625-2849, [palm\\_prints@fbi.gov](mailto:palm_prints@fbi.gov)) which is open 24/7, to ensure the individual is in the database and then finalize the request by emailing.

## AFIS Request Form

An AFIS request form is available on the SAN under Latent Prints Uncontrolled Documents for use by the Latent Print Unit personnel to request assistance from the AFIS section. This form requests information, including but not limited to, case information, latent numbers, previously searched, which databases, and comments. After filling out the form, LPU personnel can email the AFIS team members with the attached request form. The AFIS team will conduct requested work, fill out Mideo information, and generate reports as needed.

## REVERSE NOTIFICATIONS (TLI HITS) SENT FROM MSP

The AFIS team should do comparison images of any possible TLI notifications received via email by the MSP. Should the result be "No Hit" a consultation will be performed by another AFIS team member. If any non-consensus decisions are reached the AFIS section will follow the Non-Consensus Decisions from the LPU SOP. When a consensus decision is made, the comparison images generated by the AFIS team are **not** required to be saved and the LPU stats Reverse State/FBI hits Google sheet will be updated.

If the notification is an **Identification** email the information to the original criminalist and delete the latent from the state unsolved latent database.

"Good morning/afternoon Analyst,

A candidate was generated by the MSP Identification System after a ten-print inquiry and latent# (case#, i#) added to the unsolved state database:

Search BOSLW01-20999-001-01-01B (latent #)  
COLBERT, Chelsea SID# MA999999999 (RI)

Please let me know if there is any further information needed to complete your analysis.

Thanks"

ID: LPU-AFIS	Approval Date: 5/2/2022	Revision # 2022.0 - Effective date: 5/2/2022	Page 19 of 19
Approval Authority: Director of Latent Print Unit		<b>ALL PRINTED COPIES ARE UNCONTROLLED</b>	

**Appendix DD - List of BPD Software and Databases**

	<b>Software/Database</b>	<b>Description</b>
1)	AFIX	Local AFIS database that contains Boston Police ten print and palm print records; implemented in March 2009 and identifies the candidates list by name
2)	AirTable Applications	Database management and development application
3)	Axon View	Video management software for Body Worn Cameras
4)	Bar Coded Evidence Analysis Statistics and Tracking (BEAST)	Software provides Forensic Laboratory Information Management Systems (LIMS) for case management and tracking for the Crime Laboratory Unit, Latent Print Unit, and Firearms Analysis Unit
5)	BRIC Data Warehouse	Custom configured SQL server data environment where records management data sources are replicated, collated, coded, and formatted in preparation for analysis
6)	BRIC Search Tool	Custom coded data attribute search application used to search BPD records
7)	Brief Cam Software and Upgrade	Video analytics software that provides detection and extraction capabilities to improve post-event investigation productivity by pinpointing objects of interest with speed and precision
8)	Central Square: CrimeView Dashboard	Crime analysis software; charts, graphs and maps; data used in analysis features law enforcement RMS data from the 9 city/town UASI region
9)	CI Technologies Case Info	Criminal Investigation Case Management database
10)	CI Technologies CrimeNtel	Criminal intelligence database to manage intelligence information under 28 C.F.R. Part 23
11)	Criminal Justice Information System (CJIS)	Application for accessing criminal offender record information, warrant related information, firearms licensing, and RMV records; also provides access to the National Crime Information Center (NCIC) records and National Law Enforcement Telecommunications System (NLETS). CJIS is managed by the Executive Office of Public Safety and Security.
12)	Clear	Public records data provider for law enforcement applications
13)	Combined DNA Index System (CODIS)	The CODIS database primarily consists of two indexes, the Forensic Index and the Offender Index. The Forensic Index contains DNA profiles from casework evidence and the



## Appendix DD - List of BPD Software and Databases

		Offender Index contains DNA profiles from convicted offenders and arrestees.
14)	CopLink	Search tool and database of law enforcement records management data collected from agencies across Massachusetts. System is managed by the Massachusetts State Police. The Department does not currently contribute data.
15)	Detective Case Management	Electronic case/content management system
16)	ESRI Enterprise GIS Applications	Enterprise-level Geographic Information System (GIS) software for conducting analysis and visualization of law enforcement/crime data while utilizing various geographic data sets (i.e., crime mapping).
17)	eTrace	Internet-based system that allows participating law enforcement agencies to submit firearm traces to the ATF National Tracing Center (NTC) and allows for the secure exchange of crime gun incident-based data
18)	evidence.com	Internet-based system through Axon which stores out body worn camera video
19)	FATPOT	Regional computer aided dispatch (CAD) system aggregation software and database. Provides situational awareness of emergency situations occurring throughout the Metro Boston Region.
20)	Gang Assessment Database	Database and application for maintaining gang and gang associate information in accordance with BPD Rule 335.
21)	Gun Licensing Database	Public Service Counter data management tool for gun licensing information.
22)	Hackney Driver Report Database	Public Service Counter data management tool for hackney records.
23)	Haystax Constellation	Web-based data portal used to house data on critical infrastructure assets in the UASI region
24)	Hexagon Intergraph CAD System	Computer aided dispatch system
25)	Homicide Manager	BRIC-administered database containing details specific to homicide incidents, intended to track such incidents for analysis



## Appendix DD - List of BPD Software and Databases

26)	i2 Enterprise Insight Analysis	Data management, analysis and visualization system. Includes i2 Enterprise Insight Analysis concurrent user software licenses, i2 Recommendation Engine software (entity resolution), i2 Analysts Notebook, and i2 Investigate (web-based application)
27)	Innoreader	RSS feed aggregator, which monitors news media and subject matter specific content provider site's RSS feeds and centrally organizes and displays the new materials for the user. The user then has a single source where all the latest content is automatically available.

28)	Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI)	Federal AFIS database that contains federal ten print and palm print records. The database identifies the candidate list by FBI number
29)	Intellicheck Age Verification Software	Software application used by Licensed Premises Unit for age verification. Scan history function and capability is disabled.
30)	ISO ClaimSearch	System maintained by the National Insurance Crime Bureau reporting insurance claim information from member insurance companies.
31)	Julota Database	Office of Research and Development (ORD) and the Street Outreach Unit (SOU) utilize the Julota database for case management purposes. Julota enables the SOU to track proactive outreach efforts to vulnerable populations with medical, mental health, homelessness and substance use challenges and referrals made to the SOU from external providers. This database is not used for investigative purposes. The database is used solely to improve and document the Department's response to individuals impacted by mental illness, substance use, and/or homelessness.
32)	LEEP: eGuardian	An FBI system managed by the FBI Office of Partner Engagement and used by federal agencies, state, local, tribal, and territorial law enforcement entities, and Fusion Centers to document, share and track potential threats, suspicious activity, and cyber, counterterrorism, counterintelligence, or criminal activity with the FBI and each other.
33)	LEEP: National Data Exchange (N-Dex)	Search tool and database of law enforcement records management data collected from contributing agencies. System is managed by the FBI. The Department does not currently contribute data.

## Appendix DD - List of BPD Software and Databases

34)	Lexis Nexis Accurint LE	Public records data provider for law enforcement applications
35)	LinX	Search tool and database of law enforcement records management data collected from contributing agencies. System is managed by the Naval Criminal Investigative Service. The Department does not currently contribute data.
36)	Lost Property Database	Public Service Counter data management tool for lost property records
37)	Mark43 Record Management System	Record management system for Department reports; Legacy Incidents for records prior to implementation of Mark43

38)	Medallion Report Database	Public Service Counter data management tool for medallion records
39)	Microsoft SQL Server	Microsoft database software
40)	MORPHO/Idemia	State AFIS database that contains Massachusetts ten print and palm print records. The database was implemented in June 2013 and identifies the candidates list by a State Identification (SID) Number
41)	MSDN/Visual Studio Pro	Database management and development application
42)	NetAbstraction	Malware protected web browsing solution to reduce cyber threat to law enforcement employees
43)	Neustar	Public records data provider for law enforcement applications
44)	PenLink	Analytic and investigative system for managing phone related investigative data.
45)	RICI Booking System	Booking database
46)	Safe and Successful Youth Initiative (SSYI) Database	Electronic case management system that includes individual-level data on SSYI clients
47)	Shootings Database	BRIC-administered database containing details specific to shootings incidents, intended to track such incidents for analysis and investigation. (i.e. individuals struck by gunfire)
48)	Shots Fired Database	BRIC-administered database containing details specific to shots fired incidents, intended to track such incidents for analysis and investigation. (i.e. gunfire with no victim -- person-- struck by ballistics). Contains references to ShotSpotter notifications.

## Appendix DD - List of BPD Software and Databases

49)	ShotSpotter Applications (“Respond” and “Insight)	Acoustic gunshot detection software.
50)	SITE Intelligence Group Analytic Services	Subscription website of information produced by SITE Intelligence Group, which is an American non governmental organization that tracks online activity of domestic extremists and jihadist organizations.
51)	Special Events Manager	BRIC-administered database used to manage information related to upcoming special events for public safety purposes.
52)	Tip/Lead Database	BRIC-administered database containing records related to tips and investigative leads collected for analysis and investigative vetting as potentially indicative of terrorism pre-operational planning, or mass violence.
53)	View Commander	Video management system to view and record from cameras that are not on the FLIR or GENETEC VMS systems.

54)	WebEOC	Emergency management message board system operated by Massachusetts Emergency management Agency and Boston office of Emergency Management.
55)	ZetX Trax	Cell phone analysis/investigative solution including applications to facilitate call detail record and geolocation analysis.

The Department does not own or pay for subscription-based licensing for “Social Media Monitoring Software.” The Department accesses information from publicly available sources, such as social media platforms, including, but not limited to, Facebook, Twitter, Instagram, and SnapChat, and utilizes publicly available applications to improve efficiency in reviewing such information, such as Snapmap and Tweetdeck.

The Department has not purchased, does not own, and does not use any “Predictive Policing Software.”

Boston Police Department  
Unmanned Aircraft System (UAS)  
Operations Manual

November 10, 2021

## **Table of Contents**

Preface

Mission Statement

Protection of Privacy

Definitions

### Section 1- Administration

1.1 Preface

1.2 Operations Manual

1.3 Organization

1.4 Personnel

1.5 Facilities

### Section 2- Safety

2.1 Preface

2.2 Safety Policy

2.3 Safety Awareness

2.4 Emergency Procedures

2.5 Medical Factors

### Section 3- Training

3.1 Preface

3.2 Instructors

3.3 Training Policies

3.4 Initial Training

3.5 Pilot Training

3.6 Visual Observer Training

3.7 Recurrent Training

3.8 Miscellaneous

### Section 4- General Operating Procedures

4.1 Preface

4.2 General Deployment Rules

4.3 Deployment Rules

4.4 Pre-flight

4.5 Weather

4.6 Post-flight

4.7 Documentation

4.8 Communication Requirements

4.9 Tactical Beyond Visual Line of Sight Operations

4.10 Emergency Procedures/Operational Anomalies

Section 5- Maintenance

5.1 Preface

5.2 Maintenance Policy

5.3 Aircraft Registration

5.4 Logs and Records

Section 6- Miscellaneous

6.1 Preface

6.2 Data Retention Policy

6.3 UAS Footage For Training Purposes

6.4 Retention Timelines

6.5 Complaints

## **Preface**

The purpose of this operations manual is to provide members of the Boston Police Department (BPD) with a set of operational procedures intended to promote the safe, efficient, and lawful operation of all Unmanned Aircraft Systems utilized by the Department.

## **Mission**

The mission of the Boston Police Department's UAS Program is to provide aerial assistance to Boston Police employees, and other first responders, in a safe and transparent manner to help enhance the safety and quality of life for the people of the City of Boston.

All Remote Pilots in Command who take part in the use of a UAS shall make every reasonable effort to mitigate the invasion of a person's reasonable expectation of privacy when operating the UAS. All Department Personnel who utilize a Department UAS, including Remote Pilots in Command, shall abide by all federal laws, state laws, local ordinances, FAA Regulations, and Department Rules and Procedures.

## **Protection of Privacy**

Safety and the protection of citizens' civil rights and reasonable expectations of privacy are key components of the decision to deploy a UAS. Remote Pilots in Command and Visual Observers shall ensure that all Department operations of UAS shall be as minimally intrusive as possible upon private persons and businesses. To accomplish this primary goal, the Department observes the following:

1. When a UAS is deployed the onboard cameras shall be turned to be facing away from all persons and occupied structures, unless the camera needs to be used solely for the purposes of safely navigating the UAS, until said UAS reaches the subject of the deployment.
2. Department UAS shall not be intentionally used for viewing, recording or transmitting images and/or video in a criminal investigation at any location or property where a person has a reasonable expectation of privacy unless:
  - a. A warrant or court order has been approved for the search of the property

- b. Exigent circumstances exist, including: search and rescue deployments, tactical deployments, crash scenes, fire scenes, hazardous material scenes, and natural disasters
  - c. Consent is given by the owner or person responsible for the property
- 3. The Department UAS Manager shall ensure that annual statistics are saved for all UAS deployments, to include training flights.

## **Definitions and Abbreviations**

**Above Ground Level (AGL):** The altitude expressed in the actual number of feet measured above the ground.

**Air Traffic Control (ATC):** Manages traffic from the airport to a radius of 3 to 30 miles. Provide pilots taxiing and take off instructions, air traffic clearance, and advice based on their own observations and experience. Maintains separation between landing and departing aircraft, transfers control of aircraft to the en-route center controllers when the aircraft leave their airspace, and receives control of aircraft on flights coming into their airspace.

**Certificate of Authorization (COA):** An authorization issued by the Air Traffic Organization to a public operator for a specific UA activity including granting permission to fly within specific boundaries and parameters.

**Federal Aviation Administration (FAA):** Federal agency in the United States and part of the Department of Transportation. The FAA regulates U.S. civil aviation, U.S. commercial space transportation, operates control towers, builds, installs, and maintains electronic aids to navigation, and registers all pilots and aircrafts in the United States.

**Instrument Flight Rules (IFR):** Rules and regulations established by the FAA to govern flight under conditions in which flight by outside visual reference is not safe. IFR flight depends upon flying by reference to instruments in the flight deck, and navigation is accomplished by reference to electronic signals. Under IFR, ATC exercises positive control (i.e., separation of all air traffic within designated airspace) over all aircraft in controlled airspace, and is primarily responsible for aircraft separation. Aircraft operating under IFR must meet minimum equipment requirements. Pilots must also be specially certified and meet proficiency requirements. IFR aircraft fly assigned routes and altitudes, and use a combination of radio navigation aids and vectors from ATC to navigate.

**National Airspace System (NAS):** The overall environment for the safe operation of aircraft that are subject to the FAA's jurisdiction. This includes: air navigation facilities, equipment and services, airports or landing areas; aeronautical charts, information and services; rules, regulations and procedures, technical information, and manpower and material.

**Navigable Airspace:** The airspace at or above the minimum altitudes of flight that includes the airspace needed to ensure safety in the takeoff and landing of aircraft. The FAA administers this



Unmanned Aircraft System Operations Manual

airspace in the public interest as necessary to ensure the safety of aircraft and its efficient use. Controlled airspace is classified as: A, B, C, D, E, and G.

**Notice to Airmen (NOTAM):** A notice containing essential information to personnel concerned with flight operations but not known far enough in advance to be publicized by other means. It states the abnormal status of a component of the NAS, not the normal status. NOTAMs indicate the real-time and abnormal status of the NAS impacting every user; concern the establishment, condition, or change of any facility, service, procedure or hazard in the NAS; and have unique language using special contractions to make communication more efficient. The NOTAM provides knowledge that is essential to personnel concerned with flight operations in designated areas. NOTAMs may be filed as a temporary change to the NAS publications.

**Part 107 Certification:** Certificate issued by the FAA to individual pilots who have completed an FAA examination that grants permission to fly UAS within specific parameters set forth in 14 CFR Part 107.

**Remote Pilot-in-Command (PIC):** A person who holds a remote pilot certificate with a UAS rating and has final authority and responsibility for the operation and safety of a UAS operation conducted under 14 CFR 107.

**Temporary Flight Restrictions (TFRs):** A regulatory action issued by the FAA via the U.S. Notice to Airmen (NOTAM) system to restrict certain aircraft from operating within a defined area, on a temporary basis, to protect persons or property in the air or on the ground.

**Unmanned Aerial Vehicle (UAV):** An aircraft that is operated without a physical human presence within or on the aircraft which, depending on how it is utilized, is capable of capturing and documenting photographs and video of the affected area or providing an aerial perspective of the area and is guided by remote control under the supervision of the assigned operating officer.

**Unmanned Aircraft System (UAS):** Consists of a UAV weighing less than 55 lbs., a ground control station, command and control links, and crew members in support of unmanned flight operations.

**Unmanned Aerial System Crewmember:** A Remote Pilot in Command (Remote PIC), Visual Observer (VO), and any other persons assigned UAS duties for the purpose of flight.

**Special Government Interest (SGI) Waiver:** FAA expedited waiver process for current Part 107 Pilots, or current (COA) holders to accommodate real-time application requests that will directly support a UAS operation benefiting a critical public good and addressing exigent circumstances. Such operations include: Firefighting, Search and Rescue, Law Enforcement, Utility or other Critical Infrastructure Restoration, Damage Assessments supporting Disaster Response and Recovery, and Media Coverage Providing Crucial Information to the Public.

**Tactical Beyond Visual Line of Sight (TBVLOS):** A waiver issued by the FAA, pursuant to 14 CFR 91.113(b), that allows public UAS operators, acting in an active first responder capacity, to

Unmanned Aircraft System Operations Manual

temporarily operate UAS beyond visual line of sight to assess an operational environment in a time of extreme emergencies to safeguard human life.

**Visual Line of Sight (VLOS):** Visual contact between PIC or VO and the UAS sufficient to maintain safe operational control of the aircraft, known location, and be able to scan the airspace in which it is operating to see and avoid other aircraft or any other objects that may affect the safety of the flight.

**Visual Observer (VO):** A person acting as a flight crew member who assists the small UA Remote PIC to see and avoid other air traffic or object in flight or on the ground. The Visual Observer is equally responsible for the visual observation of the UAS while in-flight. The VO shall alert the PIC of any conditions (obstructions, terrain, structures, air traffic, weather, etc.) that may affect the safety of flight. The VO shall be certified by successful completion of an approved training course outlined by the UAS Program Manager.

## Section 1 Administration

### **1.1 Preface**

The following procedures are intended to promote the safe, efficient, and lawful operation of Boston Police Department Unmanned Aircraft System (UAS).

### **1.2 Operations Manual**

The operations manual is written to satisfy the following criteria

- 1.2.1** The policies and procedures contained in this manual are to be adhered to for all Department deployments of a UAS.
- 1.2.2** This manual is not intended to be all-inclusive. It shall serve as a supplement to other department rules and procedures, FAA regulations, the Department's COA, all federal and state laws, local ordinances, and the aircraft manufacturer's approved user manual.
- 1.2.3** This manual has been written to address UAS operations as they existed at the time the manual was drafted. The manual will be reviewed and updated in the same manner and time frame as necessary. Any revision to this manual will be in accordance with the policies and procedures of the Boston Police Department.
- 1.2.4** The Department UAS manager shall ensure a copy of this manual is issued to each person having any UAS responsibilities.

### **1.3 Organization**

- 1.3.1** The UAS unit shall be comprised of those personnel approved by the UAS Manager. Personnel includes pilots, visual observers, and anyone else with an assignment to the UAS program.
- 1.3.1** The UAS unit will be comprised of trained Boston Police Department personnel.

### **1.4 Personnel**

- 1.4.1** UAS Manager: The UAS Manager shall oversee the implementation, management, training, documentation, deployments and adherence to current FAA regulations for all UAS owned, maintained, or deployed by the Boston Police Department. The UAS Manager shall create unit specific SOPs and ensure the safe operation of all Department UAS. The UAS Manager is assigned to the Homeland Security Unit of

the Bureau of Field Services, reporting directly to the unit commander. The UAS Manager's responsibilities will also include.

- Equipment evaluation and purchasing
- Selection of UAS Program members
- Development and approval of training modules
- Maintain all training, flight, and maintenance records for each pilot, observer, and each individual airframe
- Maintain contact with the FAA and familiarity with applicable FAA regulations
- Maintain proficiency on all UAS operated by the UAS Program
- Selection of UAS Program members
- Evaluation and purchasing of equipment
- Obtain and maintain an FAA *remote pilot FAA Part 107 certificate with a small UAS rating*

**1.4.2** Pilot in Command: The Pilot in Command (PIC) is the sole person responsible for the safety and operation of the UAS during a mission or training. All PICs shall hold a remote pilot certificate with a UAS rating. PICs have the final authority and responsibility for the operation and safety of a Department UAS operation.

**1.4.2.1** Pilot in Command requirements and responsibilities include:

- Proficiency in filing NOTAMS
- Compliance with all weather safety protocols, including maximum airspeed each UAS can be operated in
- Proficiency in conducting mission briefings and identifying any hazards that can potentially affect the flight
- Have an understanding of, and comply with, all FAA regulations applicable to the airspace where the UAS will operate
- Have an understanding of, and comply with, the manufacturer's user manual for any UAS that is being deployed
- Proficiency in utilizing the UAS Preflight Checklist, ensuring that the UAS is properly prepared for flight
- All pilots must know the procedure for reporting an accident through the Department and FAA. Accidents must be reported within ten (10) days if it results in a serious injury or accident requiring hospitalization or if there is damage to any property, other than the UAS, that is greater than \$500.00 to repair or replace.

---

Unmanned Aircraft System Operations Manual

- All pilots must properly document all Department flights electronically, via AirData log book or, if AirData is not compatible with the UAS, with equivalent software.
- Obtain and maintain an FAA *remote pilot certificate with a small UAS rating*

**1.4.3** Visual Observer: The Visual Observer (VO) is a person acting as a flight crew member who assists the PIC to see and avoid other air traffic or objects in flight or on the ground.

**1.4.3.1** Visual Observer requirements and responsibilities include:

- The ability to effectively communicate with the PIC, incident commander, and manned aircraft (if applicable) via radio or face-to-face (whichever is most appropriate)
- Compliance with regulations concerning right of way rules, operating near other aircraft, careless operation, etc.
- Knowledge of, and the ability to use, UAS support equipment such as radios, cameras, and charging stations

## **1.5 Facilities**

**1.5.1** The UAS Manager will be based in the Bureau of Field Services, Homeland Security Unit of the Boston Police Department.

**1.5.1.1** Certified UAS pilots will check out a UAS for use on duty.

**1.5.1.2** Weekly checks will be performed on all UAS equipment to ensure a state of readiness. Each pilot is responsible for their own weekly checks. Each weekly check shall be documented and provided to the UAS Manager.

**1.5.1.3** All UAS Program members are equally responsible for maintaining, cleaning, and securing the UAS equipment.

## Section 2 Safety

### **2.1 Preface**

The safety of the community and Department Personnel, above all else, is the primary concern in every operation, regardless of the nature.

### **2.2 Safety Policy**

The above goal is achieved through the following:

- The ongoing pursuit of an accident-free workplace, including no harm to people, equipment, property, or the environment
- Continuous safety training and awareness programs
- Conducting regular audits of safety policies, procedures, and practices
- Monitoring the UAS community to ensure best safety practices are incorporated into the organization

**2.2.1** It is the duty of every member within the UAS Program to contribute to the goal of continued safe operations. This contribution may come in many forms and includes always operating in the safest manner practicable and never taking unnecessary risks. Any safety hazard, whether procedural, operational, or maintenance-related, should be identified as soon as possible. Any suggestions in the interest of safety should be made through the UAS Manager.

**2.2.2** If any member of the Department observes or has knowledge of an unsafe or dangerous act committed by another member of the Department, the UAS Manager is to be notified immediately.

### **2.3 Safety Awareness**

In regards to safety, all members of the UAS Program are safety officers and therefore, shall at all times:

- Ensure all flight personnel understand applicable regulatory requirements, standards, and organizational safety policies and procedures
- Observe and control safety systems by monitoring all operations
- Review standards and practices of Department personnel as they impact operational safety
- Communicate all reported safety related problems and the corrective action(s) taken. If there were any in-flight problems, lessons learned, and the proper procedures for handling the problem should be shared and discussed
- Copy and circulate pertinent safety information

- Copy and circulate emergency safety bulletins

## **2.4 Medical Factors**

The health of the flight crew is paramount and any member of the UAS Program can stand down if they feel they are not able to perform their duties to the highest level.

- 2.4.1** A self-assessment of physical condition shall be made by all flight crew members during pre-flight activities.
- 2.4.2** No member shall act as a PIC, VO, or in any other capacity as a member of the flight crew, within eight hours after consumption of any alcoholic beverage pursuant to 14 CFR 91.17(a).
- 2.4.3** No member shall act as a PIC, VO, or in any other capacity as a member of the flight crew, if they are using any drug that affects the person's faculties in any way contrary to safety pursuant to 14 CFR 91.17(a)(3).

## Section 3 Training

### **3.1 Preface**

To ensure the continued safe operation of Department UAS, all PICs must achieve and maintain a high level of competency in the operation of Department UAS. Proficiency, in both academic knowledge and practical skills, is best realized through regular training.

### **3.2 Instructors**

- 3.2.1** The primary instructor for all Department pilots will be the UAS Manager. The UAS Manager will conduct training based on the varying needs of the program. The UAS Manager will designate who is a qualified instructor.
- 3.2.2** Duties of instructing new members shall fall upon those who have the most flight time and knowledge of UAS operations. Instructors will be designated based on experience and competency with UAS operations and approved by the UAS Manager.

### **3.3 Training Policies**

- 3.3.1** All members shall be issued a copy of this manual.
- 3.3.2** Training plans will be developed by the UAS Manager; trainings will be implemented by the UAS instructors.
- 3.3.3** All deployments and/or exercises will be documented and counted toward a member's training / flight hours.
- 3.3.4** Each member of the UAS Program has the responsibility to verify and log their own flight hours and training using AirData online logbook or, if AirData is not compatible with the UAS, with equivalent software.
- 3.3.5** All flight times, for both training and operations, shall be maintained for each pilot in the pilot's flight record. The flight record for each pilot shall be maintained by the UAS Manager.

### **3.4 Initial Training**

- 3.4.1** Upon acceptance into the UAS Program, each new member will attend an orientation and be given a copy of the policy procedure manual, and position task book.
  - 3.4.1.1** The new member orientation shall address the following:



- The Boston Police Department UAS Operations Manual review
- PowerPoint presentation

### **3.5 Pilot Training**

**3.5.1** All PICs selected to fly Department-approved missions will be properly trained by Department instructors and, in some instances, manufacturer representatives. Each PIC shall be required to attend a Department PIC certification course along with passing a proficiency test established by the UAS Manager. The proficiency test shall be in accordance with Standard Test Methods for Small Unmanned Aircraft Systems established by the Institute of Standards and Technology (NIST) and/or a practical application test established by the UAS Manager. A member is authorized to conduct flight operations as the PIC when the following criteria has been met:

**3.5.1.1** PICs and VOs must have completed sufficient training to communicate to the pilot any instructions required to remain clear of conflicting traffic. This training, at a minimum, shall include knowledge of the rules and responsibilities described in 14 CFR 91.111, Operating Near Other Aircraft; 14 CFR 91.113, Right-of-Way Rules: Except Water Operations; and 14 CFR 91.155, Basic VFR Weather Minimums; knowledge of air traffic and radio communications, including the use of approved ATC/pilot phraseology; and knowledge of appropriate sections of the Aeronautical Information Manual.

**3.5.1.2** In conjunction with fulfilling all training requirements for PIC or VO duties, the PIC

must also become familiar with UAS operations, the aircraft and its equipment.

**3.5.1.3** Before a member can operate as a PIC, they must obtain his/her Remote Pilot Certificate

issued by the FAA. Prior to flying any mission, the PIC must complete at least 40 hours of training to include flight training. The PIC must show proficiency of the flight training exercises and the airframe. This must be accomplished to show their ability and knowledge of the UAS.

**3.5.2** Any member that has the status of 'pilot' may act as a VO while the PIC is at the controls of the UAS.

**3.5.3** Any member who fails to successfully complete the initial training may be denied as a member

of the UAS Program by the UAS Manager.

### **3.6 Visual Observer Training**

- 3.6.1** Following the completion of the required training approved by the UAS Manager, authorized personnel may serve in the role of Visual Observer.

### **3.7 Recurrent Training**

- 3.7.1** All members shall maintain proficiency in their pilot/VO abilities. Members who do not have any documented training or flight time within 90 days of their previous operation/training/exercise, must meet with the UAS Manager before they can be returned to full flight status.
- 3.7.2** All members within the program shall maintain proficiency in their pilot/VO abilities. All PICs must ensure they conduct at least three flights to include three take-offs and landings every ninety days. These flights will be documented and maintained in the AirData log book or, if AirData is not compatible with the UAS, with equivalent software. Failure to maintain proficiency will result in suspension of flight status for the UAS Program. Members who do not have any documented training or flight time within a span of 30 days will have to show proficiency before being a PIC/VO during a mission or exercise.
- 3.7.3** Once every quarter, the PICs will be required to pass a proficiency test established by the UAS Manager. The proficiency test will be in accordance with Standard Test Methods for Small Unmanned Aircraft Systems established by NIST and/or a practical application test established by the UAS Manager. Failure to maintain proficiency or pass the proficiency test will result in suspension from flight operations from the UAS Program. All results of the PIC's proficiency test shall be entered into the PIC's pilot flight record.
- 3.7.4** If any of the PICs fail the quarterly proficiency test, they will be given remedial training and afforded another opportunity to pass the proficiency test. If the PIC fails to pass the second proficiency test, they will be suspended from flight operations until they are able to pass the proficiency test. All results of the PIC's proficiency test shall be entered into the PIC's pilot flight record.

### **3.8 Miscellaneous**

- 3.8.1** All requests for outside training shall be approved through the UAS Program Manager.
- 3.8.2** Training shall only be conducted at approved locations and authorization per Part 107 using "AirMap" or equivalent software application.

## Section 4

# General Operating Procedures

### 4.1 Preface

Deployment of the UAS in the safest and most efficient manner is the purpose of this section and the goal of the UAS Program.

### 4.2 General Deployment Rules

**4.2.1** For daytime operations a minimum of one pilot and at least one observer are preferred for all deployments.

**4.2.2** UAS night operations are those operations that occur between the end of evening civil twilight and the beginning of morning civil twilight, as published in the American Air Almanac, converted to local time (This is equal to approximately 30 minutes after sunset until 30 minutes before sunrise). The following guidelines shall be followed for all nighttime operations:

**4.2.2.1** A minimum of one pilot and at least one observer are required for all deployments.

**4.2.2.2** Night operations shall only be considered if the PIC provides a safety case and sufficient mitigation to avoid collision hazards at night. This must include a plan to stay below 400' AGL and above the highest known obstacle in the flight area. If the PIC cannot confirm hazards in the flight area night operations will not be authorized.

**4.2.2.3** Prior to conducting night operations the PIC and VO must be trained to recognize and overcome visual illusions caused by darkness, and understand physiological conditions which may degrade night vision. This training must be documented and must be presented for inspection upon request from the Administrator or an authorized representative. This documentation shall remain in the PIC's flight record.

**4.2.2.4** External pilots and observers must be in place 30 minutes prior to night operations to ensure sufficient dark adaptation (eye adjustment from seeing in the light to seeing in the dark).

**4.2.2.5** The PIC must conduct at least three takeoffs and three landings in the UAS that is to be deployed, at night, to a full stop, within the previous 90 days.

**4.2.2.6** The UAS must be equipped with lighted anti-collision lighting visible from a distance of no less than 3 statute miles. The intensity of the anti-collision lighting may be reduced if, because of operating conditions, it would be in the interest of safety to do so. Additionally, in order to comply with 14 CFR § 91.209, the aircraft must have position lighting that enables determination of location altitude, attitude, and direction of flight.

**4.2.3** No pilot may act as a PIC for more than 10 hours in any 24-hour period.

**4.2.4** Requests for deployment will be prioritized in a manner that has life safety as the main objective.

**4.2.5** Rules, regulations, policies, and procedures in place for flights within the Department's COA will remain as such should the UAS provide mutual aid to an allied agency.

**4.7.6** Mutual aid to an allied agency outside of the City of Boston, will occur only after obtaining FAA Part 107 authorization, or by obtaining an FAA SGI waiver authorization.

**4.2.7** The pilot is ultimately responsible for the UAS operation.

**4.2.8** No member of the Department (or other entity), regardless of rank, may order a pilot to:

- Accept a mission not in compliance with safety procedures
- Fly outside of FAA Part 107, the COA, or the UAS manufacturer's parameters
- Violate any rules or regulations that the PIC feels would put first responders, members of the public, or the flight team at a greater risk than is normally assumed with flight operations

**4.2.8.1** Should the pilot decline a mission, the pilot must inform the UAS Manager of the reason for declining the mission as soon as practicable

### **4.3 Deployment Rules**

**4.3.1** Requests for UAS deployments shall be made through the Boston Police Department Operations Division. Upon request the Operations Division shall immediately notify and relay all pertinent information to the UAS Manager, or the UAS Manager's designee, of the UAS request. The Pilot in Command will determine if the UAS can be deployed safely and practically and will either accept or decline the mission.

**4.3.2** Requests for deployment can be made at any time during the day or night

**4.3.3** The pilot will screen the request based on the following criteria

- Is the proposed mission of the UAS within the capabilities of the equipment and personnel to perform?
- Does the proposed mission fall within FAA Part 107 or COA requirements?
- Does the proposed mission fall within department rules, regulations, policies, and procedures?
- Can the UAS be deployed safely given the current and future weather conditions?

**4.3.4** If the mission is accepted, the following will take place when the pilot arrives on scene (if not already present)

- The Incident Commander and the pilot will conduct a face to face briefing
- The pilot will make an on-scene assessment of the conditions and determine if the UAS can fulfill the requested goals of the mission
- Normal pre-flight operations will be initiated including obtaining Part 107 authorization or the filing of a NOTAM when required by the COA

#### **4.4 Pre-flight**

**4.4.1** Every Department UAS will have a pre-flight checklist that is unique to that UAS and its capabilities. A laminated copy of the pre-flight checklist shall be kept with each system and a digital copy will be maintained by the UAS Manager. PICs shall strictly adhere to the UAS pre-flight checklist prior to flight.

**4.4.2** Before launch, a thorough pre-flight inspection must be completed by the designated PIC and VO.

#### **4.5 Weather**

**4.5.1** Before launch, a thorough check of the weather shall be conducted and all members of the flight team will be made aware of the findings.

**4.5.2** Weather information shall be obtained through an FAA Approved resource.

**4.5.3** Weather information obtained during flight operations shall be documented in the flight log.

#### **4.6 Post-flight**

- 4.6.1** After landing, a thorough post-flight inspection must be completed by the designated PIC.
- 4.6.2** The post-flight checklist that will be utilized to the fullest extent.
- 4.6.3** The PIC shall ensure the UAS batteries are recharged as soon as practicable after all UAS flights.

#### **4.7 Documentation**

- 4.7.1** After each mission and as soon as practicable, the PIC will download their flight to AirData log book or, if AirData is not compatible with the UAS, with equivalent software. In the note field the PIC will make note of all flight crew members, the weather conditions, whether the flight was under Part 107 (document the FAA authorization number) or under the FAA COA. The UAS Manager will retrieve a flight log report at the end of each month for FAA required reporting pursuant to the COA.
- 4.7.2** All pictures and videos captured during a mission involving a criminal investigation shall be collected and stored pursuant to Boston Police Department Rule 331.

#### **4.8 Communication Requirements**

- 4.8.1** When operations are in Class B and D airspace, the PIC must monitor the appropriate ATC frequency as assigned for situational awareness. However, ATC may require two-way frequency communications on a case-by-case basis. One of the crew members may monitor, so long as they maintain direct communication with the PIC at all times
- 4.8.2** For operations within 5 NM of any closed tower, non-towered airport, helipad, or water landing area the PIC must monitor and coordinate as necessary on the appropriate UNICOM, CTAF frequency.
- 4.8.3** If direct two-way communication is not required, Air Traffic Control Special provisions will be used in lieu of maintaining direct two-way Communications.
- 4.8.4** The PIC must, at all times, have a telephone available as backup communications.
- 4.8.5** Every UAS case shall be clearly marked with the appropriate frequencies that need to be monitored, to include, at a minimum: Logan Airport ATC 128.800 and helicopter frequency 123.025.

#### **4.9 Tactical Beyond Visual Line of Sight Operations**

- 4.9.1** In times of extreme situations, and to safeguard human life, the PIC may temporarily operate

UAS beyond visual line of sight to assess the operational environment, so long as:

- The PIC must not operate any higher than 50 feet above or greater than 400 feet laterally of the nearest obstacle. Combination of 50 feet above the obstacle must not exceed 400 feet AGL or the depicted UASFM value
- The UAS must remain within 1500 feet of the PIC
- The PIC will return to visual line of sight operations as soon as practical or upon termination of the threat

#### **4.10 Emergency Procedures/Operational Anomalies**

**4.10.1 Lost Link Procedures:** ATC does not need to be notified provided the PIC complies with the following provisions:

1. In the event the data link is lost for at least three (3) seconds: The UAS will execute the flight controller fail safe mode and climb to an altitude not exceeding the upper limits of the approved COA to attempt to re-establish link
2. If the link cannot be reestablished for a period of thirty (30) seconds:
  - a. The PIC must notify any ground assets that could be affected
  - b. The VO must be instructed to note bearing and approximate distance to commence recovery operations
  - c. The aircraft will fly back to the home point and land
3. The UAS will remain within the defined incident perimeter
4. The UAS will not interfere with the traffic pattern nor arrival/departure procedure of airports within the defined incident perimeter.
5. The PIC will notify the appropriate ATC facility within fifteen (15) minutes of the end of the flight.

**4.10.2 Line of Sight Loss:** If a Visual Observer loses sight of the UAS, unless operating in accordance with TBVLOS operations, the PIC must be notified immediately. If not, the PIC must immediately terminate the operation and notify the appropriate ATC facility within 15 minutes at the end of the flight. This is not applicable if a VO loses sight of a UA when it is being operated in a time of extreme emergencies to safeguard human life so long as the COA grants a 91.113 waiver.

**4.10.3 Loss of Communications between the PIC and VO:** If there is a loss of communication between the VO and PIC, the PIC will execute lost link procedures. If communications are reestablished, the mission may resume. If communication cannot promptly be reestablished, the flight must be terminated and the appropriate ATC facility notified no more than 15 minutes at the end of the flight.

**4.10.4 Loss of Communications between the PIC and ATC:** If direct communication between the PIC and ATC is required, in the event the PIC is unable to establish communications, the PIC will immediately land the UAS until communications can be regained.

**4.10.5 Fly away or Loss of Control:** In the event of a fly-away, the PIC will immediately notify the ATC facility with jurisdiction over the operations area. The PIC will provide the following information:

1. Altitude
2. Last known location
3. Direction of flight/heading
4. Fuel on board or battery time
5. PIC intentions
6. Termination of flight or emergency condition



## Section 5

# Maintenance

### **5.1 Preface**

Routine maintenance of Department UAS is integral to ensuring UAS are being deployed in the safest and most efficient manner.

### **5.2 Maintenance Procedures**

**5.2.1** All UAS aircraft, control systems, and equipment are required to be maintained and in operational condition prior to flight. Maintenance is, at a minimum, required to follow recommendations from the UAS manufacturer. All batteries must be recharged immediately following a UAS deployment.

**5.2.2** All UAS that have received mechanical, firmware, or software maintenance are required to perform a functional test. The system must be deemed airworthy before being used by the UAS Manager or designee.

**5.2.3** It is a requirement that any maintenance, whether scheduled or unscheduled, be documented in a UAS maintenance log. The maintenance log must be presented for inspection when requested by the UAS Commander.

### **5.3 Aircraft Registration**

All UAS aircraft must be registered with the FAA. The assigned aircraft registration number must be placed on the aircraft in a manner acceptable to the FAA.

### **5.4 Logs and Records**

#### **5.4.1 Pilot Log**

Every UAS Program member is required to maintain a pilot log with detailed entries of prior flight history.

The log is required to include the following information:

1. The flight date(s) of the project.
2. The aircraft model.
3. Time of flight.
4. A general description of the flight mission.

The pilot log shall be maintained in one electronic file for every flight.

The logbook of each pilot shall be maintained by the UAS Manager.

#### **5.4.2 Aircraft Maintenance Log**

Boston Police Department

---

Unmanned Aircraft System Operations Manual

A maintenance log must be kept for each UAS aircraft.

The log will document all scheduled and unscheduled maintenance to the aircraft.

The log will include the date of the maintenance and the specific maintenance or repair being done.

The maintenance log shall be maintained by the UAS Manager.

## Section 6 Miscellaneous

### **6.1 Preface**

Additional information, used to supplement Sections 1-5, can be found in this section.

### **6.2 Data Retention Policy**

Unauthorized use, duplication, and/or distribution of UAS digital media files is prohibited. All recorded digital media, images, and audio are property of the City of Boston and shall not be copied, released or disseminated in any form or manner outside the parameters of this policy without the authorization of the Police Commissioner or his or her designee.

1. **Prosecutorial / Law Enforcement Access:** Federal and State prosecutors shall make requests for UAS footage directly to the UAS Manager. In accordance with current practice, should any officer receive a subpoena for UAS footage, the officer shall direct the subpoena to the UAS Manager with a Form 26. The officer shall indicate in their Form 26 that a request for video has been made. Upon receipt of the request, the UAS Manager shall determine if the case has been assigned to a detective. If so, the Manager will notify the assigned detective and/or detective supervisor of the request. The detective and detective supervisor will then be responsible for providing all responsive and related case video directly to the Federal or State prosecutor.
2. **Public Records Requests:** All public records requests will be responded to in accordance with M.G.L. c. 66 and all other applicable laws and regulations. When practical, Department personnel will be advised prior to any release of UAS digital media files pursuant to a Massachusetts Public Records Request.
3. **Media Requests:** When Department personnel receive a request for UAS recordings from the media, the request shall be directed to the Office of Media Relations.

### **6.3 UAS Footage for Training Purposes**

1. A UAS digital media file may be utilized as a training tool for individuals, specific units, and the Department as a whole, so long as it is used for instructional purposes only.
2. Boston Police Department personnel requesting utilization of a UAS digital media file for training purposes shall submit the recommendation through the chain of command to the UAS Manager. Recordings may not be copied or sent beyond its training intent without the approval of the UAS Manager.

### **6.4 Retention timelines**

1. UAS footage is the sole property of the City of Boston and shall be retained per the Massachusetts Statewide Retention Schedule.

#### **6.5 Complaints:**

All complaints and concerns from the public and/or other agencies that are made to the PIC or any other crew members shall be immediately reported to the UAS Manager and forwarded to the appropriate Bureau.

## **AirMap App Part 107 FAA Authorization**

### **Electronic**

1. Open AirMap App
2. Enter your username and password
3. Drop Pin
4. Select flight area Click: **Next**
5. Enter required flight information
6. Submit flight
7. Document FAA authorization number.

## **NOTAM Filing Procedures**

### **Electronic**

1. Go to: **www.1800wxbrief.com**
2. Username:
3. Password:
4. Click **UAS** along top ribbon
5. Under **UAS Management**, click **Planning**
6. Enter required information
7. If including GPS coordinates, follow this format: xxxxxx.xNxxxxxx.xW

### **Telephone**

1. Obtain GPS coordinates prior to calling
2. Call **1-877-487-6867**
3. Enter **22**
4. Enter **1**
5. Speak to a **“Flight Data Specialist”**
6. Provide required information



**Technical Proposal for Subscription-Based  
Gunshot Detection, Location, and Forensic Analysis Service  
for the City of Boston**

**April 28, 2021**

**Proposal ID: EV00009078**

Submitted by: Jack Pontious, Director – Northeast Region  
202.258.0141 mobile  
703.940.1085 fax  
jpontious@shotspotter.com

ShotSpotter, Inc.  
VENDOR: 0000047809  
7979 Gateway Boulevard, Suite 210  
Newark, California 94560  
888.274.6877  
www.shotspotter.com

## Table of Contents

Executive Summary .....	1
Introduction .....	1
How it Works .....	4
Company History .....	5
Coverage Area .....	6
ShotSpotter Respond Service Overview .....	7
ShotSpotter Dispatch™ and ShotSpotter Respond™ Applications .....	7
ShotSpotter Insight™ .....	8
Mobile Alerts .....	10
Notifications API .....	11
Investigative Lead Summary .....	12
Detailed Forensic Reports and Expert Witness Testimony .....	13
Ongoing Customer Support .....	14
Response to Specifications .....	15
Staffing and Key Staff Qualifications .....	22
ShotSpotter Senior Management Team .....	22
ShotSpotter Project Team .....	24
References and Additional Information .....	25
Exceptions to IFB Instructions, Terms, and Conditions .....	26
Exhibit A - ShotSpotter Respond Services Agreement.....	28



## Executive Summary

### Introduction

ShotSpotter, Inc. is proposing ShotSpotter Respond™ (formerly ShotSpotter Flex™) gunshot detection, location, and forensic analysis service in response to this IFB. Delivered as a managed service, the City of Boston will simply continue its subscription to gunfire alert data with no downtime for installation, training, or testing of a new, unfamiliar system. As the incumbent vendor, ShotSpotter, Inc. will continue delivering gunfire incident data within the current ShotSpotter coverage area in the City of Boston, uninterrupted from day one of the term of this contract. Therefore, there is no need to submit a project work plan or schedule since this work has already been completed.

ShotSpotter has a long and successful track record with medium and large Public Safety Gunshot Detection/Location projects, including Metropolitan Police Department, DC; New York Police Department, NY; Chicago Police Department, IL; San Francisco Police Department, CA; and Oakland Police Department, CA among the largest deployments.

The City of Boston has been a customer since 2006, and ShotSpotter is highly familiar with technologies and network components used with ShotSpotter systems in Massachusetts and local governments. In addition to Boston and the Metro Boston Homeland Security Region (MBHSR), ShotSpotter has been successfully deployed in Springfield, Brockton, Worcester, Pittsfield, and New Bedford.

ShotSpotter currently owns 34 patents for Gunshot Detection/Location technology. ShotSpotter is a publicly traded company on the NASDAQ (SSTI). Financial statements are filed with the SEC and are available for inspection. Regardless, ShotSpotter is financially stable and is fully capable to undertake this project, as it did when ShotSpotter deployed Boston's original six square mile ShotSpotter system in 2006, and the MBHSR six square mile system in August 2014.

ShotSpotter has successfully delivered Gunshot Detection/Location services to over 100 customers both domestically and internationally since 1996.

The ShotSpotter gunshot detection, alert, and analysis services provide what would be otherwise unobtainable, critical real-time gunfire intelligence. The core capabilities of the ShotSpotter solution are:

- **DETECT** – ShotSpotter detects and locates gunfire incidents enabling a fast, precise response to over 90% of shooting incidents within the targeted areas. This has a powerful deterrent effect and disrupts the gun violence cycle.
- **PROTECT** – ShotSpotter helps to protect officers by providing them with comprehensive data on the actual amount of gunfire activity that occurs in the neighborhoods they patrol and provides critical situational awareness when responding to specific incidents.
- **CONNECT** – By applying community policing-oriented best practices, ShotSpotter provides a unique opportunity for law enforcement agencies to connect with vulnerable communities. Rapid response to gunfire incidents in communities that have been most impacted by gun violence builds positive attitudes towards law enforcement and leads to more constructive engagements and cooperation.

ShotSpotter has become an indispensable crime-fighting tool for these agencies, in light of the community dynamics that fuel gun violence and the well-documented challenges of relying solely on 9-1-1 calls for service:

- **Under-reporting of persistent gunfire:** Nationwide, on average, less than 20% of gunfire incidents are reported to 9-1-1. Why don't residents call? The answer is complex, but typically involves the following concerns:
  - Recognition: "Was that gunfire, fireworks, or something else?"
  - Retaliation: "If they find out I called, will they come after me?"
  - Resignation: "No one came the last time I called..."

Without ShotSpotter, most law enforcement agencies are working with an 80% to 90% deficiency in their gun violence-related intelligence.

- **Late and inaccurate information:** When a citizen reports a gunfire incident, the 9-1-1 call typically comes several minutes after the event has occurred, and based on analysis, the location provided is usually mislocated by 750 feet (on average). As a result, valuable time and resources are wasted trying to locate the incident, greatly diminishing the opportunity to identify suspects and witnesses, recover evidence, and, most important, render life-saving aid to victims.

The ability to receive near real-time gunfire intelligence data provides law enforcement agencies with a critical advantage in their efforts to reduce and prevent gun violence and improve officer safety. Specific results include:

- Officers can more quickly and more accurately go directly to the scene of the shooting.
- Situational awareness is vastly improved over what is available when relying solely on the 9-1-1 system.
- Law enforcement has a better chance of arriving before the shooter has left the scene.
- Officers are much more likely to find evidence in the form of shell casings (which, in conjunction with NIBIN/IBIS, provide valuable investigative leads) and/or other ground truth that can aid in the investigation.
- Officers are more likely to find witnesses who may have information that can aid in the investigation.
- Community engagement is heightened, which often translates into more information from the community (e.g., tip lines, field interviews, etc.)
- Targeted enforcement (precision policing) is enhanced.
- More court-admissible and scientifically sound forensic evidence is available to strengthen prosecutions of the worst offenders.

## How it Works

Based on an analysis of known gunfire-related crimes, the ShotSpotter team designs and deploys networked sensors within the targeted coverage area. These acoustic arrays detect and locate gunshot activity within the coverage area and report that information to ShotSpotter's Incident Review Center (IRC) which is staffed 24/7/365 by highly trained acoustic experts. ShotSpotter uses a two-factor incident review process to minimize false alerts. The first tier is performed by sophisticated AI software. Once the software has performed an initial review and filtered out any incidents that are determined not to be gunfire (e.g., helicopter noise, fireworks, etc.), the data is received at our IRC.

The IRC review process is performed by a team of highly trained acoustic experts. In addition to examination of the incident audio, the review process involves examination of visual characteristics of the detected pulses and the incident, such as the number of participating sensors, the wave form, pulse alignment, and the direction of sound. The IRC review results in publishing (Gunshot or Probable Gunshot) or dismissal (Non-Gunshot) of the incident with a high level of precision. If the reviewer classifies the incident as a gunshot, the reviewer sends an alert, including location information and an audio snippet, to law enforcement agencies via a password-protected application on a mobile phone, in-car laptop, or computer. In addition to the dot on the map and audio, ShotSpotter provides details such as number of shots fired, whether multiple shooters are involved, and whether high-capacity and/or fully automatic weapons are being used. This entire process (i.e., recording the impulsive sound, two-factor review, and publishing alerts to authorized users) is designed to take 60 seconds (but is often completed within 25 to 30 seconds).

ShotSpotter customers receive a contextually rich, detailed gunfire alert that enables a fast, precise, and safer response to gunfire incidents. In addition, ShotSpotter alerts can also trigger other technology platforms such as cameras that can pan and zoom in the direction of an event. ShotSpotter has also successfully integrated with a wide range of third-party applications such as CAD, RMS, License Plate Readers, drones, and other applications.

We look forward to working with the City of Boston and the Boston Police Department to continue delivering the benefits of ShotSpotter to your existing coverage area and to support your efforts to reduce gun violence in your communities.

## Company History

ShotSpotter was founded in 1995 and has been providing gunshot detection solutions since its inception. ShotSpotter is the world leader in gunshot detection, with nearly 750 square miles operational; more than 14 million incidents reviewed; and 34 issued patents. ShotSpotter is a publicly traded corporation (NASDAQ: SSTI) with approximately 100 full-time employees and is headquartered in Newark, California.

ShotSpotter provides precision-policing solutions for law enforcement to help deter gun violence and make cities, campuses, and facilities safer. Our flagship product, ShotSpotter Respond™, is the leading gunshot detection, location, and forensic analysis system, and is trusted by 100 cities. Other product offerings include:

- ShotSpotter SecureCampus®, designed to provide outdoor gunfire coverage at university and school campuses.
- ShotSpotter SiteSecure™ for critical infrastructure designed to detect gunfire attacks on commercial and federal buildings, electrical substations, airports, and large outdoor structures.
- ShotSpotter Connect™ (formerly Missions™), which uses artificial intelligence-driven analysis to help strategically plan patrol missions and tactics for maximum crime deterrence.
- ShotSpotter Labs, which focuses on innovative applications of ShotSpotter to help protect wildlife and the environment; currently helping combat rhino poaching in South Africa and will soon launch other applications for global wildlife protection, such as combatting illegal blast fishing in Malaysia with underwater sensors.



## Coverage Area

The perimeter of the “Phase I” deployment is denoted by a red boundary line in the image below. For reference purposes only, the blue boundary line denotes Boston “Phase II.” “Phase II” renewal pricing is not included or covered under this proposal.

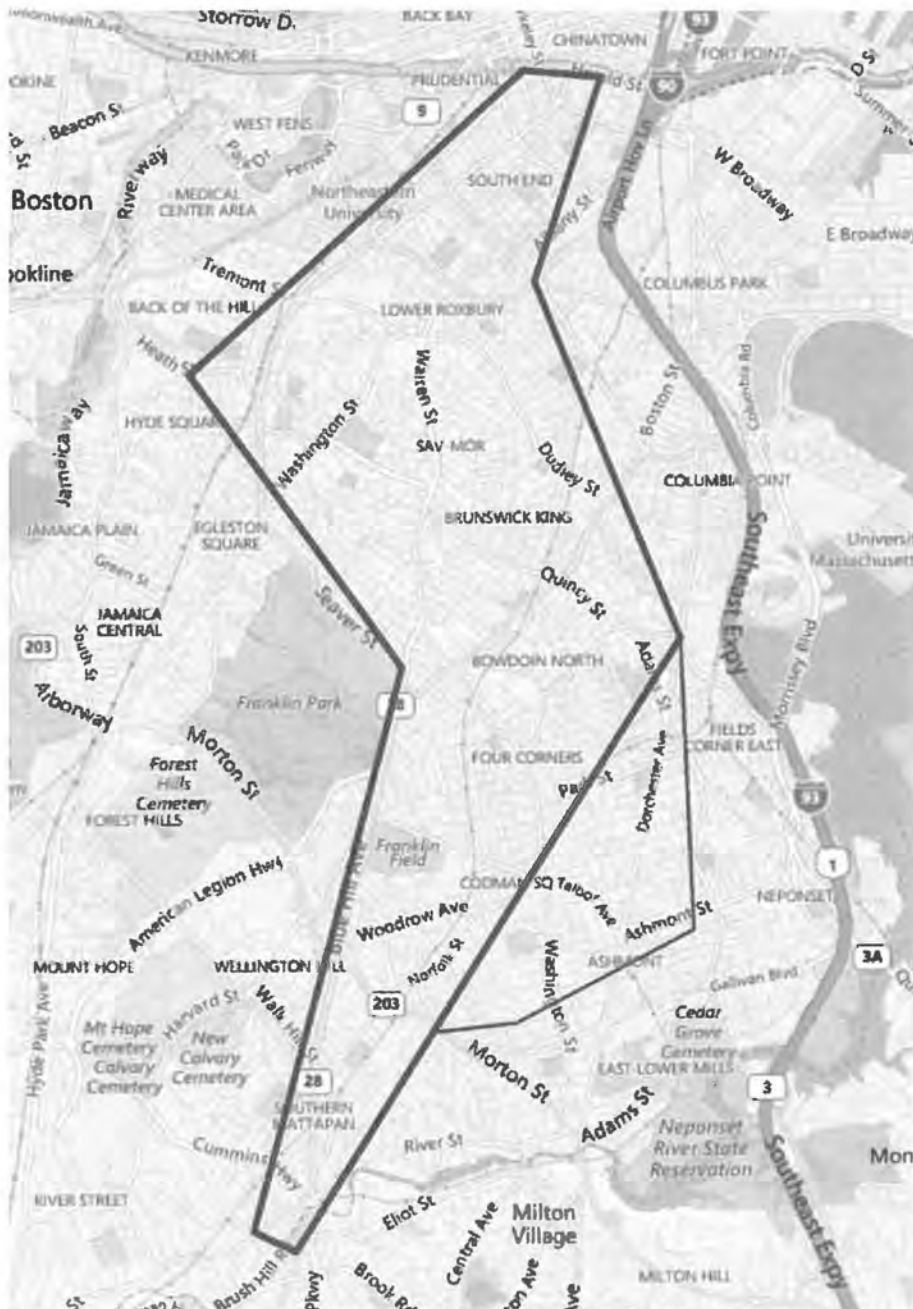


Figure 1: “Phase I” ShotSpotter Coverage (RED) = 6.0 mi<sup>2</sup>

“Phase II” ShotSpotter Coverage Expansion (BLUE) = 1.0 mi<sup>2</sup>

## ShotSpotter Respond Service Overview

ShotSpotter helps law enforcement agencies by directing resources to the precise location of more than 90% of gunfire incidents. ShotSpotter rapidly notifies first responders of shootings via dispatch centers, in-vehicle computers, and smart phones. Instant alerts enable first responders to aid victims, collect evidence, and identify witnesses. ShotSpotter's actionable intelligence can then be used to prevent future crimes by positioning law enforcement when and where crime is likely to occur. ShotSpotter gunshot detection and location services are delivered as an easily implemented Software as a Service (SaaS) solution, with no requirement for customer investment in or maintenance of expensive hardware or software. ShotSpotter hosts, secures, monitors, and maintains the ShotSpotter infrastructure. Contracts are based on an affordable one-year or multi-year subscription agreement, and the subscription includes unlimited licenses for the proposed ShotSpotter applications.

## ShotSpotter Dispatch™ and ShotSpotter Respond™ Applications

The ShotSpotter Dispatch and ShotSpotter Respond applications are used by Call Takers, Dispatchers, and Patrol Officers in the field. Real-time notifications of gunfire incidents are delivered to these apps and include the following data:

- Incident location (dot on the map)
- Type of gunfire (single round, multiple round)
- Unique identification number
- Date and time of the muzzle blast (trigger time)
- Nearest address of the gunfire location
- Number of shots
- District identification
- Beat identification



Figure 2: ShotSpotter Dispatch App

A ShotSpotter analyst may add other contextual information such as the possibility of multiple shooters, high-capacity weapons, full-automatic weapons, and the shooter's location related to a building (front yard, back yard, street, etc.). The report also includes an audit trail of the time the alert was published, acknowledged, and closed at the customer facility. All notes entered by Call Takers and Dispatchers added to the alert are time- and date-stamped with the operator's ID. For Patrol Officers, the alert includes an audio snippet of the incident.



**Figure 3: ShotSpotter Respond App**

### ShotSpotter Insight™

ShotSpotter Insight™ enables customers to explore details about prior gunshot incidents in their ShotSpotter coverage area and use the data for investigation and analysis. Crime analysts, investigators, and command staff can view, filter, sort, report, and transform historical gunshot data into meaningful insights, ultimately informing strategies for reducing gun violence.

Insight enables users to find and identify the incidents using an extensive array of filters for date, time, location, keywords, single vs. multiple gunshots, patrol areas, as well as shapes drawn on the map. The shape filters narrow a search for shooting incidents within a radius of a known address, across several blocks, or look for and monitor activity on both sides of a jurisdictional border. Saved reports retain common filter settings for quick retrieval (e.g., "District 4 Gunfire – Last 28 days").





**Figure 4: ShotSpotter Insight App**

Insight shows how a shooting event unfolded by watching a shot-by-shot animation that details the location and sequence of each shot. The software also highlights other nearby incidents that may be potentially related based on its relative distance and time of occurrence.

Insight comes with a set of reports that make it easy to share incident data throughout an agency:

- The Investigative Lead Summary report give details of a shooting incident including audio, location, sequence, and timing of each shot fired. This report is often used to share incident audio and details with colleagues, aid investigators with collecting evidence at the scene of a shooting and conducting better interviews of witnesses, suspects, and victims, or attach to a case file.
- The Multi-Incident report provides a summary of shooting incidents broken out by single, multiple, and probable gunshot incidents as well as any non-gunfire incidents if they were included in the search. The summary is followed by details for each incident including the date, time, location, number of rounds, CAD ID, Respond ID, and other details.

For custom ad hoc reporting and analysis, Insight can export incident data to other off-the-shelf products such as Microsoft Excel, Tableau, Google Earth, ArcGIS, and other tools.

## Mobile Alerts

Real-time gunfire alert data can be delivered to smart phones and smart watches via the Respond smartphone application, available for use on iPhones and Android platforms. The gunfire location is displayed as a dot on a map, and the data also includes the number of rounds fired and access to the incident audio.



Figure 5: Smart Watch Notification



Figure 6: ShotSpotter Respond App Smartphone Notification

## Notifications API

The ShotSpotter Notifications API allows client applications to receive accurate, timely details about ShotSpotter gunfire alerts, including precise latitude and longitude (geolocation), GPS-synchronized timestamps, incident audio, and situational context provided by the 24x7x365 ShotSpotter Incident Review Center. Typical integrations include:

- Video Management Systems (VMS)
- Computer-Aided Dispatch (CAD) systems
- Records Management Systems (RMS)
- Automated License Plate Readers (ALPRs)
- Crime analysis and statistics packages (including COMPSTAT software)

Each Notifications API license pack is available for an annual subscription fee that includes:

- Up to three (3) interfaces
- Establishing an instance of the API for the BPD on ShotSpotter-hosted servers
- Consulting with the BPD and third parties to ensure the API operates according to the API specifications
- 24x7 alerts to up to three third-party interfaces
- Supporting the third party and BPD as systems are upgraded

Additional API licenses can be purchased in packs of three interfaces.

## Investigative Lead Summary

ShotSpotter recently introduced a new, on-demand report available through the ShotSpotter Respond application. The Investigative Lead Summary (ILS) provides useful details about the location, timing, and sequence of each shot fired during an incident. The ILS is very valuable on scene, helping law enforcement find shell casings, confirm witness accounts, and identify suspects. ILS reports are available immediately after an incident occurs through a single click of a button within the mobile, web, or desktop ShotSpotter Respond application.

The ILS will fulfill the majority of law enforcement agency needs, particularly in situations where a report is not intended for presentation to court (since the ILS report is electronically produced, it is not court admissible).

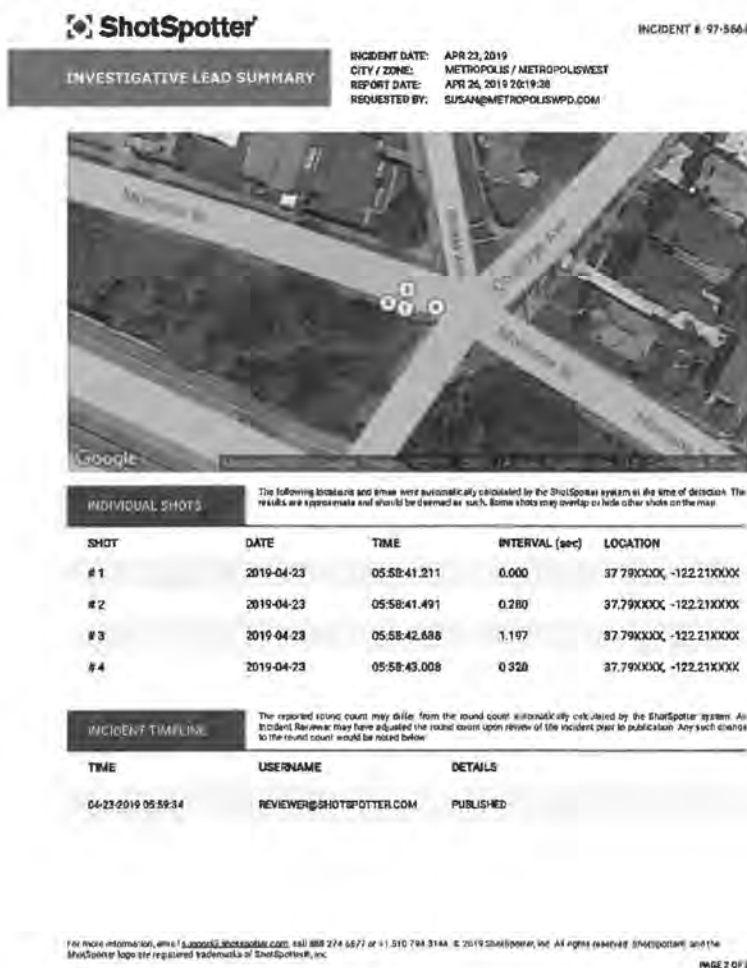


Figure 7: ShotSpotter Investigative Lead Summary (ILS)

## Detailed Forensic Reports and Expert Witness Testimony

In nearly all the criminal proceedings in which our experts have been called to testify, ShotSpotter has produced detailed, round-by-round analysis of the timing and location of the shots fired by one or more weapons. To the best of our knowledge, no other acoustic-based gunshot detection system has been accepted in a court of law as providing this kind of forensic evidence.

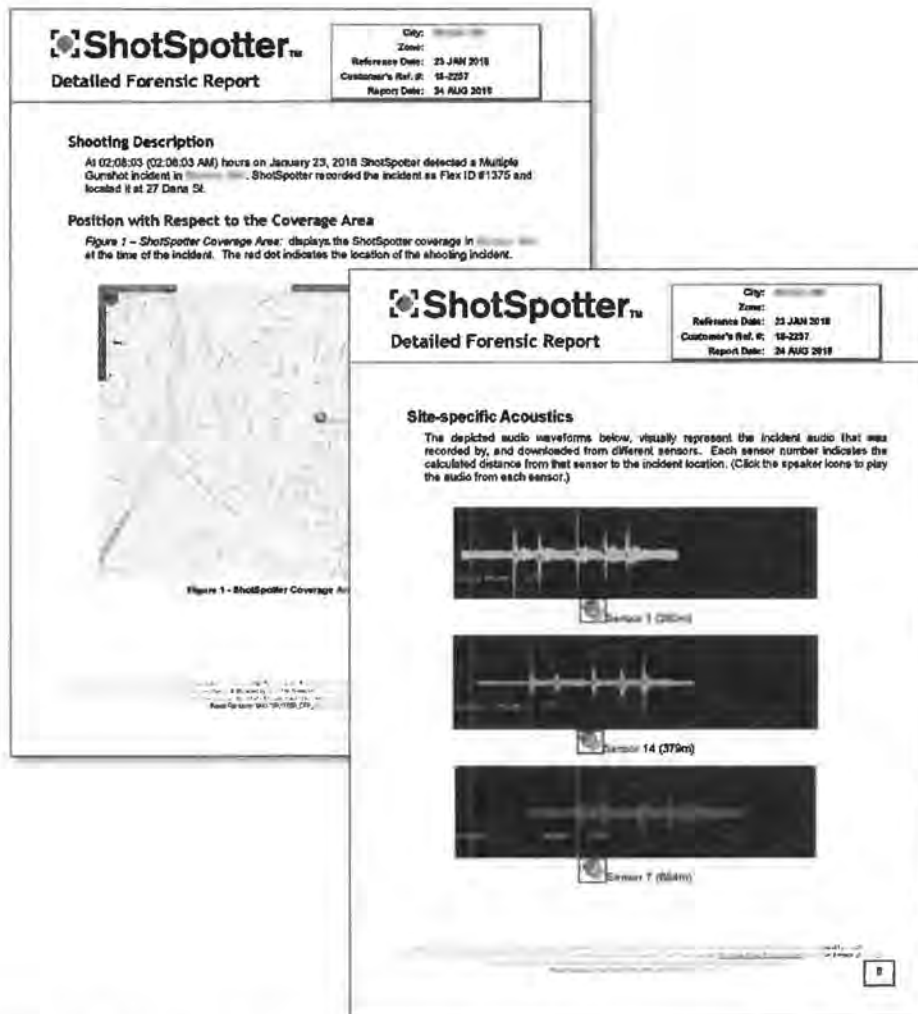


Figure 8: ShotSpotter Detailed Forensic Report (DFR)

ShotSpotter data supports detailed forensic analysis of gunfire incidents, including:

- Weapon type (e.g., automatic vs. semi-automatic)
- Number of rounds fired
- Possibility of multiple shooters

Unlike the ILS, the DFR is a court-admissible document prepared by our forensic engineers. The DFR is intended to be used by attorneys as part of a court case for the exact, verified timing, sequence and location of each shot fired. Secondly, DFRs are available for use by law enforcement to obtain search warrants or to investigate Officer Involved Shootings. DFRs are available upon written request, and our goal is to deliver all DFRs within ten business days of the request.

To support prosecutions, audio snippets provide powerful demonstrative evidence to prosecutors and allow jurors to gain a deeper understanding of the victims' experience of the incident. For prosecutors who wish to have a ShotSpotter expert witness testify regarding a DFR, to help interpret and clarify crime scene activity derived from ShotSpotter data, or provide other forensic consultation services, these services are available for an hourly fee.

In 17 states and in the District of Columbia, ShotSpotter evidence and ShotSpotter expert witness testimony have been successfully admitted in over 100 court cases. ShotSpotter forensic evidence has prevailed in nine Frye challenges, including four in California, and five Daubert challenges throughout the United States.

## Ongoing Customer Support

ShotSpotter standard customer support includes 24/7 assistance with user accounts, software interface, tools, features, incident (re)classification, and review. Tier 1 Support is provided by our Incident Review Center (IRC). IRC staff have extensive experience with ShotSpotter applications and provide real-time support of basic issues, and first level of support for information gathering and triage for advanced troubleshooting by Tier 2 Support. The Tier 2 Support Team comprises technically advanced, experienced Customer Support professionals who are responsible for advanced levels of troubleshooting and analysis, IT Support, mapping issues, etc.

Support Level	Tier 1 Support (IRC)	Tier 2 Support (Customer Support)
<b>Features</b>	<ul style="list-style-type: none"> <li>• Login support</li> <li>• Report a misclassification</li> <li>• Report a missed incident</li> <li>• Report a mislocated incident</li> <li>• Basic audio request</li> <li>• General/application questions</li> <li>• Request for ILS</li> </ul>	<p>Normal Support:</p> <ul style="list-style-type: none"> <li>• Analysis of missed gunshots</li> <li>• Detailed audio search</li> <li>• Performance analysis</li> <li>• Integration issues</li> </ul> <p>Critical Support:</p> <ul style="list-style-type: none"> <li>• System outage</li> </ul>
<b>Hours of Operation</b>	24x7x365	<p>Normal Support: 5 am – 11 pm Pacific Time Zone</p> <p>Escalation: 24x7x365</p>



## Response to Specifications

### Response Terminology

ShotSpotter has responded point by point to the IFB requirements using the following response terminology:

Response Terminology	Definition
Understood	ShotSpotter has read and understands the requirement.
Complies	ShotSpotter's response complies with the requirement.
Partially Complies	ShotSpotter's response partially complies with the requirement; specific exceptions or deviations are described in detail.
Exception	ShotSpotter's response does not comply with the requirement.
Alternative Method	ShotSpotter's response provides an alternative methodology, described in detail, which meets the intent of the requirement.

#### IFB Requirement

- Gunshot Detection System and Location System
  - Utilization of sensor network to provide gunshot detection/location coverage for the Shotspotter [sic] Coverage Area shown above.

#### ShotSpotter Response: Complies

ShotSpotter has already deployed six square miles of ShotSpotter Respond (formerly Flex) coverage within the red-outlined geographic area illustrated in Figure 1 on page 6.

#### IFB Requirement

- The system must produce the precise time, location, and audio snippet associated with impulsive noise that may represent a gunshot

#### ShotSpotter Response: Complies

This is standard functionality of the ShotSpotter Respond service.

#### IFB Requirement

- Incident alerts provided directly to department's desired endpoints from the acoustic sensors

#### ShotSpotter Response: Complies

This is standard functionality of the ShotSpotter Respond service.

**IFB Requirement**

- Viewable mapping identification allowing for geo-location of gunfire and explosive events

**ShotSpotter Response: Complies**

The ShotSpotter Dispatch, Respond, and Insight apps feature Google Maps, including road aerial, and “street view” map views.

**IFB Requirement**

- Complete turnkey workstations for BPD’s dispatch center

**ShotSpotter Response: Complies**

ShotSpotter delivers gunfire alert data through standard web browsers and smartphone apps. ShotSpotter will not be providing any workstation hardware or software as a part of this proposal.

**IFB Requirement**

- Vendor must integrate new systems with the department’s existing Critical Infrastructure Monitoring System, future camera systems in the region, and CAD systems

**ShotSpotter Response: Complies**

The City of Boston has already purchased the ShotSpotter Notification API license which may be used by the City of Boston to integrate/interface with third party systems.

**IFB Requirement**

- Mobile Capabilities
  - Mobile specific software for patrol units

**ShotSpotter Response: Complies**

ShotSpotter Respond apps are specifically designed for use by patrol units.



**IFB Requirement**

- Integrated capable system (iOS, Android, etc.)

**ShotSpotter Response: Complies**

ShotSpotter Respond, Dispatch, and Insight apps are compatible with Microsoft Windows PCs, in addition to iOS and Android based smartphones.

**IFB Requirement**

- Management system software to support operations
  - Direct reporting to the department's dispatch centers/patrol units, including the precise time, location and audio snippet associated with impulsive noise that is likely to represent a gunshot.
  - Viewable mapping software or integration with Google Maps or other standard mapping platform.
  - District and Area specific incidents identification for multiple dispatch stations/channels.
  - Audio playback capabilities.
  - Able to generate statistical reports of incidents.
  - Viewable sound wave pattern screen at the workstations.
  - Vendor must have the ability to detect gunshots within the coverage area.
  - Vendor must have the ability to send all alerts (including fireworks)
  - Vendor must have the ability to show all impulsive noise system activations, whether detected as gunshot or not.

**ShotSpotter Response: Complies**

The ShotSpotter Insight™ app supports all the features listed above.

**IFB Requirement**

- Vendor participation in:
  - Onsite training as well as unlimited phone support

**ShotSpotter Response: Complies**

ShotSpotter has already completed a comprehensive training program for both users and trainers of the BPD. 24x7 ShotSpotter support is offered through an online chat feature, or BPD can call toll-free for phone support.

**IFB Requirement**

- Service/Warranty/Maintenance
  - 24/7 emergency number for critical incidents with on-site response when required.
  - 8 hour/5 days a week non-critical issues.
  - Remote online monitoring of the sensors/system by the vendor.
  - Maximum 24 hour response for non-critical system components (weekdays).
  - Minimum 1 year warranty upon completion

**ShotSpotter Response: Complies**

ShotSpotter support levels are detailed in Exhibit B of the ShotSpotter Respond Services Agreement included in Exhibit A of this proposal response.

**IFB Requirement**

- Provide a list of recommended spare parts list to include quantity and unit prices.
- Warranty for all equipment and software installation work for a minimum of one (1) year after system acceptance. Warranty shall include all parts, labor, and travel necessary to return the equipment to its original working condition.
- Automated notification to department via text or email in the event of a sensor outage within 15 minutes

**ShotSpotter Response: Complies**

There is no hardware offered as a part of this proposal. All gunshot data is delivered as a fully managed service. ShotSpotter owns, monitors, and maintains all sensor equipment deployed in the coverage areas. The sensor array will be maintained at service levels as outlined in the ShotSpotter Respond Services Agreement. Planned system maintenance windows and critical

system outage notifications are delivered to Dispatch and Respond apps.

**IFB Requirement**

- System hardware

**ShotSpotter Response: Complies**

There is no hardware offered as a part of this proposal. All gunshot data is delivered as a fully managed service.

**IFB Requirement**

- System software (to include upgrades/updates)

**ShotSpotter Response: Complies**

All gunshot data is delivered as a fully managed service. Access to the service is delivered through common browser software and/or smartphone application. All upgrades and updates are automatically pushed out to all ShotSpotter users.

**IFB Requirement**

The Contractor will work at the programmatic direction of the BPD Shotspotter program manager group and under the administrative and financial direction of the BPD.

**ShotSpotter Response: Understood****IFB Requirement**

The Contractor will collaborate with the BPD IT and any contractor or vendor of the City to establish/support the gunshot detection and location services system.

**ShotSpotter Response: Understood**

**IFB Requirement**

The Contractor shall provide the most cost-effective solution to BPD, providing that such a solution meets the minimum requirements listed above. Specific requirements and services are to be completed include, but are not limited to, the following:

- Technical consulting including network infrastructure, equipment installation, training, maintenance.

**ShotSpotter Response: Complies**

ShotSpotter will provide technical consulting, documentation, and training as required. ShotSpotter owns and maintains the acoustic sensors, therefore, there is no network, installation, or maintenance training is necessary for the BPD.

**IFB Requirement**

- Network engineering in support of the Gunshot Detection/Location system;

**ShotSpotter Response: Complies**

ShotSpotter will deliver ShotSpotter Respond as a managed service. As such, the only networking requirements are for the BPD is to ensure workstation connectivity through the internet to the ShotSpotter secure hosted server.

**IFB Requirement**

- Network operations support to include fault resolution assistance and network administration function performance;

**ShotSpotter Response: Complies**

ShotSpotter ensures the hosted ShotSpotter Respond service is fault tolerant. However, ShotSpotter does not provide internal network operations support. This is the responsibility of the BPD.

**IFB Requirement**

- Furnishing certain necessary equipment, hardware, labor, and procedures to direct support Gunshot Detection/Location;

**ShotSpotter Response: Complies**

ShotSpotter will provide support as outlined in Exhibit B of the ShotSpotter Respond Services

Agreement (included as Exhibit A of this proposal).

**IFB Requirement**

- Managing the security design and implementation, ensuring various technical standards, configuring device setup and providing other configuration services and training.

**ShotSpotter Response: Complies**

ShotSpotter will provide support as outlined in Exhibit B of the ShotSpotter Respond Services Agreement (included as Exhibit A of this proposal). ShotSpotter cannot provide security design of the networks owned by the BPD.

## Staffing and Key Staff Qualifications

### ShotSpotter Senior Management Team

**Ralph A. Clark - President and Chief Executive Officer**

rclark@shotspotter.com (LinkedIn Profile)

Ralph A. Clark brings 30 years of extensive corporate, financial and organizational leadership to his position as ShotSpotter, Inc.'s President and Chief Executive Officer. Most recently, Clark was CEO of GuardianEdge Technologies Inc., where he led the transformation of the company into a leader in endpoint data protection and was instrumental in its acquisition by Symantec.

Prior to GuardianEdge, Clark served as Vice President of Finance for Adaptec through its acquisition of Snap Appliance, which he helped engineer. He was responsible for worldwide financial planning and analysis of Snap Appliance, serving as its Chief Financial Officer. Previous to his role at Snap Appliance, he worked at several venture capital backed start-up companies, leading several to successful acquisitions. Early in his career, Clark held executive sales and marketing roles at IBM; post business school he was an investment banker at Goldman Sachs and Merrill Lynch.

He is a member of the board of directors Tactical Survey Group, and also serves as Chairman of The Board of Pacific Community Ventures. Clark holds a bachelor's degree in economics from the University of the Pacific, and a master's degree in business administration from Harvard Business School.

**Gary Bunyard – Senior Vice President, Public Safety Solutions**

gbunyard@shotspotter.com (LinkedIn Profile)

Gary brings a solid 30-year record of senior leadership experience in sales and general management to ShotSpotter. Most recently he was the Vice President of Sales for TriTech Software Systems. He was formerly the President and CEO of Tiburon and also lead the sales organization of the Vision Air. His unique combination of scaling enterprise sales organizations and executing value based selling techniques extend and compliment ShotSpotter's customer relationship driven philosophy.

Gary leads the public safety sales organization along with our customer training/success/onboarding team.

**Paul Ames - Senior Vice President, Products and Technology**

pames@shotspotter.com (LinkedIn Profile)

Paul Ames, a 25-year technology veteran, leads ShotSpotter's product development, software, hardware, and operational engineering teams. Before ShotSpotter, he founded Deckchair Software LLC, to conceive, develop and market consumer facing mobile apps. At Premier Retail Networks (PRN), a division of Technicolor, Ames served as Vice President of Product Development, responsible for driving development of a \$100MM yearly revenue video advertising platform. Paul started his career in the UK and has held senior technology leaderships roles across a broad range of industries including communications, financial, professional information, and media.

He received his Computer Science education at the Polytechnic of South Wales and post graduate studies in Electronic Sound at University College, Cardiff.

**Nasim Golzadeh - SVP of Customer Support and Professional Services**

mgolzadeh@shotspotter.com (LinkedIn Profile)

Nasim brings a rich history of leading and scaling public safety technology customer support and professional services organizations in her 15+ years at TriTech Software Systems. Her passion for customers and cross functional collaboration skills are very important assets to ShotSpotter's efforts as we continue to add new customers and new capabilities. As a Senior Vice President, Nasim reports directly to the CEO.

**Mike Will - VP of Customer Support**

mwill@shotspotter.com (LinkedIn Profile)

Mr. Will is responsible for delivery and oversight of ShotSpotter Customer and Technical Support, including remote monitoring and management of the ShotSpotter sensor network and fulfillment of all customer service requests from basic technical support to forensic data services, gunshot investigation support, and expert witness testimony for ShotSpotter Respond customers. Mr. Will has over 25 years of experience delivering customer service and technical support for terrestrial and wireless data and telecommunications networks. Mr. Will holds a bachelor's degree in Computer Science.



## ShotSpotter Project Team

### **Jeffery A. Magee – Director, Customer Success**

[jmagee@shotspotter.com](mailto:jmagee@shotspotter.com) (LinkedIn Profile)

The mission of Customer Success is to work with ShotSpotter agencies to ensure they are utilizing the full potential of our gunfire detection system. More importantly, it is our goal that clients are combining the benefits of timely & accurate gunfire notifications provided by ShotSpotter, with other effective strategies to identify violent offenders and hold them accountable.

Mr. Magee is an accomplished and proven law enforcement professional and expert criminal investigator with 25 years of service to the Departments of Justice and Treasury. He has demonstrated ability to implement and manage strategic mission-oriented programs related to Federal alcohol, tobacco, firearms, explosives, and arson laws and regulations and to the personnel who carry out the ATF mission. He is a well-regarded leader employing open-mindedness, positivity, empathetic listening, and creative problem-solving to mitigate risk, address challenges, reduce costs, and produce results. He is a proven, trusted, and decisive leader with high social and emotional intelligence who has worked consistently in diverse high-stress environments. He has a known ability to work well with anyone and to form and galvanize teams to accomplish a mission. He has a long history of senior executive service with sustained outstanding demonstration of core competencies.

### **Doris Cohen – Manager, Customer Success - Analysis**

[dcohen@shotspotter.com](mailto:dcohen@shotspotter.com) (LinkedIn Profile)

Working in conjunction with the Customer Success Director and closely with the customer, responsible for ShotSpotter Program Development and training for ShotSpotter customers, including specialized training and "best practices" consultation for Trend Analysis, Hotspot Mapping, and Forecasting. Ms. Cohen has over 20 years of experience working as a crime analyst with law enforcement departments throughout northern California and five years of experience as ShotSpotter Manager of Training. Ms. Cohen holds a master's in emergency services administration and a Bachelor's in Public Administration. She is actively involved in the Bay Area Crime and Intelligence Analysts Association (BACIAA) and was the Vice President from 2011-2014.



## References and Additional Information

ShotSpotter has more than 100 customers covering more than 750 square miles. ShotSpotter is the leader in the development and deployment of wide area acoustic gunshot detection and location systems. Today, ShotSpotter provides gunshot detection and location services to law enforcement agencies across the country.

Among these are:

**New Haven Police Department, CT (2009 to Present)**

One Union Avenue, New Haven, CT 06519

Assistant Chief Karl Jacobson (kjacobson@newhavenct.gov, 203.946.6294)

Coverage Area: 5.5 square miles

**Pittsfield (MA) Police Department (2017 to Present)**

39 Allen Street, Pittsfield, MA 01201

Chief Michael Wynn (mwynn@cityofpittsfield.org, 413.448.9700 x.717)

Coverage Area: 3.0 square miles

**Worcester (MA) Police Department (2014 to Present)**

9-11 Lincoln Square, Worcester, MA 01608

Deputy Chief Paul B. Saucier (SaucierPB@worcesterma.gov, 508.799.8693 x.28320)

Coverage Area: 6 square miles

## Exceptions to IFB Instructions, Terms, and Conditions

### IFB Requirement

#### 3.3 *Failure Of Performance; Liquidated Damages*

If the successful bidder fails to perform his agreement to execute a contract and furnish the required security for performance within ten (10) days (Saturdays, Sundays and legal holidays excluded) after an award is made, or within such additional time as the Official may authorize in writing, the bid deposit shall become and be the property of the City of Boston as liquidated damages; provided, that the amount of the bid deposit which becomes the property of the City shall not, in any event, exceed the difference between the bidder's price and the price of the next lowest eligible and responsible bidder; and provided further, that, in case of death, disability or other unforeseen circumstance affecting the bidder, the bid deposit shall be returned to the bidder after submission of a sworn affidavit delivered to, and accepted by, the Official.

#### ShotSpotter Exception to Section 3.3:

The City of Boston is an existing end user customer of ShotSpotter's gunshot location and detection system, which is provided on a software as a service, subscription basis. ShotSpotter's proposal is for the City's ongoing use, and ShotSpotter's support of the subscription services, which will be provided in accordance with ShotSpotter's Respond (formerly Flex) Services Agreement, a copy of which is provided as Exhibit A to this proposal. ShotSpotter respectfully proposes that section 3.3 is not applicable.

### IFB Requirement

#### 12. PERFORMANCE BOND

12.1 A performance bond of a surety company authorized to do business in Massachusetts and satisfactory in form to the Official, or a certified check, or a treasurer's or a cashier's check, issued by a responsible bank or trust company, payable to the City of Boston, may be required of the successful bidder as security to guarantee the faithful performance of the contract. If security is required, the penal sum of such bond or amount of such check shall be as specified in the Advertisement.

12.2 Simultaneously with the execution of the contract, the successful bidder shall deliver such bond or other security to the Official. Failure to provide the required bond or other security within the time herein specified in paragraph 11.3 shall render the contract award void and result in the forfeiture of the bid deposit as liquidated damages.

**ShotSpotter Exception to Section 12:**

As an existing end user customer of ShotSpotter's gunshot location and detection system, ShotSpotter's proposal is for the City of Boston's continued use, and ShotSpotter's ongoing support of, the subscription services rather than a new project implementation. As such, ShotSpotter respectfully proposes that section 12 is not applicable. ShotSpotter will continue to provide the subscription services in accordance with ShotSpotter's Respond (formerly Flex) Services Agreement, a copy of which is provided as Exhibit A to this proposal.

**Exhibit A - ShotSpotter Respond Services Agreement**

The proposed services will be delivered according to the terms of ShotSpotter's Respond Services Agreement, to be incorporated as an exhibit to the City of Boston Standard Contract General Conditions and its Supplemental Information Technology Terms and Conditions. A copy of ShotSpotter's Respond Services Agreement is attached as an exhibit to this proposal.

**RESPOND SERVICES AGREEMENT**



**ShotSpotter, Inc.**  
**7979 Gateway Blvd., Suite 210**  
**Newark, California 94560**  
**+1.888.274.6877**  
**[info@shotspotter.com](mailto:info@shotspotter.com)**  
**[www.shotspotter.com](http://www.shotspotter.com)**

## Contents

1.	EXHIBITS .....	1
2.	DEFINITIONS .....	1
3.	SUBSCRIPTION SERVICES .....	2
4.	INITIAL TERM AND RENEWAL .....	4
5.	LICENSE, OWNERSHIP, AND DATA RIGHTS .....	4
6.	CONFIDENTIALITY AND PROPRIETARY RIGHTS .....	7
7.	LIMITED WARRANTIES .....	9
8.	CUSTOMER OBLIGATIONS. ....	10
9.	INTELLECTUAL PROPERTY INFRINGEMENT .....	11
10.	INDEMNIFICATION AND LIMITATION OF LIABILITY .....	12
11.	DEFAULT AND TERMINATION; REMEDIES .....	13
12.	TAXES .....	13
13.	NOTICES .....	13
14.	FORCE MAJEURE .....	13
15.	ENTIRE AGREEMENT .....	14
16.	GOVERNING LAW .....	14
17.	NO WAIVER .....	14
18.	SEVERABILITY .....	14
19.	DISPUTE RESOLUTION .....	14
20.	ASSIGNMENT .....	14
21.	GENERAL PROVISIONS .....	15
	EXHIBIT A – SHOTSPOTTER PROPOSAL .....	16
	EXHIBIT B – SERVICE LEVEL AGREEMENT .....	17

This ShotSpotter® Respond™ Services Agreement (this "Agreement") is entered into by and between ShotSpotter, Inc. (referred to herein as "ShotSpotter"), with offices located at 7979 Gateway Blvd., Suite 210, Newark, CA 94560 and the City of Boston (hereinafter referred to as "Customer"), with offices located at One City Hall Square, Boston, MA 02201, effective as of the last date of signature herein. ShotSpotter and Customer may also be referred to in this Agreement individually as a "Party" or collectively as the "Parties".

This Agreement and its exhibits define the deliverables, implementation, and subscription services for ShotSpotter's gunshot location system ("ShotSpotter® Respond™ Gunshot Detection, Location, and Forensic Analysis Service") to be provided under this Agreement.

In consideration of the Parties' mutual covenants and promises set forth in this Agreement, the Parties agree as follows:

## 1. EXHIBITS

The following exhibits ("Exhibits") are attached to, and incorporated in this Agreement:

- A. ShotSpotter Proposal ID # EV00009078
- B. Service Level Agreement

## 2. DEFINITIONS

All capitalized terms not otherwise defined in this Agreement shall have the meanings set forth below:

- A. Insight means the internet portal to which Customer will have access to Reviewed Alerts.
- B. Confidential Information means that information designated by either Party as confidential or proprietary as further defined in Section 6 of this Agreement.
- C. Coverage Area means the area in square miles covered by the Services as set forth in Exhibit A and any subsequent amendments thereto.
- D. Data means all data created, generated, modified, compiled, stored, kept, or displayed by ShotSpotter in performance of the Subscription Services, including the Software.
- E. Reviewed Alerts means the data reviewed by ShotSpotter's incident review staff related to gunfire incidents detected by the ShotSpotter Gunshot Detection, Location, and Forensic Analysis Service.
- F. ShotSpotter Respond System means the ShotSpotter Respond Gunshot Detection, Location, and Forensic Analysis Service provided on a subscription basis under this Agreement.
- G. Software means the ShotSpotter Respond Gunshot Detection, Location, and Forensic Analysis Service, Reviewed Alerts, ShotSpotter Respond™, and ShotSpotter Dispatch™ and ShotSpotter® Insight applications to which Customer will have access under this Agreement on a subscription basis. The term Software shall also mean any new applications supplemental to the Subscription Services provided by ShotSpotter to Customer subsequent to the execution date of this Agreement, and if purchased by Customer, the ShotSpotter API Subscription License.



H. Subscription Services means the services provided to Customer on a subscription basis to access, and ShotSpotter's maintenance of, the Software.

I. System means collectively the Software and Subscription Services provided under this Agreement.

### 3. SUBSCRIPTION SERVICES

A. ShotSpotter will install the ShotSpotter Respond System in the Coverage Area specified in Exhibit A attached to this Agreement. ShotSpotter will host the Subscription Services and may update the functionality and Software of the Subscription Services from time to time at its sole discretion and in accordance with this Agreement.

B. ShotSpotter will be responsible for determining the location(s) for installation of acoustic sensor(s) (the "Sensors") that detect gunshot-like sounds, and obtaining permission from the premises owner/property manager/lessee.

C. The ShotSpotter Respond System acoustic Sensor may use wired, wireless, or cellular wireless communications which necessitates the existence of a real-time data communications channel from each Sensor to the ShotSpotter hosted servers via a commercial carrier. The unavailability or deterioration of the quality of such wired, wireless, or wireless cellular communications may impact the ability of ShotSpotter to provide the Subscription Services. In such circumstances ShotSpotter will use commercially reasonable efforts to obtain alternate wired or wireless cellular communications or adjust the coverage area as necessary. In the event ShotSpotter is unable to do so, ShotSpotter will terminate the Subscription Services and refund a pro-rata portion of the annual Subscription Services fee to Customer.

D. ShotSpotter will provide Customer with user documentation, online help, written or recorded video training material, and other applicable documentation (as available).

E. ShotSpotter will provide reasonable efforts to respond via email to requests for support relating to incident classification as defined in the Support Level Matrix provided in Exhibit B.

F. During the term of this Agreement, ShotSpotter will provide real-time gunfire analysis and alert services. After an explosive (or impulsive) sound triggers enough ShotSpotter Sensors that an incident is detected and located, audio from the incident is sent to the ShotSpotter Incident Review Center (IRC) via secure, high-speed network connections for real-time qualification. Within seconds, a ShotSpotter professional reviewer analyzes audio data and recordings to confirm gunfire or explosions. The qualified alert is then sent directly to the Customer's dispatch center, PSAP, mobile/patrol officers, and any other relevant safety or security personnel, as determined by the Customer. ShotSpotter's IRC will review gunfire incidents as further defined in Exhibit B.

G. The Subscription Services provided under this Agreement shall consist of (i) providing access to the Customer of Reviewed Alerts delivered via the Insight password-protected internet portal and user interface supplied by ShotSpotter; (ii) providing Customer access to historical Reviewed Alerts and incident information via the Software; and (iii) other services as specified in this Agreement and its Exhibits.

H. ShotSpotter will use commercially reasonable efforts to respond to support requests as set forth in the Support Level Matrix provided in Exhibit B. These requests may be made to ShotSpotter



through one of the following methods: 1) email to [support@shotspotter.com](mailto:support@shotspotter.com); 2) Live Chat through our ShotSpotter applications; 3) A phone call to our Customer Support organization at 888,274.6877, option 4. These are the only methods ShotSpotter will receive and respond to support requests.

A Tier 1 (as defined in the Support Matrix in Exhibit B) ShotSpotter Customer Support specialist will be responsible for receiving Customer reports of missed incidents, or errors in the Subscription Services, and, to the extent practicable over email or telephone, making commercially reasonable efforts to assist the Customer in resolving the Customer's reported problems. In the event the problem cannot be resolved within 24 hours, requiring further research and troubleshooting, ShotSpotter will use commercially reasonable efforts to resolve the issue within seventy-two (72) hours of receipt of the report. In the event that the ShotSpotter service is fully nonfunctional, and it is not due to power outage or other reasons that are outside of ShotSpotter's control, ShotSpotter will work continuously to restore functionality of the Subscription Services in accordance with the standard ShotSpotter user documentation provided with the Subscription Services as soon as reasonably possible, and no later than seventy-two (72) hours of receipt of the report.

#### I. FORENSIC REPORTS.

- i. Investigative Lead Summary ("ILS"). ShotSpotter provides an on-demand report available through the ShotSpotter Respond Application. The Investigative Lead Summary (ILS) provides useful details about the approximate location, timing, and sequence of each shot fired during an incident. The ILS is very valuable on scene, helping law enforcement find shell casings, confirm witness accounts, and identify suspects. ILS reports are available immediately after an incident occurs via the mobile, web, or desktop ShotSpotter Respond application (machine-generated). The ILS is not a court-admissible document.
- ii. Detailed Forensic Report ("DFR"). If requested by Customer, ShotSpotter will provide a DFR for any ShotSpotter-detected incidents, including Reviewed Alerts. The DFR is intended to be a court-admissible document used by attorneys as part of a court case for the exact, verified timing, sequence and location of each shot fired. Secondly, the DFR is available for use by law enforcement to obtain a search warrant or to investigate an Officer Involved Shooting.

DFRs must be requested in writing and addressed to the ShotSpotter Customer Support Department. Requests may be submitted via the Forensics Services page under the Law Enforcement tab on ShotSpotter's website ([www.shotspotter.com](http://www.shotspotter.com)). ShotSpotter will use commercially reasonable efforts to provide a DFR within ten (10) business days of receipt of the request.

#### J. EXPERT WITNESS SERVICES.

ShotSpotter offers reasonable expert witness services, including Reviewed Alerts, for an hourly fee as set forth in Exhibit A, as well as reimbursement of all travel and per diem costs. If requested to provide such services, ShotSpotter will invoice the Customer for the number of hours expended to prepare for and provide expert witness testimony, and actual travel expenses, upon completion of the services. Customer understands that ShotSpotter undertakes to provide individuals whose qualifications are sufficient for such services, but does not warrant that any person or his or her opinion will be accepted by every court. ShotSpotter requires at least fourteen (14) days prior notice

of such a requirement in writing from the Customer. Customer must include dates, times, specific locations, and a point of contact for ShotSpotter personnel. Due to the nature of legal proceedings, ShotSpotter cannot guarantee that its services described in this section shall produce the outcome, legal or otherwise, which Customer desires. Payment for expert witness services described shall be due and payable when services are rendered regardless of the outcome of the proceedings.

#### 4. INITIAL TERM AND RENEWAL

Unless otherwise specified in Exhibit A, the initial term of the Subscription Services shall be for a period of twelve (12) months commencing on the date that the Subscription Services are made available to the Customer via Insight.

The Subscription Services may be renewed for successive periods of one year each (or multiple years as mutually agreed upon in writing by the Parties), in accordance with the following procedure. ShotSpotter shall provide Customer with a renewal notice stating the renewal fees, terms, and conditions for the next successive renewal term approximately ninety (90) days prior to the expiration date of the then current term. Customer acknowledges that the Subscription Services fees, terms and conditions, and service levels hereunder are subject to change and that such fees, terms and conditions, and service levels may vary from those applicable to this Agreement in successive renewal terms. Annual Subscription fees are subject to increase at a rate of 5% for Customers whose annual subscription fee is less than the current ShotSpotter list price.

If Customer fails to renew prior to expiration of the then current subscription term, the Subscription Services will terminate in accordance with Section 5.C. At its discretion, ShotSpotter may remove the ShotSpotter Gunshot Detection, Location, and Forensic Analysis Service and any components from the Coverage Area at that time. If ShotSpotter does not remove the ShotSpotter Gunshot Detection, Location, and Forensic Analysis Service from the Coverage Area, Customer may reinstate the Subscription Services at a later date by renewing this Agreement and payment of the applicable reactivation and Subscription Services renewal fees; however, Customer will not have access to any Reviewed Alerts that they would have had access to during the lapsed period.

#### 5. LICENSE, OWNERSHIP, AND DATA RIGHTS

In consideration for and subject to the payment of the annual Subscription Services fees as set forth in Exhibit A, Customer is granted a non-transferrable, non-exclusive and terminable license ("License") to use the Subscription Services and Data as set forth in this Section 5. Please read the terms and conditions of this Agreement carefully. By using the Subscription Services and Data, you agree to be bound by the terms and conditions of this Agreement. If you do not agree to these terms, you must notify ShotSpotter and discontinue any use of the Subscription Services and Data.

##### A. Rights in Data.

For the purposes of this Agreement, "Data" is defined as data, information, and electronic files created, generated, modified, compiled, displayed, stored or kept in the course of providing the Subscription Services, including, without limitation, information in Reviewed Alerts accessible through the Service and/or Software.

ShotSpotter shall own and have the unrestricted right to use the Data for internal purposes such as research or product development. ShotSpotter may provide, license, or sell Data on an

aggregated basis to third parties (excluding press or media) to be used for research or analytical purposes, or for law enforcement and/or security purposes.

ShotSpotter will not release or disseminate to any person or entity Data related to or consisting of specific forensic or law enforcement sensitive incident information pertaining to any active inquiry, investigation, or prosecution, unless in response to a valid order or subpoena issued by a court or other governmental body, or as otherwise required by law. ShotSpotter will not release, sell, license, or otherwise distribute the gunfire alert Data to the press or media without the prior express written consent of an authorized representative of the Customer.

Customer shall have the unrestricted right to download, make copies of, distribute, and use the Data within its own organization, exclusively for its own internal purposes, and for purposes of detecting and locating gunfire, routine archival recordkeeping, evidence preservation, and investigative, or evidentiary, and prosecutorial purposes. Customer shall not provide to, license the use of, or sell Data to any third parties, which restriction will not pertain to the collaboration with other law enforcement agencies for the purposes of investigating and prosecuting crimes detected by the ShotSpotter systems.

#### B. License and Restrictions.

**Software and Subscription Services.** The Software is the proprietary product of ShotSpotter, licensed to Customer on an annual subscription basis. The ShotSpotter Software may incorporate components supplied to ShotSpotter under license by third-party suppliers, and may be protected by United States patent, trade secret, copyright law and international treaty provisions. All such rights in and to the Software and Subscription Services any part thereof are the property of ShotSpotter or, if applicable, its suppliers. All right and title to the ShotSpotter computer programs, including, but not limited to related documentation, technology, know-how and processes embodied in or made available to Customer in connection with the Subscription Services, patent rights, copyrights, trade secret rights, trademarks, and services marks remain with ShotSpotter. Customer may not make any copies of the written materials or documentation that accompany any component of the Software, or use them, or any other information concerning the Subscription Services that ShotSpotter has designated as confidential, for any purpose other than bona fide use of the Subscription Services or Software for in accordance with the terms of this Agreement, nor allow anyone else to do so. Customer shall not: (i) modify, adapt, alter, translate, copy, perform, or display (publicly or otherwise) or create compilations, derivative, new, or other works based, in whole or in part, on the Software, or on the Subscription Services; (ii) merge, combine, integrate, or bundle the Software, in whole or in part, with other software, hardware, data, devices, systems, technologies, products, services, functions, or capabilities; (iii) transfer, distribute, make available the Subscription Services, or Software to any person other than Customer; or (iv) sell, resell, sublicense, lease, rent, or loan the Subscription Services or Software, in whole or in part. No component of the Subscription Services, or Software may be used to operate a service bureau, rental or time-sharing arrangement.

**Data.** Customer's rights to use the Data are defined in paragraph A of this section 5.

Nothing in this Agreement shall be construed as granting any right or title to the Software, Data or any component thereof, or any other Intellectual property of ShotSpotter or its suppliers to Customer.

Customer shall not alter, remove or obscure any copyright, patent, trademarks, confidential, proprietary, or restrictive notices or markings on any component of the Subscription Services, Software or any documentation.

Customer acknowledges that the ShotSpotter System has been determined by the United States Department of State to be a controlled commodity, software and/or technology subject to the United States Export Administration Regulations of the U.S. Department of Commerce. Customer is specifically prohibited from the export, or re-export, transfer, consignment, shipment, delivery, downloading, uploading, or transmitting in any form, any ShotSpotter Software, Data, documentation, or any component thereof or underlying information or technology related thereto, to any third party, government, or country for any end uses except in strict compliance with applicable U.S. export controls laws, and only with the express prior written agreement of ShotSpotter. In the event that such written agreement is provided, Customer shall be responsible for complying with all applicable export laws and regulations of the United States and destination country, including, but not limited to the United States Export Administration Regulations of the U.S. Department of Commerce, including the sanctions laws administered by the U.S. Department of Treasury, Office of Foreign Assets Control (OFAC), the U.S. Anti-Boycott regulations, and any applicable laws of Customer's country. In this respect, no resale, transfer, or re-export of the ShotSpotter Respond System or any ShotSpotter Respond System component exported to Customer pursuant to a license from the U.S. Department of Commerce may be resold, transferred, or reported without prior authorization by the U.S. Government. Customer agrees not to export, re-export or engage in any "deemed export," or to transfer or deliver, or to disclose or furnish, to any foreign (non- U.S.) government, foreign (non-U.S.) person or third party, or to any U.S. person or entity, any of the ShotSpotter Respond System, or ShotSpotter Respond System components, Data, Software, Services, or any technical data or output data or direct data product thereof, or any service related thereto, in violation of any such restrictions, laws or regulations, or without all necessary registrations, licenses and or approvals. Customer shall bear all expenses relating to any necessary registrations, licenses or approvals.

Use, duplication, or disclosure by applicable U.S. government agencies is subject to restrictions as set forth in the provisions of DFARS 48 CFR 252.227-7013 or FAR 48 CFR 52.227-14, as applicable.

In addition to the foregoing, Customer shall not disclose, discuss, download, ship, transfer, deliver, furnish, or otherwise export or re-export any such item(s) to or through: (a) any person or entity on the U.S Department of Commerce Bureau of Industry and Security's List of Denied Persons or Bureau of Export Administration's anti-proliferation Entity List; (b) any person on the U.S. Department of State's List of Debarred Parties; (c) any person or entity on the U.S. Treasury Department Office of Foreign Asset Control's List of Specially Designated Nationals and Blocked Persons; or (d) any third party or for any end-use prohibited by law or regulation, as any and all of the same may be amended from time to time, or any successor thereto.

#### C. Termination.

Customer agrees that its right to use the Subscription Services, Software and Data will terminate following thirty (30) day's prior written notice due to a material breach of the terms of this Agreement, including failure to pay any sums to ShotSpotter when due, or failure to renew the Subscription Services prior to expiration of the then current subscription term unless such has been



cured within said thirty (30) day period. In the event of a breach of ShotSpotter's intellectual property rights, ShotSpotter at its sole discretion may terminate this Agreement immediately upon written notice to Customer. In the event of termination, Customer's access to the Data and Software will be terminated, and ShotSpotter will cease delivering Reviewed Alerts, and disable Customer's access to the Data. Customer agrees that ShotSpotter shall not be liable to Customer nor to any third party for any suspension of the Subscription Services resulting from Customer's nonpayment of the Subscription Services fees as described in this section.

**D. Modification to, or Discontinuation of the Subscription Services.**

Upon reasonable notice to Customer, ShotSpotter reserves the right at its discretion to modify, temporarily or permanently, the Subscription Services (or any part thereof). In the event that ShotSpotter modifies the Subscription Services in a manner which removes or disables a feature or functionality on which Customer materially relies, ShotSpotter, at Customer's request, shall use commercially reasonable efforts to restore such functionality to Customer. In the event that ShotSpotter is unable to substantially restore such functionality, Customer shall have the right to terminate the Agreement and receive a pro-rata refund of the annual Subscription Services fees paid under the Agreement for the subscription term in which this Agreement is terminated. Customer acknowledges that ShotSpotter reserves the right to discontinue offering the Subscription Services at the conclusion of Customer's then current term. Customer agrees that ShotSpotter shall not be liable to Customer or to any third party for any modification of the Subscription Services as described in this section.

**E. New Applications.**

From time to time, at ShotSpotter's discretion, ShotSpotter may release to its customer base, new applications supplemental to the Subscription Services. Customer's use of such new applications shall be subject to the license, warranty, intellectual property, and support terms of this Agreement. Prior to general release, ShotSpotter may request Customer to act as a pre-release test site for new applications, or major upgrades. Provided that Customer agrees in writing to such request, ShotSpotter will provide a pre-release package explaining the details and requirements for Customer's participation.

**F. No Use by Third Parties.**

Use by anyone other than Customer of the Subscription Services, documentation, and Data is prohibited, unless pursuant to a valid assignment of this Agreement as set forth in Section 18 of this Agreement.

## **6. CONFIDENTIALITY AND PROPRIETARY RIGHTS**

**A. ShotSpotter Privacy Policy.**

ShotSpotter has structured its technology, processes and policies in such a way as to minimize the risk of privacy infringements from audio surveillance while still delivering important public safety benefits to its customers. These efforts to maintain privacy include the following:

- 1) ShotSpotter will not provide extended audio to customers beyond the audio snippet (1 second of ambient noise prior to a gunshot, the gunshot audio itself, and 1 second after

the incident). ShotSpotter will vigorously resist any subpoena or court order for extended audio that goes beyond an audio snippet.

- 2) ShotSpotter will not provide a list or database of the precise location of Sensors to police or the public if requested and will challenge any subpoenas for this location data.

**B. ShotSpotter Confidential Information.**

Customer acknowledges and agrees that the source code, technology, and internal structure of the Software, Data, and Subscription Services, as well as documentation, operations manual(s) and training material(s), are the confidential information and proprietary trade secrets of ShotSpotter, the value of which would be destroyed by disclosure to the public. Use by anyone other than Customer of the Subscription Services, documentation, and Data is prohibited, unless pursuant to a valid assignment under this Agreement. Unless prohibited by applicable law, the terms and conditions of this Agreement, including pricing and payment terms shall also be treated as ShotSpotter's confidential information. Customer shall not disassemble, decompile, or otherwise reverse engineer or attempt to reconstruct, derive, or discover any source code, underlying ideas, algorithms, formulae, routines, file formats, data structures, programming, routines, interoperability interfaces, drawings, or plans from the Software, or any data or information created, compiled, displayed, or accessible through the Subscription Services, in whole or in part. Customer agrees during the term of this Agreement, and thereafter, to hold the confidential information and proprietary trade secrets of ShotSpotter in strict confidence and to not permit any person or entity to obtain access to it except as required for the Customer's exercise of the license rights granted under this Agreement. Nothing in this Agreement is intended to or shall limit any rights or remedies under applicable law relating to trade secrets, including the Uniform Trade Secrets Act as enacted in applicable jurisdictions.

**C. Customer Confidential Information**

During the term of this Agreement or any subsequent renewals, ShotSpotter agrees to maintain Customer information designated by the Customer as confidential to which ShotSpotter gains access in the performance of its obligations under this Agreement, and not disclose such Customer Confidential Information to any third parties except as may be required by law. ShotSpotter agrees that Customer's Confidential Information shall be used solely for the purpose of performing ShotSpotter's obligations under this Agreement.

**D. Obligations of the Parties.**

The receiving Party's ("Recipient") obligations under this section shall not apply to any of the disclosing Party's ("Discloser") Confidential Information that Recipient can document: (a) was in the public domain at or subsequent to the time such Confidential Information was communicated to Recipient by Discloser through no fault of Recipient; (b) was rightfully in Recipient's possession free of any obligation of confidence at or subsequent to the time such Confidential Information was communicated to Recipient by such Discloser; (c) was developed by employees or agents of Recipient independently of and without reference to any of Discloser's Confidential Information; or (d) was communicated by Discloser to an unaffiliated third party free of any obligation of confidence. A disclosure by Recipient of any Discloser Confidential Information (a) in response to a valid order by a court or other governmental body; (b) as otherwise required by law; or (c) necessary to establish the rights of either party under this Agreement shall not be considered to be a breach of

this Agreement by the Recipient; provided, however, that Recipient shall provide prompt prior written notice thereof to the Discloser to enable Discloser to seek a protective order or otherwise prevent such disclosure. The Recipient shall use reasonable controls to protect the confidentiality of and restrict access to all Confidential Information of the Discloser to those persons having a specific need to know for the purpose of performing the Recipient's obligations under this Agreement. The Recipient shall use controls no less protective than Recipient uses to secure and protect its own confidential, but not "Classified" or otherwise Government-legended, information. Upon termination of this Agreement the Recipient, as directed by the Discloser, shall either return the Discloser's Confidential Information, or destroy all copies thereof and verify such destruction in writing to the Discloser.

Unless the Recipient obtains prior written consent from the Discloser, the Recipient agrees that it will not reproduce, use for purposes other than those expressly permitted in this Agreement, disclose, sell, license, afford access to, distribute, or disseminate any information designated by the Discloser as confidential.

## 7. LIMITED WARRANTIES

ShotSpotter warrants that the Software will function in substantial conformity with the ShotSpotter documentation accompanying the Software and Subscription Services. The Software covered under this warranty consists exclusively of the ShotSpotter Dispatch, ShotSpotter Respond, and ShotSpotter Insight applications and user interface made available to the Customer under this Agreement. ShotSpotter will provide support services as defined in Exhibit B Service Level Agreement.

- A. ShotSpotter further warrants that the Subscription Services, Data, and Software shall be free of viruses, Trojan horses, worms, spyware, or other malicious code or components.
- B. The Subscription Services are not designed, sold, or intended to be used to detect, intercept, transmit, or record oral or other communications of any kind. ShotSpotter cannot control how the Subscription Services are used, and, accordingly, ShotSpotter does not warrant or represent, expressly or implicitly, that use of the Subscription Services will comply or conform to the requirements of federal, state, or local statutes, ordinances, and laws, or that use of the Subscription Services will not violate the privacy rights of third parties. Customer shall be solely responsible for using the Subscription Services in full compliance with applicable law and the rights of third persons.
- C. ShotSpotter does not warrant or represent, expressly or implicitly, that the Software or Subscription Services or its use will: result in the prevention of crime, apprehension or conviction of any perpetrator of any crime, or detection of any criminal; prevent any loss, death, injury, or damage to property due to the discharge of a firearm or other weapon; in all cases result in a Reviewed Alert for all firearm discharges within the designated coverage area; or that the ShotSpotter-supplied network will remain in operation at all times or under all conditions.
- D. ShotSpotter expressly disclaims, and does not undertake or assume any duty, obligation, or responsibility for any decisions, actions, reactions, responses, failure to act, or inaction, by Customer as a result of or in reliance on, in whole or in part, any Subscription Services or Reviewed Alerts provided by ShotSpotter, or for any consequences or outcomes, including any death, injury, or loss or damage to any property, arising from or caused by any such decisions, actions, reactions,

responses, failure to act, or inaction. It shall be the sole and exclusive responsibility of the Customer to determine appropriate decisions, actions, reactions, or responses, including whether or not to dispatch emergency responder resources. The Customer hereby expressly assumes all risks and liability associated with any and all action, reaction, response, and dispatch decisions, and for all consequences and outcomes arising from or caused by any decisions made or not made by the Customer in reliance, in whole or in part, on any Subscription Services provided by ShotSpotter, including any death, injury, or loss or damage to any property.

- E. Any and all warranties, express or implied, of fitness for high-risk purposes requiring fail-safe performance are hereby expressly disclaimed.
- F. The Parties acknowledge and agree that the Subscription Services is not a consumer good, and is not intended for sale to or use by or for personal, family, or household use.

**EXCEPT AS EXPRESSLY SET FORTH IN THIS SECTION 7, SHOTSPOTTER MAKES AND CUSTOMER RECEIVES NO OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTIES OF NON-INFRINGEMENT, QUALITY, SUITABILITY, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.**

#### **8. CUSTOMER OBLIGATIONS.**

Customer acknowledges and agrees that ShotSpotter's duties, including warranty obligations, and ability to perform its obligations to Customer under this Agreement shall be predicated and conditioned upon Customer's timely performance of and compliance with Customer's obligations hereunder, including, but not limited to:

- A. Customer agrees to pay all sums due under this Agreement when they are due pursuant to the payment terms in Exhibit A for implementation, and ongoing annual subscription fees. Actual access and use of the ShotSpotter Service shall constitute evidence that the Subscription Services are active, and the final implementation payment is due.

Customer's address for invoicing:

City of Boston – Auditing Department

One City Hall Plaza, Room M-4

Boston, MA 02201

- B. Customer agrees to use reasonable efforts to timely perform and comply with all of Customer's obligations allocated to Customer under this Agreement, including providing assistance to ShotSpotter, as needed in obtaining premise permissions for installation of the Sensors.
- C. Customer shall not permit any alteration, modification, substitution, or supplementation of the ShotSpotter Subscription Services or web portal, or the combining, connection, merging, bundling, or integration of the ShotSpotter Subscription Services or web portal into or with any other system, equipment, hardware, software, technology, function, or capability, without ShotSpotter's express prior written consent.
- D. Unless otherwise expressly agreed in advance in writing by ShotSpotter, Customer shall not authorize or appoint any contractors, subcontractors, original equipment manufacturers, value added integrators, systems integrators, or other third parties to operate, or have access to any part of the Subscription Services.



- E. In order to use the Subscription Services, Customer must have and maintain access to the World Wide Web to enable a secure https connection from the Customer's workstation(s) to ShotSpotter's hosted services, either directly or through devices that access Web-based content. Customer must also provide all equipment necessary to make such (and maintain such) connection.
- F. ShotSpotter will assist the Customer in initially setting up passwords and user names for Customer's employees, agents, or representatives to whom Customer designates access to the Subscription Services ("Authorized Users"). Thereafter, Customer shall be responsible for assigning passwords and user names for its Authorized Users. Customer shall be responsible for maintaining the confidentiality and use of Customer's password and user names and shall not allow passwords and/or user names to be shared by Authorized Users; nor shall Customer permit any unauthorized users to access the Subscription Services.
- G. Customer shall comply with all applicable laws, rules and regulations relating to the goods and services provided hereunder.

## **9. INTELLECTUAL PROPERTY INFRINGEMENT**

ShotSpotter will, at its expense, defend and indemnify Customer from and against losses, suits, damages, liability, and expenses (including reasonable attorney fees) arising out of a claim asserted in a lawsuit or action against the Customer by a third party unrelated to the Customer, in which such third party asserts a claim that the Subscription Services and/or Software, when used in accordance with ShotSpotter's user documentation, infringes any United States patent which was issued by the U.S. Patent and Trademark Office, or United States copyright which was registered by the U.S. Copyright Office, as of the effective date of Customer's agreement to license the ShotSpotter Respond System (collectively "Action"), provided that Customer provides ShotSpotter with reasonably prompt notice of any such Action, or circumstances of which Customer becomes aware that could reasonably be expected to lead to such Action including but not limited to any cease and desist demands or warnings, and further provided that Customer cooperates with ShotSpotter and its defense counsel in the investigation and defense of such Action.

ShotSpotter shall have the right to choose counsel to defend such suit and/or action, and to control the settlement (including determining the terms and conditions of settlement) and the defense thereof. Customer may participate in the defense of such action at its own expense.

This Section 9 shall not apply and ShotSpotter shall have no obligation to defend and indemnify Customer in the event the Customer or a third party modifies, alters, substitutes, or supplements any of the Subscription Services, or Software, or to the extent that the claim of infringement arises from or relates to the integration, bundling, merger, or combination of any of the same with other hardware, software, systems, technologies, or components, functions, capabilities, or applications not licensed by ShotSpotter as part of the Subscription Services, nor shall it apply to the extent that the claim of infringement arises from or relates to meeting or conforming to any instruction, design, direction, or specification furnished by the Customer, nor to the extent that the Subscription Services or Software are used for or in connection with any purpose, application, or function other than detecting and locating gunshots exclusively through acoustic means.

If, in ShotSpotter's opinion, the Subscription Services, or Software may, or is likely to become, the subject of such a suit or action, does become the subject of a claim asserted against Customer in a lawsuit which

ShotSpotter is or may be obliged to defend under this section, or is determined to infringe the foregoing patents or copyrights of another in a final, non-appealable judgment subject to ShotSpotter's obligations under this section, then ShotSpotter may in full and final satisfaction of any and all of its obligations under this section, at its option: (1) procure for Customer the right to continue using the affected Subscription Services or Software, (2) modify or replace such Subscription Services or Software to make it or them non-infringing, or (3) refund to Customer a pro-rata portion of the annual Subscription Services fees paid for the Subscription Services for the term in which the Agreement is terminated.

**This Section 9 states the entire liability of ShotSpotter and is Customer's exclusive remedy for or relating to infringement or claims or allegations of infringement of any patent, copyright, or other intellectual property rights in or to the Subscription Services, the ShotSpotter Gunshot Detection, Location and Forensic Analysis Service components, and Software. This section is in lieu of and replaces any other expressed, implied, or statutory warranty against infringement of any and all intellectual property rights.**

#### **10. INDEMNIFICATION AND LIMITATION OF LIABILITY**

ShotSpotter shall, at its expense, indemnify, defend, save, and hold Customer harmless from any and all claims, lawsuits, or liability, including attorneys' fees and costs, arising out of, in connection with, any loss, damage, or injury to persons or property to the extent of the gross negligence, or wrongful act, error, or omission of ShotSpotter, its employees, agents, or subcontractors as a result of ShotSpotter's or any of its employees, agents, or subcontractor's performance pursuant to this Agreement. ShotSpotter shall not be required to indemnify Customer for any claims or actions caused to the extent of the negligence or wrongful act of Customer, its employees, agents, or contractors. Notwithstanding the foregoing, if a claim, lawsuit, or liability results from or is contributed to by the actions or omissions of Customer, or its employees, agents, or contractors, ShotSpotter's obligations under this provision shall be reduced to the extent of such actions or omissions based upon the principle of comparative fault.

**In no event shall either Party, or any of its affiliates or any of its/their respective directors, officers, members, attorneys, employees, or agents, be liable to the other Party under any legal or equitable theory or claim, for lost profits, lost revenues, lost business opportunities, exemplary, punitive, special, indirect, incidental, or consequential damages, each of which is hereby excluded by agreement of the Parties, regardless of whether such damages were foreseeable or whether any Party or any entity has been advised of the possibility of such damages.**

**Except for its Intellectual Property Infringement indemnity obligations under Section 9 of this Agreement, ShotSpotter's cumulative liability for all losses, claims, suits, controversies, breaches or damages for any cause whatsoever arising out of or related to this Agreement, whether in contract, tort, by way of indemnification or under statute, and regardless of the form of action or legal theory shall not exceed two (2) times the amount paid to ShotSpotter under this Agreement, or the amount of insurance maintained by ShotSpotter available to cover the loss, whichever is greater. The foregoing limitations shall apply without regard to any failure of essential purpose of any remedies given herein.**

## **11. DEFAULT AND TERMINATION; REMEDIES**

Either Party may terminate this Agreement in the event of a material breach of the terms and conditions of this Agreement upon thirty (30) days' prior written notice to the other Party; provided that the Party alleged to be in breach has not cured such breach within said thirty (30) day period.

In addition to the termination provisions in Section 5.C for failure to pay annual Subscription Services fees, upon the occurrence of a material breach of Customer's obligations under this Agreement not susceptible to cure as provided in the preceding paragraph, ShotSpotter may at its option, effective immediately upon written notice to Customer, either: (i) terminate ShotSpotter's future obligations under this Agreement, terminate Customer's License to use the Subscription Services and Software, or (ii) accelerate and declare immediately due and payable all remaining charges for the remainder of the Agreement and proceed in any lawful manner to obtain satisfaction of the same. In either case, Customer shall also be responsible for paying court costs and reasonable attorneys' fees incurred by or on behalf of ShotSpotter, as well as applicable repossession, shipping, repair, and refurbishing costs.

## **12. TAXES**

Unless otherwise included as a line item in Exhibit A, the fees due under this Agreement exclude any sales, use, value added or similar taxes that may be imposed in connection with this Agreement. Customer agrees that it shall be solely responsible for payment, or reimbursement to ShotSpotter as applicable, of all sales, use, value added or similar taxes imposed upon this Agreement by any level of government, whether due at the time of sale or asserted later as a result of audit of the financial records of either Customer or ShotSpotter. If exempt from such taxes, Customer shall provide to ShotSpotter written evidence of such exemption. Customer shall also pay any personal property taxes levied by government agencies based upon Customer's use or possession of the items acquired or licensed in this Agreement.

## **13. NOTICES**

Any notice or other communication required or permitted to be given under this Agreement shall be in writing delivered to the address set forth in this Agreement by certified mail return receipt; overnight delivery services; or delivered in person. A Party's address may be changed by written notice to the other Party.

## **14. FORCE MAJEURE**

In no event shall ShotSpotter be liable for any delay or default in its performance of any obligation under this Agreement caused directly or indirectly by an act or omission of Customer, or persons acting under its direction and/or control, fire, flood, act of God, an act or omission of civil or military authority of a state or nation, strike, lockout, or other labor disputes, inability to secure, delay in securing, or shortage of labor, materials, supplies, transportation, or energy, failures, outages or denial of services of wireless, power, telecommunications, or computer networks, acts of terrorism, sabotage, vandalism, hacking, natural disaster or emergency, war, riot, embargo, or civil disturbance, breakdown or destruction of plant or equipment, or arising from any cause whatsoever beyond ShotSpotter's reasonable control. At ShotSpotter's option and following notice to Customer, any of the foregoing causes shall be deemed to suspend such obligations of ShotSpotter so long as any such cause shall prevent or delay performance, and ShotSpotter agrees to make and Customer agrees to accept performance of such obligations whenever such cause has been remedied.

**15. ENTIRE AGREEMENT**

This Agreement and its Exhibits represent the entire agreement and understanding of the Parties and a final expression of their agreements with respect to the subject matter of this Agreement and supersedes all prior written or oral agreements, representations, understandings, or negotiations with respect to the matters covered by this Agreement.

**16. GOVERNING LAW**

The validity, performance, and construction of this Agreement shall be governed by the laws of the Commonwealth of Massachusetts, without giving effect to the conflict of law principles thereof. The United Nations Convention on Contracts for the International Sale of Goods is expressly disclaimed and shall not apply.

**17. NO WAIVER**

No term or provision of this Agreement shall be deemed waived and no breach excused unless such waiver or consent is in writing and signed by both Parties. Any consent by either Party to, or waiver of, a breach by the other, whether expressed or implied, shall not constitute a consent to, waiver of, or excuse for any other, different, prior, or subsequent breach.

The failure of either Party to enforce at any time any of the provisions of this Agreement shall not constitute a present or future waiver of any such provisions or the right of either Party to enforce each and every provision.

**18. SEVERABILITY**

If any term, clause, sentence, paragraph, article, subsection, section, provision, condition or covenant of this Agreement is held to be invalid or unenforceable, for any reason, it shall not affect, impair, invalidate or nullify the remainder of this Agreement, but the effect thereof shall be confined to the term, clause, sentence, paragraph, article, subsection, section, provision, condition or covenant of this Agreement so adjudged to be invalid or unenforceable.

**19. DISPUTE RESOLUTION**

If the Parties disagree as to any matter arising under this Agreement or the relationship and dealings of the Parties hereto, then at the request of either Party, ShotSpotter and Customer shall promptly consult with one another and make diligent, good faith efforts to resolve the disagreement by negotiation prior to either Party taking legal action. If such negotiations do not resolve the dispute within sixty (60) days of the initial request, either Party may take appropriate legal action.

**20. ASSIGNMENT**

This Agreement may not be assigned or transferred by either Party, nor any of the rights granted herein, in whole or in part, by operation of law or otherwise, without the other Party's express prior written consent, which shall not be unreasonably withheld. Provided, however, that ShotSpotter may assign or transfer this Agreement and/or ShotSpotter's rights and obligations hereunder, in whole or in part, in the event of a merger or acquisition of all or substantially all of ShotSpotter's assets. No assignee for the benefit of Customer's creditors, custodian, receiver, trustee in bankruptcy, debtor in possession, sheriff, or any other



officer of a court, or other person charged with taking custody of Customer's assets or business, shall have any right to continue or to assume or to assign these without ShotSpotter's express consent.

## 21. GENERAL PROVISIONS

- A. This Agreement shall be binding on and inure to the benefit of the Parties and any permitted successors and assigns; however, nothing in this paragraph shall be construed as a consent to any assignment by either Party except as provided in Section 18 of this Agreement.
- B. This Agreement shall not become a binding contract until signed by an authorized representative of each Party, effective as of the date of signature.
- C. This Agreement may be executed in any number of identical counterparts, each of which shall be deemed a duplicate original.
- D. The provisions of this Agreement shall not be construed in favor of or against either Party because that Party or its legal counsel drafted this Agreement, but shall be construed as if all Parties prepared this Agreement.
- E. A facsimile or scanned signature copy of this Agreement and its Exhibits, notices and documents prepared under this Agreement shall be considered an original. The Parties agree that any document in electronic format or any document reproduced from an electronic format shall not be denied legal effect, validity, or enforceability, and shall meet any requirement to provide an original or hard copy.
- F. This Agreement is made for the benefit of the Parties, and is not intended to benefit any third party or be enforceable by any third party. The rights of the Parties to terminate, rescind, or agree to any amendment, waiver, variation or settlement under or relating to this Agreement are not subject to the consent of any third party.

**EACH PARTY'S ACCEPTANCE HEREOF IS EXPRESSLY LIMITED TO THE TERMS OF THIS AGREEMENT AND NO DIFFERENT OR ADDITIONAL TERMS CONTAINED IN ANY CONFIRMATION, PURCHASE ORDER, AMENDMENT OR OTHER BUSINESS FORM, WRITING OR MATERIAL SHALL HAVE ANY FORCE OR EFFECT UNLESS EXPRESSLY AGREED TO IN WRITING BY THE PARTIES.**

**CITY OF BOSTON**

**SHOTSPOTTER, INC.**

\_\_\_\_\_  
Accepted By (Signature)

\_\_\_\_\_  
Accepted By (Signature)

\_\_\_\_\_  
Printed Name

\_\_\_\_\_  
Printed Name

\_\_\_\_\_  
Title

\_\_\_\_\_  
Title

\_\_\_\_\_  
Date

\_\_\_\_\_  
Date

**EXHIBIT A – SHOTSPOTTER PROPOSAL**

ShotSpotter Proposal No.: EV00009078 (Attached)

**EXHIBIT B – SERVICE LEVEL AGREEMENT****ShotSpotter Respond Gunshot Location System****Reviewed Alert Service Levels****Summary**

Under the terms and conditions of the ShotSpotter Services Agreement between ShotSpotter, Inc. ("ShotSpotter") and Customer, ShotSpotter commits to meet or exceed the following Service Level Agreement (SLA) standards as it provides its ShotSpotter Gunshot Location Services<sup>1</sup>:

<b>Service</b>	<b>SLA and Measurement</b>
Gunshot Detection & Location	90% of unsuppressed, outdoor gunfire incidents, using standard, commercially available rounds greater than .25 caliber, inside the Coverage Area will be detected and located within 25 meters of the actual gunshot location.
Reviewed Alerts	90% of gunshot incidents will be reviewed and published in less than 60 seconds.
Service Availability	The ShotSpotter Gunshot Location System service will be available to the Customer 99.9% of the time with online access to ShotSpotter data, excluding scheduled maintenance windows.

**Gunshot Detection & Location Performance**

ShotSpotter will detect and accurately locate to within 25 meters of the actual gunshot location 90% of unsuppressed, outdoor gunshots fired inside the contracted coverage area using standard, commercially available rounds greater than .25 caliber.

**Reviewed Alerts Service**

The ShotSpotter real-time Incident Review Center (IRC) will review at least 90% of all gunfire incidents within 60 seconds. This human review is intended to confirm or change the machine classification of the incident type, and, depending on the reviewer's confidence level that the incident is or may be gunfire, will result in an alert ("Reviewed Alert") sent to the Customer's dispatch center, patrol car mobile data terminals (MDT), and officer smartphones (via the ShotSpotter App), based on the following criteria:

<b>Incident Type</b>	<b>Action</b>
High confidence incident is gunfire	Reviewed Gunfire Alert, (Single Gunshot "SG" or Multiple Gunshots "MG") sent to Customer's dispatch center, patrol car mobile data terminals (MDT), and officer smartphones (via the ShotSpotter Respond App)
Uncertain if incident is gunfire or not	Reviewed Probable Gunfire ("PG") Alert sent to Customer's dispatch center, patrol car MDTs, and officer smartphones
Low confidence incident is gunfire	<b>No alert</b> will be sent; incident available for Customer review in the incident history available through Insight

<sup>1</sup> See attached "ShotSpotter – Definition of Key Terms" for a complete definition of terms associated with this SLA and further details in the expanded definitions listed below the Summary. The basis for this SLA and performance measurement will be total gunshot incidents as defined by the Definition of Key Terms.

Reviewed Alerts are sent to the Customer's dispatch center, patrol car MDTs, and officer smartphones. Information in a Reviewed Alert will include the following:

- "Dot on the map" with latitude and longitude indicating the location of the incident.
- Parcel address closest to location of the incident.
- When available, additional situational awareness data points may be included, such as:
  - Qualitative data on the type/severity of incident: Fully automatic, High Capacity
  - Other comments (if any)

The ShotSpotter Respond App, and Insight provide the Customer with full and immediate access to incident history including information ShotSpotter uses in its internal review process. This information includes, among other things, the initial incident classification and any reclassifications of an incident, incident audio wave forms, and incident audio files. This data access is available as long as the Customer is under active subscription.

### **Service Availability**

The ShotSpotter Respond System<sup>2</sup> will be able to detect gunfire and available to users with online access to ShotSpotter data 99.9% of the time, on a 24x7 by 365 day per year basis, excluding: a) scheduled maintenance periods which will be announced to Customer in advance; b) select holidays; and c) third party network outages beyond ShotSpotter's control.

### **Customer SLA Credits**

Each Service Level measurement shall be determined quarterly, the results of which will be reviewed during the periodic account review meetings with Customer. For each calendar quarter that ShotSpotter does not meet at least two of the three above standards, a fee reduction representing one free week of service (for the affected Coverage Area) for each missed quarter shall be included during a future Customer renewal.

### **Service Level Exclusions and Modifications**

ShotSpotter takes commercially reasonable efforts to maintain Service Levels at all times. However, Service Level performance during New Year's Eve and Independence Day and the 48-hour periods before and after these holidays, are specifically excluded from Service Level standards. During these excluded periods, because of the large amount of fireworks activity, ShotSpotter uses fireworks suppression techniques<sup>3</sup>.

The ShotSpotter sensors send incident information to the ShotSpotter cloud via third party cellular, wireless or wired networks. ShotSpotter is not responsible for outages on the third-party networks.

---

<sup>2</sup> Respond service includes all database, applications, and communications services hosted by ShotSpotter, Inc. at our data center and specifically exclude Customer's internal network or systems or 3<sup>rd</sup> party communications networks, e.g. Verizon, AT&T, Sprint/T-Mobile, or Customer's Internet Service Provider.

<sup>3</sup> ShotSpotter will put the ShotSpotter system into "fireworks suppression mode" during this period in order to reduce the non-gunfire incidents required for human classification. ShotSpotter will formally inform the customer prior to the system being placed in fireworks suppression mode and when the mode is disabled. While in fireworks suppression mode, the incident alerts determined to be fireworks are not sent to the reviewer nor the Customer dispatch center, patrol car MDTs, and officer smartphones; however, these non-gunfire incidents will continue to be stored in the database for use if required at a later time.



### Service Failure Notification

Should ShotSpotter identify any condition (disruption, degradation or failure of network, cloud, servers, sensors etc.) that impacts ShotSpotter's ability to meet the Gunshot Detection & Location standard (above), ShotSpotter will proactively notify the Customer with: a) a brief explanation of the condition; b) how the Customer's service is affected; and c) the approximate timeframe for resolution. ShotSpotter will also notify the Customer once any such condition is resolved.

### Customer Responsibilities

The purpose of the Reviewed Alert service is to provide incident data to the Customer, reviewed, analyzed and classified in the manner described above. However, it is the sole responsibility of the Customer to interpret the data provided, and to determine any appropriate follow-up reaction or response, including whether or not to dispatch emergency responder resources based on a Reviewed Alert. ShotSpotter does not assume any obligation, duty or responsibility for reaction, response, or dispatch decisions, which are solely and exclusively the responsibility of Customer, or for the consequences or outcomes of any decisions made or not made by the Customer in reliance, in whole or in part, on any services provided by ShotSpotter.

Customer must inform ShotSpotter when Verified Incidents of gunfire are missed by the ShotSpotter Respond System in order to properly calculate Performance Rate, as defined below.

Customer is responsible for providing any required workstations, mobile devices and internet access for the Customer's dispatch center, patrol car MDTs, and officer smartphones, or Insight.

### Support Level Matrix

Support Level	Tier 1 Support (IRC)	Tier 2 Support (Customer Support)
<b>Features</b>	<ul style="list-style-type: none"> <li>Login support</li> <li>Report a misclassification</li> <li>Report a missed incident</li> <li>Report a mislocated incident</li> <li>Basic audio request</li> <li>General/application questions</li> <li>Request for ILS</li> </ul>	Normal Support: <ul style="list-style-type: none"> <li>Analysis of missed gunshots</li> <li>Detailed audio search</li> <li>Performance analysis</li> <li>Integration issues</li> </ul> Critical Support: <ul style="list-style-type: none"> <li>System outage</li> </ul>
<b>Hours of Operation</b>	24x7x365	Normal Support: 5 am – 11 pm Pacific Time Zone Escalation: 24x7x365

### ShotSpotter – Definition of Key Terms

The ShotSpotter Respond System will provide data for correct detection and accurate location for ninety percent (90%) of detectable (outdoor, unsuppressed) community gunfire which occurs within a coverage area, the "Coverage Area", provided the measurement is Statistically Significant, as defined below. This performance rate shall be calculated as a percentage as follows:

$$\text{Performance Rate} = \frac{\text{NumberAccuratelyLocated}}{(\text{NumberAccuratelyLocated} + \text{NumberNotDetected} + \text{NumberMislocated})}$$

where the "Performance Rate" is a number expressed as a percentage, "NumberAccuratelyLocated" is the number of "Gunfire Incidents" occurring within the Coverage Area during the specified period for which the ShotSpotter produced an Accurate Location, NumberMislocated is the number of Verified Incidents (a "Verified Incident" is an incident where Customer has physical or other credible evidence that gunfire took place) for which the ShotSpotter produced an inaccurate location (i.e., a Mislocated Incident), and NumberNotDetected is the number of Verified Incidents for which the ShotSpotter failed to report a location at all (i.e., Missed Incidents).

An "Accurate Location" shall mean an incident located by the ShotSpotter to a latitude/longitude coordinate that lies within a 25-meter radius of the confirmed shooters location (25 meters = approximately 82 feet). "Detectable Gunfire" incidents are unsuppressed discharges of ballistic firearms which occur fully outdoors in free space (i.e. not in doorways, vestibules, windows, vehicles, etc.) using standard commercially available rounds of caliber greater than .25.

ShotSpotter Review Period is measured as the period commencing when the Incident Review Center (IRC) receives the alert and the first audio download to the time it is published to the customer

ShotSpotter performance is guaranteed after a "Statistically Significant" set of incidents has been detected in accordance with timeframes set forth herein and following DQV and commercial system acceptance. The ShotSpotter system is designed to detect gunfire which is typically well distributed throughout the Coverage Area; however, performance should not be construed to mean that 90% of gunfire fired at any given location within the Coverage Area will be detected and located within the guaranteed accuracy.

The ShotSpotter Respond System is not a "point protection" system and is therefore not designed to consistently detect gunfire at every single location within the Coverage Area, but rather to Accurately Locate 90% of the Detectable Incidents in aggregate throughout the entire Coverage Area. There may be certain locations within the Coverage Area where obstacles and ambient noise impede and/or overshadow the propagation of acoustic energy such that locating the origin at those positions is inconsistent or impossible. The Performance Rate calculation is thus specifically tied to the Community Gunfire across the entire Coverage Area.

Statistically Significant shall be defined as measurements and calculations which shall be performed as follows: (a) Across an entire Coverage Area; (b) Aggregating over a period of at least 30 days under weather conditions seasonally normal for the area; and (c) Provided that the total number of gunfire incidents being counted is equal to or greater than: (i) thirty (30) incidents for systems of up to three (3) square miles of Coverage Area, or (ii) ten (10) incidents multiplied by the number of square miles of Coverage Area for systems where one or more Coverage Areas are three (3) square miles or larger.

# CODIS MANUAL

**TABLE OF CONTENTS**

<b><u>SECTION</u></b>	<b><u>PAGE NUMBER</u></b>
I. INTRODUCTION	3
II. CODIS PROGRAM OVERVIEW	5
III. SECURITY AND ORGANIZATION DATA BACKUP	7 10
IV. DATA ENTRY MATCH ESTIMATOR	12 16
V. UPLOADING DATA TO SDIS	19
VI. UPLOADING DATA TO NDIS	21
VII. AUTOSEARCHER	22
VIII. SEARCHER	23
IX. VIEWING MATCHES FROM LDIS SEARCH	24
X. VIEWING MATCHES FROM SDIS/NDIS SEARCH	27
XI. EXPUNGEMENT OF DNA PROFILE	32

## **I. INTRODUCTION**

The policies and procedures described in this manual were originally implemented in September, 2000.

The Combined DNA Index System, or CODIS, is a computer database that can be used to generate investigative leads through the comparison of DNA profiles. The CODIS database primarily consists of two indexes, the Forensic Index and the Offender Index. The Forensic Index contains DNA profiles from casework evidence and the Offender Index contains DNA profiles from convicted offenders and arrestees. Through the use of computers and high speed electronic communications technology, the database can rapidly compare the DNA profiles from casework evidence against each other for any possible “hits”, or matches. This process is valuable to the identification of serial offenders. The database can also compare the DNA profiles from casework evidence to the DNA profiles from convicted offenders and other known individuals to potentially identify a suspect in a case that previously was unsolved.

The Boston Police Crime Laboratory serves as a caseworking CODIS laboratory. A caseworking CODIS lab is responsible for analyzing casework evidence and entering any resulting qualified DNA profiles from casework evidence into the Forensic Index of CODIS. Examples of types of evidentiary samples whose DNA profiles would be entered into CODIS include, but are not limited to, semen or saliva recovered from a Sexual Assault Evidence Collection Kit, blood, semen, saliva, or other biological evidence collected from a crime scene, samples recovered from unidentified human remains, samples from a missing person (deduced missing person sample), and relatives of missing persons. Samples collected from known individuals for comparison purposes are not eligible for CODIS entry at this time, and are not entered.

The DNA database legislation in Massachusetts currently requires anyone convicted of **any felony** crime to submit a DNA sample to the state. The Massachusetts State Police (MSP) Crime Laboratory is responsible for analyzing the DNA samples from these convicted offenders and entering the DNA profiles into CODIS.

The casework DNA profiles from the Boston Police Crime Laboratory are routinely uploaded to the MSP Crime Laboratory for comparison to the casework profiles and convicted offender DNA profiles from across the state. The MSP Crime Laboratory is responsible for sending the eligible casework and convicted offender DNA profiles to the national level for comparison to profiles from across the United States.

A CODIS Laboratory must have properly trained personnel, a well-managed facility, and validated procedures for sample collection and subsequent DNA analysis. The FBI is responsible for ensuring that laboratories that participate in CODIS meet national standards for quality assurance and quality control. To ensure that the Boston Police Crime Laboratory meets quality standards, the DNA Section of the Crime Laboratory was first inspected by the National Forensic Science Technology Center (NFSTC) in August of 1998, and found to be in compliance with the FBI's Quality Assurance Standards (QAS). The DNA Section has maintained ongoing compliance with the QAS since August, 1998 and accreditation since June, 2002.

Policies and procedures specific to CODIS are described in the following sections.

## II. CODIS PROGRAM OVERVIEW

Casework samples are analyzed using a minimum of the 13 core STR loci according to procedures described in the DNA Lab Manual. The 13 core CODIS loci are: D3S1358, vWA, D16S539, CSF1PO, TPOX, D8S1179, D21S11, D18S51, TH01, FGA, D5S818, D13S317, and D7S820,

CODIS Eligible evidence from cases without comparison samples are grouped into two categories, or Batches:

SA	Sexual Assault cases
Other	Homicide, Assault and Battery, Breaking and Entering, Car-Jacking, or any <u>non</u> -sexual assault. "Other" batches can occasionally include Sexual Assaults.

An individual Processing Report will be issued to the investigator in charge of the case containing the results of the DNA analyses. The Processing Reports will indicate whether or not a DNA profile was obtained from an evidence item and whether it is suitable for comparison. The Processing Report will indicate whether the DNA profile will be entered into CODIS software for searching, the level at which it will be searched (LDIS, SDIS, NDIS), and whether further testing is recommended (e.g. Y-STR testing).

All DNA profiles entered into CODIS are searched against a local database of Boston Police Department (BPD) casework profiles for possible case to case hits. Qualifying casework profiles are sent electronically to the Massachusetts State Police (MSP) Crime Laboratory for comparison to casework and known (e.g. convicted offender) profiles from across Massachusetts. Casework specimens with data from 6 (or less than 5 with approval) or more core loci meeting Match Rarity Estimate (MRE) can be uploaded to the MSP. The MSP Crime Lab ultimately sends all of the casework with data from 8 or more of the core loci meeting Match Rarity Estimate (MRE) and known (e.g. convicted

offender) profiles from Massachusetts to the FBI for comparison to casework and convicted offender or arrestee profiles from across the United States.

Case to case and case to convicted offender/arrestee hits are reported via Hit Notification to the investigator in charge of a case, as well as to the Suffolk County District Attorney's Office. The Hit Notification will contain the identifying information for the case(s), the evidence tested, and the name of the linked individual (if a convicted offender/arrestee or other known hit). Additional information about the convicted offender/arrestee may be listed, such as the social security number or date of birth. This information will vary according to the state jurisdiction that collected the DNA sample from the known offender/arrestee.

A convicted offender/arrestee hit made through CODIS can serve as probable cause to obtain a new DNA sample from the offender/arrestee. The new DNA sample will be processed by the Boston Police Department DNA Section to ensure the accuracy of the DNA match. Upon completion of testing of the new DNA sample from the offender/arrestee, a Comparison DNA Report will be issued to the investigator in charge of the case, as well as the Suffolk County District Attorney's Office, if known.



### **III. SECURITY AND ORGANIZATION**

The CODIS server is located in the Examination Room within the Crime Laboratory. CODIS workstations are located in Office rooms S259 and S263. Electronic access to the CODIS computer and its information is limited to the members of the DNA Section, or to members of the ISG Department only in the presence of a member of the DNA Section with CODIS access. Each member of the DNA Section will have a unique user ID and password which are required for access to the CODIS computer. Additionally the CODIS Administrator and Alternate CODIS Administrator will have elevated user access to CODIS.

To further ensure the integrity of the CODIS computer and its contents, the system is backed up after hours by backup Tape Monday through Friday. It is recommended that a new tape is inserted every week and rotated each week of the month (a minimum of 4 total tapes). The active tape will be in the server. The other, inactive tapes for the month will be stored in a key-locked safe within the monitored and limited access Crime Laboratory Unit.

Additionally, ideally done in the first week of every month, a monthly backup is performed, and sent off-site to a secure location at BPD Records and Archives. BPD Records and Archives is a limited access facility which is secured and monitored. The monthly backup media are stored in a key-locked safe at BPD Records and Archives. Several tapes and/or other media will be kept, and rotated through to serve as the off-site monthly backup.

Members of the DNA Section have been assigned specific roles in the CODIS program. The roles are described below:

**CODIS Administrator:** The CODIS Administrator role will be filled by a qualified individual appointed by the DNA Section supervisor or Technical Leader. The CODIS Administrator shall be an employee of the laboratory, and must be, or have been, a qualified DNA analyst. (Have six months of documented forensic human-DNA laboratory experience, performed analysis on a range of samples routinely encountered

in forensic casework, have documented mixture interpretation training, and completed a competency test). The CODIS Administrator will manage the overall CODIS program. This will include responsibility for administering the laboratory's local CODIS network, scheduling and documenting the CODIS computer training of casework analysts, assuring that the security of data stored in CODIS is in accordance with state and/or federal law and NDIS operational procedure, assuring that the quality of data stored in CODIS is in accordance with state and/or federal law and NDIS operational procedures. The CODIS Administrator is responsible for ensuring the security and restricted access of CODIS, handling any computer or network- related issues, management and assignment of computer passwords and privileges. Additional duties include data entry, data upload and search, and match interpretation, management, and reporting. The CODIS Administrator will provide documentation of completion of the FBI auditor training, or will complete such training within one year of appointment. The CODIS Administrator will provide documentation of completion of the FBI CODIS software training, or will complete such training within six months of appointment.

The CODIS Administrator is authorized to terminate an analyst's, or the laboratory's, participation in CODIS until the reliability and security of the computer data can be assured, if an issue with the data is identified.

**Alternate CODIS Administrator:** CODIS Administrator privileges will be given to a second qualified or previously qualified DNA analyst from the laboratory to serve as Alternate CODIS Administrator. The Alternate CODIS Administrator will serve as the CODIS Administrator in the absence of the primary CODIS Administrator. The Alternate CODIS Administrator is subject to the same education and training requirements as the CODIS Administrator, listed above.

Both the CODIS Administrator and the Alternate CODIS Administrator will have an elevated user account. Contact CODIS helpdesk to set up.

**CODIS Analyst:** All authorized casework analysts in the DNA Section may generate casework DNA profiles for entry into CODIS. Authorized analysts may also enter DNA

profiles into CODIS, verify data entry in a Candidate Match, and determine if Candidate Matches should be confirmed.

All CODIS Users (Administrators and Analysts) are subject to the requirements of the most current NDIS Procedures Manual.

## **DATA BACKUP**

### **WEEKLY DATA BACKUP**

1. Login into CODIS server using the elevated user account. Go to search and look up Device Manager. Click on Disk Drives and right click on Dell RD1000. Click disable and click on Yes. Manually eject disk and replace with alternating RD1000 tape (A/B), obtained from key-lock safe in Crime Laboratory. Right click on Dell RD1000 and click enable. It is recommended that backup tapes are replaced each week, preferably on the same day each week (e.g. every Monday), wherever possible.
2. On the CODIS Server, open the Cobian Backup 11 Gravity in bottom right panel (Black and white swirl box). Highlight Cobian Backup and click on history tab. Ensure full backups have been running each night with no red flags.
3. To run a backup manually, highlight Cobian Backup and click on Play button.
4. The tape will run the backup, taking several minutes. Once the tape shows successful backup, (100%) close out of the software and log off.
5. The tape will automatically run the backup each weeknight at 11:00pm, EST.
6. Place the previous week's tape in the key-lock safe for storage.

### **MONTHLY DATA BACKUP**

1. On the CODIS Server login in using the elevated user account. Using a USB cable, plug in the monthly (Passport) backup media, obtained from the key-lock safe in the Crime Laboratory. Ideally, this backup is run during the first week of the month (e.g. the first Monday of the month). Open the Cobian Backup 11 Gravity in bottom right panel (Black and white swirl box). Highlight Cobian Backup and click on Play button to run manual back up.
2. Open Administrative tools and open RD1000 drive. Highlight most recent backup (either one run manually that day or from the previous night during automatic backup). Right click and press copy. Open Passport drive and right click paste into the Passport drive.
3. Once successful copying of the backup is displayed, (100%), unplug the monthly backup from the server.
4. Close out of the software and log off.

5. The monthly backup will be hand carried to BPD Records and Archives, and the next month's media will be retrieved during that trip.
6. Upon return to the Crime Laboratory, the next month's backup media is stored in the key-lock safe with the other weekly backup tapes.

#### **To Schedule the Backup**

1. Contact the CODIS Help Desk for assistance in programming the software to appropriate specifications.

#### **IV. DATA ENTRY**

DNA profiles for data entry will be technically reviewed by a second qualified DNA analyst prior to entry. The technical review will confirm the data calls as well as the eligibility of the profile for CODIS entry, using the Technical Review Notes worksheets and the CODIS Entry Worksheet. DNA profiles are entered into CODIS according to the following steps:

1. Log on to the CODIS computer using the unique user ID and password.
2. From the Start Menu, open Analyst Workbench,
3. Choose the STR Data Entry tab. Alternatively, in the file view, under Go, choose STR/Y-STR Data Entry.
4. Enter the specimen information, as documented on the CODIS Entry Worksheet:
  - a. Specimen ID based on the BPD case # and Item #. Samples originating from a SAECK will not be labeled with item number and only swab type V1A or G1A. A dash D (-D) is added if the profile has been deduced from a mixture. (e.g. 220062IT3SW5 or 211250V1A-D)
  - b. Specimen Category
    - i. Select the appropriate Specimen Category as indicated on the worksheet.
      1. Forensic Unknown, Forensic Mixture, Forensic Partial for upload to NDIS
      2. SDIS Forensic Mixture and SDIS Forensic Partial for upload to SDIS
      3. LDIS Forensic Mixture and LDIS Forensic Partial for searching at LDIS
    - ii. No – if the sample has not been matched to a known reference
  - c. Analyst Assigned To the sample
  - d. Case ID: Enter the case file name where the data can be found and assigned analyst initials – i.e. SA108 RWB, OB126 JDR, 13-0987 HLK.
  - e. Source ID
    - i. Yes – if the sample has been matched to a known reference
    - ii. No – if the sample has not been matched to a known reference

- f. Partial Profile
  - i. Yes – if the sample generated a partial profile at any of the core 13 loci.
  - ii. No – if the sample has generated a full profile at all 13 core loci tested.
- g. Comments: If the analyst who generated the data does not have a drop down under 'Analyst Assigned To', enter the initials in this field.
- 5. Enter the STR DNA profile. The record is entered in duplicate on the screen to ensure the accuracy of the data entered.
  - a. Partial Profile: On a locus by locus basis, if a partial profile is entered (i.e. inconclusive locus, single obligate allele), the locus is designated as Partial. Choose Yes from the drop down menu displayed under "Partial Locus" column next to profile data entry readings. The Partial Locus indicator is only used on single allele entries. If more than one allele is present, the partial locus is not used. For casework profiles that are partial profiles, the profile can only be uploaded to CODIS if it meets the Match Estimation criteria. See Match Estimation section.
  - b. If an allele is designated as obligate, then a + is placed right after the designated allele. See Mixture Profiles section.
  - c. If an allele is outside the ladder/accepted allele calls, allele should be entered as <# or ># and noted on the CODIS Entry Worksheet.
- 6. Click the Save button.
- 7. Print the Specimen Detail Report for the sample by clicking the Print button. Include this report in the DNA case file containing the data.
  - a. Alternatively, the Specimen Details Report can be printed from Specimen Manager.
    - i. In Analyst Workbench, click on Specimen Manager.
    - ii. Locate the sample of interest.
    - iii. From the File Menu, click New. Alternatively, in the toolbar, click on the Edit View Icon.
    - iv. In the General Criteria Tab:

1. Under Specimen ID: choose 'Like' from the dropdown and enter your sample name in the box.
2. Under Lab: choose My Lab
  - v. Click OK
  - vi. When the search results come up, highlight the row containing your specimen and right click on it.
  - vii. Click Print and choose Specimen Detail Report (short), and click Print.
8. Click the Clear button twice to clear the screen. Enter the next sample using above steps, or close the program if data entry is complete.
9. All specimen detail reports need to be confirmed by another qualified analyst within the same business day as entry.

#### **TO EDIT AN EXISTING PROFILE**

A sample may be edited by the analyst assigned to the specimen in the CODIS software, or by an individual with elevated user privileges.

A sample may be edited in order to: Change Specimen Category, Change sample information such as Partial Profile or Source ID, change allele calls.

To change a Specimen ID, the sample must be Deleted and re-entered, unless changed prior to the sample being uploaded to SDIS/NDIS. See the Expungement Section.

1. In Analyst Workbench, click on Specimen Manager.
2. Locate the sample of interest: From the File Menu, click New. Alternatively, in the toolbar, click on the Edit View Icon.

In the General Criteria Tab:

- a. Under Specimen ID: choose 'Like' and enter your sample name in the box.
- b. Under Lab: Choose 'My Lab'
- c. Click OK.
- d. When the search results return, highlight the row containing your specimen.



- e. In the File Menu, under Tools, choose STR/Y-STR Data Entry. Alternatively, in the toolbar, choose the Edit STR/YSTR data entry icon.
  - f. Enter the new information to be edited and updated, as documented on the CODIS Entry Worksheet.
3. Print the Specimen Details Report for the sample by clicking the Print button. All specimen detail reports need to be confirmed by another qualified analyst within the same business day as entry. Include this report in the DNA case file containing the data.
  - a. Alternatively, the Specimen Details Report can be printed from Specimen Manager.
    1. In Analyst Workbench, from the File Menu under Go, click on Specimen Manager.
    2. Locate the sample of interest. From the File menu, click New. Alternatively, in the toolbar, click on the Edit View Icon.
    3. In the General Criteria Tab:
    4. Under Specimen ID: choose 'Like' from the dropdown and enter your sample name in the box.
    5. Under Lab: choose My Lab
    6. Click OK
    7. When the search results come up, highlight the row containing your specimen and right click on it.
    8. Click Print and choose Specimen Detail Report (short), and click Print

### **Mixture Profiles**

For casework profiles that are mixtures, the profile can only be uploaded to SDIS/NDIS if it meets the Match Estimation criteria.

The DNA Analyst generating the mixture profile may be able to interpret the mixed profile data to deduce an eligible profile for purposes of CODIS entry and upload to SDIS/NDIS. The DNA Analyst may examine the electrophoresis data for the mixture profile and record a deduced profile based on the appearance of the data and other

available information (e.g. peak heights, Amelogenin, known reference types related to the case, etc.). The deduced profile will be indicated on data entry by adding a “-D” extension on the Specimen ID (e.g. 07985IT3ST5-D). The deduced profile is recorded by the Analyst, and a second, qualified Analyst technically reviews the deduced profile allele calls prior to CODIS Entry. The deduced profile should contain a minimum of 8 loci for NDIS upload or 6 loci for SDIS upload, and should conform to the Match Estimator criteria. If the profile **cannot** be deduced to conform to the Match Estimation criteria, the entire original mixture profile will not be entered into the database.

Match Estimation criteria: A sample must have an estimation of no more than 1 match in 10 million at moderate stringency (Moderate Rarity Estimate [MRE]) to be allowed to search at NDIS, no more than 1 match in 10,000 to be allowed to search at SDIS, and no more than 1 in 1,000 to be allowed to search at LDIS.

### **MATCH ESTIMATOR**

1. From Analyst Workbench, click on Popstats. Alternatively, from Analyst Workbench, from the File Menu under Go, click on Popstats.
2. Under Workbench Explorer, in Popstats, choose Match Estimation.
3. Enter your Specimen ID and Specimen Details (allele calls.)
  - a. Only include the original 13 CODIS core loci in the calculations.
  - b. Indicate any obligate allele by marking the allele with a plus sign (+) [e.g. 8,9+,10] as well as for a partial locus [e.g. 10+].
  - c. Number of Loci Allowed to Miss = 0
  - d. Click Calculate
4. Evaluate the Match Estimation calculation results, as shown in the Match Estimation Summary page that opens when the calculation is complete.
  - a. In order for a sample to be eligible for CODIS entry and searching, the inverse MRE results should be:
    - i. >10,000,000 for NDIS searching
    - ii. >10,000 for SDIS searching
    - iii. >1,000 for LDIS searching

1. If the inverse MRE number is too low for searching, the analyst may be able to add in obligate alleles, additional loci, etc. depending on the quality of the profile, to attempt to enable the profile to be eligible for searching.
  2. To view the profile information, click on the Match Estimator Target Profile tab. (A vertical tab on the left side of the Match Estimation tab screen).
5. Print the Match Estimation Report for the sample by clicking the Print Icon. Include this report for review in the DNA case file containing the data.
- a. Alternatively, the Match Estimation Report can be printed by clicking on the File Menu, and choosing Print. Choose Match Estimation Report.

### **Obligate Alleles - Mixtures**

Mixture profiles that have been compared to knowns and/or other profiles in the case may result in the determination of 'obligate alleles'. Obligate alleles can be alleles that are foreign to the known reference in the case, or alleles deemed to be likely attributed to the perpetrator, based on the overall evaluation of the data. (Obligate alleles are often used when the mixture profile is obtained from an intimate sample.) If the obligate alleles have been determined to be from a putative perpetrator, these alleles can be designated as such for CODIS entry by marking the allele with a plus sign (+). They are considered 'obligate' since they are required to be present in any candidate profile returned from a database search. The use of obligate alleles will narrow the pool of possible candidate profiles returned from a database search. (For example, with an intimate sample, if the casework profile is 8,9,10 and the victim is 8,9, then the obligate allele is 10 and would be indicated on the CODIS Entry sheet as 10 {partial}, or 8,9,10+. (Only candidate matches with a 10 at that locus will be returned.)

### **Partial Profiles – Inconclusive Loci**

The obligate allele concept may also apply to situations where a partial profile is obtained from a casework sample, where some loci have yielded inconclusive data. The partial profile notation is denoted for inconclusive loci if the locus is entered. (For

example, if the casework profile is 13 below stochastic threshold, with apparent stochastic effects causing the sister allele to fall below detection threshold, then the locus could be indicated on the CODIS Entry sheet as 13, Partial Locus checked, and Partial Profile YES and entered as such.) Addition of this information will narrow the pool of possible candidate profiles returned from a database search, and may also add enough information to make a profile searchable at a higher level of the CODIS system.

## **V. UPLOADING DATA TO SDIS**

Data is sent to SDIS (Massachusetts State Police Crime Laboratory) for comparison to casework profiles and convicted offenders from across Massachusetts. Incremental uploads are autoscheduled at a minimum in concordance with the State's searching schedule; uploads can be also sent manually as needed. Full uploads are typically sent as needed, upon notification by SDIS, NDIS or the CODIS Staff (e.g. CODIS Help Desk, etc.).

### **TO MANUALLY SEND AN INCREMENTAL UPLOAD**

1. From Analyst Workbench, go to Tools in the File Menu.
2. Click on 'Incremental Upload' (will display a checkmark when chosen).
3. Under Tools, again, click on 'Generate'.
4. Exit Analyst Workbench.

### **TO MANUALLY SEND A FULL UPLOAD**

1. From Analyst Workbench, go to Tools in the File Menu.
2. Click on 'Full Upload' (will display a checkmark when chosen).
3. Under Tools, again, click on 'Generate'.
4. Exit Analyst Workbench.

### **TO CONFIRM THAT THE SAMPLES WERE SUCCESSFULLY UPLOADED**

An Upload Report is automatically sent to the BPD Crime Lab when the data from the BPD Crime Lab is uploaded at SDIS or NDIS.

1. From Analyst Workbench, click on Message Center.
2. In Workbench Explorer, double click on Upload Reports.
3. New messages will be bolded. Double click on the message to execute it. From the Print Reports tab, Click OK to view reports. **Always open the oldest upload report first to maintain the correct date history and audit trail.** There are 1-4 Upload Reports to view. Use arrows at top left of screen to view all pages of the report. Close one report to view the next.
4. Observe any samples which are reported as "Specimen Data Deleted/Rejected" or any samples which have any notations or codes displayed (the key explaining the codes is printed at the bottom of the page.) Address any codes as needed.
5. Exit Analyst Workbench.

## **VI. UPLOADING DATA TO NDIS**

Data is sent to NDIS for comparison to casework, convicted offender/arrestee, and other known profiles from across the United States. BPD (LDIS) data is sent to NDIS by the MSP (SDIS) only. Samples that meet NDIS acceptance criteria are marked for upload to NDIS at the SDIS level and then forwarded to NDIS for searching. Matches involving BPD data at the NDIS level are automatically sent to the BPD Crime Lab from NDIS and deposited in Match Manager. See “Match Manager from SDIS/NDIS Search” section for details on match disposition and reporting guidelines.

### **TO CONFIRM THAT THE SAMPLES WERE SUCCESSFULLY UPLOADED**

An Upload Report is automatically sent to the BPD Crime Lab when the data from the BPD Crime Lab is uploaded to SDIS or NDIS.

1. From Analyst Workbench, click on Message Center.
2. In Workbench Explorer, double click on Upload Reports.
3. New messages will be bolded. Double click on the message to execute it. From the Print Reports tab, Click OK to view reports. **Always open the oldest upload report first to maintain the correct date history and audit trail.** There are 1-4 Upload Reports to view. Use arrows at top left of screen to view all pages of the report. Close one report to view the next.
4. Observe any samples which are reported as “Specimen Data Deleted/Rejected” or any samples which have any notations or codes displayed (the key explaining the codes is printed at the bottom of the page.) Address any codes as needed.
5. Exit Analyst Workbench.

## **VII. AUTOSEARCHER**

The AutoSearcher program is used to search all of the casework DNA profiles entered into CODIS against each other to identify case to case hits.

1. From the Start Menu, open Analyst Workbench.
2. From Analyst Workbench, click on AutoSearcher.
3. From Workbench Explorer, click on BPDSTD.
  - a. This file was configured to include search criteria specific to BPD guidelines. BPD guidelines include searching and reporting matches of profiles meeting Match Rarity Estimate [MRE], and searching the profiles using a moderate stringency setting.
4. From the File Menu, choose AutoSearcher. From the dropdown, choose 'Perform Search'. Alternatively, click on the 'Perform Search' icon in the toolbar. Any matches will automatically be sent to Match Manager.
5. Close the AutoSearcher tab when the search is complete.
6. Open Match Manager from the Analyst Workbench to view matches. Under Workbench Explorer, click on BPD View – Candidate Match, any new matches will be bolded in red.



## **VIII. SEARCHER**

The Searcher program is used to search a single DNA profile entered into CODIS against other profiles in the database to identify case to case hits. The program is often used when searching a sample that is not stored in the database, such as search requests from External NDIS participating Labs, etc.

1. From the Start Menu, open Analyst Workbench.
2. From Analyst Workbench, click on Searcher.
3. From Workbench Explorer, Default Identity.
  - a. This file was configured to include search criteria specific to BPD guidelines. BPD guidelines include searching and reporting matches with profiles meeting Match Rarity Estimate [MRE], and searching the profiles using a moderate stringency setting.
4. A blank Specimen Screen will open. Enter the information for the DNA Profile to be searched.
  - a. Choose the Lab ID from the dropdown.
  - b. Enter the Specimen ID, Choose the sex from the dropdown (male, female, or unknown).
  - c. Enter the alleles from the profile to be searched.
  - d. The default match stringency is Moderate. The locus stringency can be changed to High or Low, by double clicking on the stringency box at the individual locus. Keep double clicking to change again.
5. From the File Menu, choose Searcher. From the dropdown, choose 'Perform Search'. Alternatively, click on the 'Perform Search' icon in the toolbar. Any matches will automatically populate in the Candidate Specimens Screen that opens. Dispositions can be updated on this screen. Matches will not be sent to Match Manager, unless they are flagged for sending to Match Manager. To flag a match or multiple matches for sending to Match Manager, Select that match or matches, and click on the Save Results to Match Manager button from the toolbar.
6. Close the Searcher tab when the search is complete.
7. Open Match Manager from the Analyst Workbench to view matches.

## **IX. VIEWING MATCHES FROM LDIS SEARCH**

Message Center will document messages relaying match information to the lab in the CODIS software. Match Manager is used to view any matches and track their subsequent interpretation and disposition.

1. From the Start Menu, open Analyst Workbench. Click on Message Center.
2. For match messages from an Autosearch or an LDIS search (Boston search against itself), Click on Match Manager in Analyst Workbench. Under Workbench Explorer, click on BPD View – Candidate Match.
  - a. There are several “BPD View” options set to commonly used views. In Match Manager, these are available under Workbench Explorer.
3. New messages will be highlighted in red.
  - a. Print out the Match Detail Report for the match. Highlight all matches and press the Print Icon. Choose Match Detail Report Short.
  - b. Change the Disposition to Pending Local Disposition while the match is evaluated.
  - c. Using the CODIS software, or the Crime Lab Files for all cases with BPD specimens involved in potential matches determine:
    - i. Which DNA analyst uploaded the sample by choosing View Specimen Details after right clicking on sample. (Newer cases will the assigned analysts initials in Case ID.)
    - ii. Which DNA case file contains the data for each specimen found in View Specimen Details. (Newer cases will list the case file in Case ID.)
    - iii. Whether either case has a suspect identified and known reference matched can be determined by looking at Source ID Yes on Match Detail Report or by looking at case file.
    - iv. Whether either case has already been involved in a previously reported Hit by checking Match Manager for previous hits to the same Specimen ID or in the CODIS Hit Manager in DNA Utilities.

- d. The CODIS Administrator will distribute the matches to the appropriate DNA analyst. Check the data for accuracy against the data recorded in the original DNA file. The original data tables and/or electropherograms are examined from each sample to confirm data accuracy.
- e. Determine whether the sample is a true match to the candidate specimen.
  - i. If the sample is not a match, the disposition should be changed to No Match in Match Manager, and the case file is filed away. The related Match Detail Report is appropriately filed away.
  - ii. If the sample is a true match, evaluate the case information in the Crime Lab Case File to determine if confirmation of the match is probative to the case.
    - 1. If confirmation is needed, fill out the information on the CODIS Match Worksheet and have the match worksheet confirmed by a second qualified analyst. Give the case files, Match Detail Reports and CODIS Match Worksheets to the CODIS Administrator. The disposition will be changed to Pending until the notification is ready for issue.

***LDIS Case to Case Hit:***

- a. If a true match has been identified, once all pertinent information is obtained, a Hit Notification is issued at a minimum to the investigator in charge of the case, the investigator's Supervisor, the Director of the Crime Lab, as well as the Suffolk County District Attorney's Office, and the Criminalist and DNA Analyst who worked the case. The notification will include the case(s) identifying information, and the evidence tested. Any/all previously reported Forensic Hit or Offender Hit linkages relating to the specimen(s) will be reported in the Hit Notification as well.
- iii. The disposition box in Match Manager is updated once the match has been confirmed (e.g. Offender Hit, Forensic Hit, and Investigative Information). NDIS guidelines on Hit Dispositioning are followed regarding final dispositions. For a non-match, with no notification, No Match is entered into the disposition box.

- iv. Investigations Aided – indicate that the investigation has been aided (if applicable) by changing the tally to 1.
  - 1. An investigation/incident can only be aided once.
  - 2. Only unsolved investigations may be aided.

## **X. VIEWING MATCHES FROM SDIS/NDIS SEARCH**

Message Center will document messages relaying match information to the lab in the CODIS software. Match Manager is used to view any matches and track their subsequent interpretation and disposition. Matches are automatically sent to the BPD Crime Lab from SDIS/NDIS and deposited in Match Manager.

1. From Start Menu, open Analyst Workbench, click on Message Center. New messages will be highlighted in red.
  - a. Print out the Match Detail Report for the match. Highlight all matches and press the Print Icon. Choose Match Detail Report Short.
  - b. Change the Disposition to Pending Local Disposition while the match is evaluated.
  - c. Using the CODIS software, or the Crime Lab Files for all cases with BPD specimens involved in potential matches determine:
    - i. Which DNA analyst uploaded the sample by choosing View Specimen Details after right clicking on sample. (Newer cases will list the assigned analysts initials in Case ID.)
    - ii. Which DNA case file contains the data for each specimen found in View Specimen Details. (Newer cases will list the case file in Case ID.)
    - iii. Whether either case has a suspect identified and known reference matched can be determined by looking at Source ID Yes on Match Detail Report or by looking at case file.
    - iv. Whether either case has already been involved in a reported Hit by checking Match Manager for previous hits to the same Specimen ID or in the CODIS Hit Manager in DNA Utilities.
  - d. The CODIS Administrator will distribute the matches to the appropriate DNA analyst. Check the data for accuracy against the data recorded in the original DNA file. The original data tables and/or electropherograms are examined from each sample to confirm data accuracy.
  - e. Determine whether the sample is a true match to the candidate specimen.

- i. If the sample is not a match, the disposition should be changed to No Match in Match Manager, and the case file is filed away. The related Match Detail Report is appropriately filed away.
- ii. If the sample is a true match, evaluate the case information in the Crime Lab Case File to determine if confirmation of the match is probative to the case.
- f. If confirmation is needed, fill out the information on the CODIS Match Worksheet and have match worksheet confirmed by a second qualified analyst. Give the case files, Match Detail Reports and CODIS Match Worksheets to the CODIS Administrator.

***SDIS/NDIS Case to Case Hit:***

- a. The matching lab is notified via Match Manager in the Note: box and a memo emailed to the contact individual for the matching laboratory. A CODIS Confirm Forensic Hit memo is prepared and sent/emailed to the matching laboratory. The memo contains case information on the Boston case including the lead investigator's contact information, the Incident #, case #, incident type, specimen ID and specimen description. (CODIS Administrators' contact information can be obtained via the CODIS Website on the CODIS computer.)
- b. Requests for confirmation of candidate matches should be routinely initiated within 30 days of the match date.
- c. The CODIS Administrator will change the disposition to Pending.
- d. If one of the BPD cases has hit to a previously confirmed offender with an SDIS/NDIS lab, then a notification may be sent to the investigators with no further confirmation process as a supplementary Hit Notification. The matching lab is notified via Match Manager in the Note: box and a memo emailed to the contact individual for the matching laboratory. Specimens will be dispositioned appropriately.
- e. A CODIS Hit Notification is prepared and administratively reviewed by a second examiner. The reviewed Hit Notification is then issued at a minimum to the investigator in charge of the case, as well as the Suffolk

County District Attorney's Office. The notification will include the case(s) identifying information and the evidence tested, as well as the information relayed from the matching laboratory (offender name, and any pertinent additional information listed, such as the social security number and date of birth. This information may vary according to the state jurisdiction that collected the DNA sample from the offender). Hit Notifications are routinely emailed at a minimum to the primary investigator, the primary investigators supervisor, district attorney's office CODIS point of contact, the Crime Lab Director, and the Criminalist and DNA Analyst assigned to the case. Additional notifications may be made as needed. A copy of the Hit Notification is included in the case file(s) and or LIMS involved in the Hit, and the original is filed with the CODIS Hit Notifications.

***SDIS/NDIS Case to Offender Hit:***

- a. If the sample is a true match, evaluate the case information in the Crime Lab Case File to determine if confirmation of the match is probative to the case.
  - i. No additional lab work is necessary if the sample has previously been reported as linked to an offender or to a known reference tested by BPD in the case. (If the sample has been linked to an investigative reference (i.e. bottle, cigarette butt) further confirmation is required.) The name of the individual who has previously been linked will be confirmed with the matching lab to verify that the two known samples have the same information. This should be done in writing (e.g. Conviction Match Memo). Documentation of the conviction match information will be maintained in the Conviction Match folder in the CODIS Hit Manager in DNA Utilities. After confirming that the information is the same for both known samples, the final disposition for this type of match is Conviction Match.

- a. If the case file is not located in a timely fashion, analysts should use computer records to determine if the case should be confirmed.
  - b. If further confirmation is required, the matching lab is notified via Match Manager in the Note: box and/or a memo emailed to the contact individual for the matching laboratory.
    - i. For Massachusetts matches, a notation in the Note: box of the Disposition window will initiate the confirmation process. (e.g. 'Offender Confirmation Required, <date> <Initials>') No additional external communication is necessary to initiate confirmation with MA SDIS.
    - ii. For interstate matches, a CODIS Confirm Offender Hit memo is also prepared and sent/emailed to the matching laboratory, requesting the matching lab initiate confirmation of their sample. (CODIS Administrators' contact information can be obtained via the CODIS Website on the CODIS computer.)
  - c. Requests for confirmation of candidate matches should be routinely initiated within 30 days of the match date. The disposition will be changed to Pending.
1. Once the confirmation information is obtained from the matching laboratory, a CODIS Hit Notification is prepared and administratively reviewed by a second examiner. The reviewed Hit Notification is then issued at a minimum to the investigator in charge of the case, as well as the Suffolk County District Attorney's Office. The notification will include the case(s) identifying information and the evidence tested, as well as the information relayed from the matching laboratory (offender name, and any pertinent additional information listed, such as the social security number and date of birth. This information may vary according to the state jurisdiction that collected the DNA sample from the offender). Hit Notifications are routinely emailed to the primary investigator, the primary investigators supervisor, district attorney's office CODIS point of contact, the Crime Lab Director, and the Criminalist and DNA Analyst assigned to the case. Additional notifications may be made as needed. A copy of the Hit



Notification is included in the case file(s) and/or LIMS involved in the Hit, and the original is filed with the CODIS Hit Notifications.

2. The Final disposition is updated only once the match has been confirmed, and a notification issued. For a true case to case match, Forensic Hit is chosen from the disposition drop down, and the Hit Notification number, date and the user's initials are entered into the Note: section of the Disposition window. For a true case to offender match, Offender Hit is chosen from the disposition drop down menu, with the Hit Notification number, date and the user's initials recorded in the Note: section. For a non-match, No Match is chosen from the disposition drop down menu; no further notations are needed for No Match dispositions
3. Investigations Aided – indicate that the investigation has been aided (if applicable) by changing the tally to 1.
  - a. An investigation/incident can only be aided once.
  - b. Only unsolved investigations may be aided.

## **XI. EXPUNGEMENT (DELETION) OF DNA PROFILE**

1. A casework DNA profile will be deleted (expunged) from the database
  - a. If the DNA profile is found to be consistent with:
    - a. The victim
    - b. An elimination standard (e.g. husband, consensual partner)
  - b. If information is obtained to indicate that the DNA profile is ineligible for CODIS entry. (e.g. was obtained from an evidence item collected from the suspect's person, or in the possession of the suspect when collected by law enforcement.)

### **To delete a specimen from LDIS:**

1. From Analyst Workbench, click on Specimen Manager.
2. Locate the sample of interest: From the File Menu, Under View, click New. Alternatively, in the toolbar, click on the Edit View Icon. In the General Criteria Tab:
  - a. Under Specimen ID: choose 'Like' and enter your sample name in the box.
  - b. Under Lab: Choose 'My Lab'
  - c. Click OK.
  - d. When the search results return, highlight the row containing your specimen.
3. From the File menu, select Delete.
4. The system displays a Specimen Delete dialogue box which prompts, "Do you want to delete: (Specimen ID)?"
5. Click the Yes button.
6. Print the Specimen Delete Report.
  - a. From Analyst Workbench, go to Message Center
  - b. Delete Reports should be bolded and show number of new reports.
  - c. Double click on Delete Reports
  - d. Double click on the relevant report in the list.

- e. Make a note on the Report as to the reason for deletion. Have a second qualified DNA Analyst confirm, including any applicable MRE calculations, and document review.
- f. Make a copy. Place the original report in the Deleted Specimen folder located in the Deleted CODIS Specimens file. Place the copy of the report in the DNA case folder containing the original data.
- g. Notify the Investigator of the removal of the Specimen from the database. Email or other notification is acceptable. Notes/copies of email should be placed in the DNA file and Criminalistics file.

**To Remove a specimen from SDIS, and continue searching at LDIS:**

1. From Analyst Workbench, click on STR Data Entry.
2. Locate the sample of interest: Type in the specimen ID in the Specimen ID box and press Query.
  - a. Highlight the sample and press ok.
    - i. In the dropdown under Specimen Category select the appropriate Specimen Category as indicated on the worksheet.
      1. LDIS Forensic Mixture and LDIS Forensic Partial for searching at LDIS
      2. Type a note in the comments section including a reason for the change, and your date and initials.
      3. Click the Save button.
3. Print the Specimen Details Report for the sample by clicking the Print button. All specimen detail reports need to be confirmed by another qualified analyst within the same business day as entry. Include this report in the DNA case file containing the data.
  - i. Alternatively, the Specimen Details Report can be printed from Specimen Manager.
    1. In Analyst Workbench, click on Specimen Manager.
    2. Locate the sample of interest. From the File menu, Under View click New. Alternatively, in the toolbar, click on the Edit View Icon.

3. In the General Criteria Tab:
4. Under Specimen ID: choose 'Like' from the dropdown and enter your sample name in the box.
5. Under Lab: choose My Lab
6. Click OK
7. When the search results come up, highlight the row containing your specimen and right click on it.
8. Click Print and choose Specimen Detail Report (short), and click Print

For additional information on the CODIS Software or other functions of the software, consult the CODIS Administrator's Handbook, the CODIS Training Manual or the CODIS Web site.

Revision Number	Effective Date	Approval Authority
2012.0	1/12/12	JKL
2013.0	12/18/13	JKL
2016.0	4/19/16	JKL
2016.1	6/1/16	JKL
2018.0	11/15/18	RWB
2018.0	6/8/20	Laboratory Director
2022.0	3/17/22	Laboratory Director



## Superintendent's Circular

School Year 2021-2022

NUMBER:  
LGL-3

DATE:  
July 14, 2021

### PUBLIC RECORDS REQUESTS

*This policy circular only applies to School Year 2021-2022.*

School Department staff members frequently receive requests from individuals and agencies, asking for information or documents and cite the Freedom of Information Act (FOIA) or the Massachusetts Public Records Law as the authority for honoring their requests.

The Massachusetts Public Records Law, M.G.L. c. 66 §10, provides that any person has a right to access public records. This right of access includes the right to inspect, copy or have copies of records provided upon payment of a reasonable fee. The Massachusetts General Laws broadly define "public records" as any books, papers, maps, photographs, electronic storage media, computer files, digitally stored material or any other information regardless of form, which is made or received by employees of public agencies unless the material falls into one of several recognized exemptions. Requests for public record information must be in writing; therefore, you should require that any oral requests for public record information be placed in writing by the requestor prior to responding to such a request. Such writing must be signed, dated and contain the address of the requestor.


**RECORDS REQUEST:** All written public records requests must be sent to the Office of Legal Advisor or filed through the City of Boston's public records request [portal](https://www.boston.gov/departments/public-records). You can access the public records request portal by visiting <https://www.boston.gov/departments/public-records> or clicking the "Public Records Request" link at the bottom of every page of the [boston.gov](https://www.boston.gov) website. In order to ensure a prompt response, use of the City's public records request portal is the preferred method for all requests. The Office of Legal Advisor will review each request to see if it falls within an exception to the public records law and will coordinate with your office or school the search, retrieval, and copying of such information. The law provides that Boston Public Schools must respond to a request for public records **within ten (10) days** of our receipt of such a request. It is imperative, therefore, that once you receive a public records request, it is faxed or delivered to the Office of Legal Advisor. It is also imperative that, if you receive a request from the Office of Legal Advisor to compile public records, you do so expeditiously or call the Office of Legal Advisor if you cannot comply in a timely manner with its request for information.

**SUBPOENA:** When receiving a subpoena for student records, personnel records, medical records, or any other document, **a copy of the subpoena must be emailed or delivered immediately to the Office of Legal Advisor for review.** Subsequent to that, please forward all responsive records with the original subpoena to the Office of Legal Advisor. Such a subpoena should be emailed or delivered even if it is addressed to an individual, rather than the "keeper of the records." Witness subpoenas (i.e., a subpoena that seeks testimony rather than documents) should also be emailed or delivered to the Office of Legal Advisor for appropriate consultation. Please email [legal@bostonpublicschools.org](mailto:legal@bostonpublicschools.org).

**For more information about this circular, contact:**

<b>Name:</b>	Catherine Lizotte
<b>Department:</b>	Office of Legal Advisor
<b>Mailing Address:</b>	2300 Washington Street, Roxbury, MA 02118
<b>Phone:</b>	617-635-9320
<b>Fax:</b>	617-635-9327
<b>E-mail:</b>	<a href="mailto:clizotte@bostonpublicschools.org">clizotte@bostonpublicschools.org</a>

Dr. Brenda Cassellius, Superintendent

 <b>BOSTON</b> Public Schools	<b>Superintendent's Circular</b>  <b>School Year 2021-2022</b>	<b>NUMBER:</b> LGL-4  <b>DATE:</b> July 14, 2021
---	--	--

## SUBPOENAS

*This policy circular only applies to School Year 2021-2022.*


**SUBPOENA:** When receiving a subpoena for student records, personnel records, medical records, or any other document, **a copy of the subpoena must be emailed or delivered immediately to the Office of Legal Advisor for review.** Subsequent to that, please forward all responsive records with the original subpoena to the Office of Legal Advisor. Such a subpoena should be emailed or delivered even if it is addressed to an individual, rather than the “keeper of the records.” Witness subpoenas (i.e., a subpoena that seeks testimony rather than documents) should also be emailed or delivered to the Office of Legal Advisor for appropriate consultation.

If sending by email, please email [legal@bostonpublicschools.org](mailto:legal@bostonpublicschools.org)

**For more information about this circular, contact:**

<b>Name:</b>	Catherine Lizotte
<b>Department:</b>	Office of Legal Advisor
<b>Mailing Address:</b>	2300 Washington Street, Roxbury, MA 02119
<b>Phone:</b>	617-635-9320
<b>Fax:</b>	617-635-9327
<b>E-mail:</b>	<a href="mailto:clizotte@bostonpublicschools.org">clizotte@bostonpublicschools.org</a>

Dr. Brenda Cassellius, Superintendent

	<b>Superintendent's Circular</b>  <b>School Year 2021-2022</b>	<b>NUMBER:</b> LGL-7  <b>DATE:</b> July 14, 2021
---	--	--

**PRIVACY OF STUDENT INFORMATION AND STUDENT RECORD PROCEDURES:  
HOW TO RESPOND TO STUDENT RECORD REQUESTS IN COMPLIANCE WITH  
FERPA AND STATE LAW**

*This policy circular only applies to School Year 2021-2022.*

**I. GENERAL INFORMATION**

These student record procedures pertain to all information maintained by the Boston Public Schools concerning a student in which he/she may be individually identified.

The student record consists of two parts: the transcript and the temporary record.

- A. The transcript contains administrative records that constitute the minimum data necessary to reflect the student's educational progress and to operate the educational system. The transcript is limited to the name, address, and phone number of the student, the student's birth date, name, address and phone number of the custodial parent or guardian, course titles, grades (or the equivalent when grades are not applicable), course credit, grade level completed, and the year completed. The transcript must be retained for at least sixty (60) years after the student leaves the school system.
- B. The temporary record is all other student record information besides the transcript. Temporary record information may include health information, disciplinary information, exemplars of student work, special education or 504 plan documents, incident reports, and any other information kept by the school which identifies the student individually. Duplicates of an original record do not need to be kept as part of the temporary record. The temporary record should be destroyed no later than **seven (7) years** after the student leaves the school system, provided proper notification is given as directed below.

**II. PARENTS (AND STUDENTS) HAVE A LEGAL RIGHT TO CONTROL ACCESS TO STUDENT INFORMATION**

Both federal and state law provide that a parent, and any student that is 14 or older and/or in grade nine or above, have a legal right to control access to the student's educational record. The [Family Educational Rights and Privacy Act \(FERPA\)](#) and



[Massachusetts law](#) define the parent's/student's right to access, seek to amend, and exercise control over the disclosure of personally identifiable information in the student record. The Boston Public Schools is legally responsible to respect and protect the parent's/student's rights to privacy and control under FERPA and state law. **Violation of these legal rights can subject BPS to sanctions, including termination of federal funding, and can subject BPS employees to discipline, up to and including termination.**

BPS notifies all students and parents of these rights annually by means of the "Guide to BPS for Students & Families." The Guide for Students & Families identifies the limited types of information that may be released without consent (see Directory Information below). By September 30 of each year, parents and students have a right to inform the school that such information shall not be released without direct consent.

Schools receive requests for student record information in many different ways and from many different sources. By law, a school's response to a request for student records must vary depending on who is making the request and what is being requested. Below are descriptions of the main categories of requests that schools may need to address. If the information below does not directly describe a situation presented, the school should contact the Office of Legal Advisor at [legal@bostonpublicschools.org](mailto:legal@bostonpublicschools.org) for more direction.

### III. REQUESTS AND CONSENT BY PARENT/STUDENT

When a parent or student seeks to access, amend or consent to share student records, the following definitions will aid you in understanding and complying with applicable law.

- A **parent** is the student's natural parent, a guardian, or an individual acting as a parent in the absence of a parent or guardian.
- A **custodial parent** is any parent with whom a child resides, whether permanently or for periods of time, and who supervises the child.
- A **non-custodial parent** is any parent who does not have physical custody of the child and who does not reside with or supervise the child, even for short periods of time, by court order.
- An **eligible student** is a student who is at least 14 years of age and/or has entered the ninth grade.

#### A. Request to Inspect/Copy Records.

1. **Custodial Parents and Eligible Student.** A custodial parent, and/or an eligible student have a right to inspect all portions of the student record upon request. The record will be made available to the custodial parent and/or

eligible student **no later than ten (10) days** after the request. The custodial parent and/or eligible student have the right to receive copies of any part of the record. In addition, the custodial parent and/or eligible student may request to have parts of the record interpreted by a qualified professional of the school, or may invite anyone else of their choosing to inspect or interpret the record with them. Please see Attachment 1 for the process of fulfilling a custodial parent's or eligible student's request for the student record.

2. **Non-Custodial Parents.** Non-custodial parents must be given access to their children's student records unless the school has been given written documentation that establishes either:

- a) The non-custodial parent has been denied legal custody by a court based upon a threat to the student or to the custodial parent;
- b) The non-custodial parent has been denied visitation or has supervised visitation;
- c) Access to the student or to the custodial parent has been restricted by a court-issued protective order against the non-custodial parent, provided such protective order does not specifically allow access to student record information;
- d) There is an order of a probate and family court judge which prohibits the distribution of student records to the non-custodial parent.

A school that receives a request for student record information from a non-custodial parent should send a copy of the notification attached as Attachment 2, via certified and first-class mail, to the custodial parent prior to providing student records to the non-custodial parent. The notification must be in English and the primary language of the custodial parent. If no documentation related to any of the four (4) scenarios above is received within 21 days, the records must be provided to the non-custodial parent. If documentation related to any of the four (4) scenarios above is received within 21 days, it must be kept in the student record and the non-custodial parent must be notified, via certified and first-class mail, of the reason for denial of access.

## **B. Request to Amend Student Record**

The custodial parent and/or eligible student have the right to add relevant comments, information, or other written materials to the student record. In addition, the custodial parent and/or eligible student have the right to make a written request that information in the record is amended or deleted, except information created by a special education team, which may not be amended or deleted until after acceptance of the individualized education plan or completion of the appeals process. The custodial parent and/or eligible student have a right to a conference with the school principal to make their objections known. Within one week after the conference, the principal must render a decision in writing. If the custodial parent and/or eligible student are not satisfied with the decision, it may be appealed to the operational leader.

### C. **Consent to Share Student Information**

The custodial parent and/or eligible student have the legal right to consent to share the student record with any person or entity they choose. A school should use Attachment 4 to document the custodial parent's and/or eligible student's specific, informed, written consent and include the signed consent in the student record.

**Except as specifically noted below, no individuals or organizations other than the custodial parent, eligible student, and authorized school personnel are allowed to have access to information in the student record without the specific, informed, written consent of the custodial parent or the eligible student.**

## IV. **THIRD-PARTY REQUESTS FOR STUDENT-IDENTIFYING INFORMATION: CONSENT NOT REQUIRED OR ASSUMED BY OPERATION OF LAW**

A. **Subpoenaed Records.** Boston Public Schools will produce documents requested in court orders or lawfully issued subpoenas. Such requests should be emailed immediately to the Office of Legal Advisor. All records sought by the court order or subpoena should be forwarded via courier mail or hand delivery as soon as possible. Attachment 3 should be completed and used to notify the parent and/or eligible student that subpoenaed information will be provided absent further court orders.

B. **Authorized School Personnel.** Authorized school personnel (those providing direct services to the student, administrative staff whose duties require them to access the student record, and an evaluation team that evaluates a student) shall have access to the student's school record when such access is required in the performance of their official duties.

C. **Directory Information.** Unless the parent or eligible student has previously indicated in writing their disapproval of the release of such information, the school may release the following directory information: student's name, age, grade level, and dates of enrollment. BPS notifies students and parents annually of the types of information that will be released by means of the "Guide to BPS for Students & Families," and allows custodial parents and students until September 30 of each year to inform BPS that such information will not be released without prior consent.

D. **Military Recruiters and Higher Education Institutions.** Unless a parent or student has previously objected in writing in response to notification through the publication of the "Guide to BPS for Students & Families," military recruiters and institutions of higher education must be provided, upon written request, with the names, addresses, and telephone numbers of secondary school students. All requests by military recruiters for such information must be forwarded to the Office of Legal Advisor for centralized processing.

**E. Specified State Agencies and Local Authorities.** A school may release student record information without prior written consent to the following agencies when acting in their official capacities: Department of Children and Families, Department of Youth Services, a probation officer, or a justice of the court. Attachment 3 should be used to notify parents of such requests.

**F. Transfer Schools.** When a student seeks or intends to transfer to another school, the student record can be sent to the receiving school.

**G. School Nurses and State Health Department.** School nurses and local and state health department officials may have access to student health record information when such access is required in the performance of their official duties. For further information related to student health information, please consult Superintendent's Circular LGL-16, Student Health Information.

**H. Health or Safety Emergency.** Without the consent of the parent or eligible student, a school may disclose information regarding a student to appropriate parties in connection with a health or safety emergency if knowledge of the information is necessary to protect the health or safety of the student or individuals and if the appropriate procedure has been followed. That does not mean that anyone who asks, and who thinks something is amiss or might happen, has a right to access personally identifiable student information.

(1) **Required Criteria.** The regulations implementing FERPA ([34 CFR § 99.36](#)) requires that each of the following criteria be met:

a. The request is made "in connection with an emergency."

i. "Emergency" means the request must be related to an **actual, impending, or imminent emergency**

ii. BPS requires that a school consider the following criteria to determine whether the request is made in connection with an emergency:

- o The seriousness of the threat to the health or safety of the student or others
- o The need for the information to meet the threat
- o Whether the requestor is in a position to deal with the emergency; and
- o The extent to which time is of the essence in dealing with the emergency.

- iii. Any release of records is **limited to the period of the emergency**; if the emergency is over no further release of student information is allowed.
- b. There is an **articulable and significant threat** to the health or safety of the student or other individuals.
- c. The requestor (usually law enforcement, public health officials, and medical professionals) **needs the information in order to protect** the health or safety of the student or other individuals.
- d. No blanket release of personally identifiable information is allowed. Any release of information must be **narrowly tailored considering the immediacy, magnitude, and specificity of the threat**.
- e. The determination is made on a **case-by-case basis taking into account the totality of the circumstances** pertaining to the threat to the health or safety of the student or others.
- f. Within a reasonable time after making the disclosure, **the school must record in the student's record** the articulable and significant threat that formed the basis for the disclosure, and to whom the information was disclosed.

## **V. THIRD-PARTY REQUESTS FOR PUBLIC RECORDS CONTAINING ONLY REDACTED AND/OR NON-STUDENT-IDENTIFYING INFORMATION**

Upon receipt of a third-party request for public records, the school should immediately send a copy of the request via email to the Office of Legal Advisor for review and direction. All public records requests must be reduced to writing, dated, and signed by the requestor, and must contain the return address information of the requestor. For more information see Superintendent's Circular LGL-3, Public Records Requests.

## **VI. DESTRUCTION OF STUDENT RECORDS**

The law sets forth different time periods for the retention and destruction of different portions of student records. These different time periods are set forth below:

**A. Transcripts** - A student's transcript must be maintained by the school department for sixty (60) years following the student's graduation, transfer, or withdrawal from the school system.

**B. Periodic Review of the Temporary Record** - While a student is enrolled in a school, the principal/headmaster or his/her designee shall periodically review all

students' temporary records and identify for destruction any misleading, outdated or irrelevant information. This may include, particularly, exemplars of student work or other impertinent information. Prior to destroying any such information, however, the student and his/her parent must be given written notification of the school's intent to destroy such information and must be given the opportunity to receive the information or a copy of the information prior to its destruction.

**C. Temporary Record Destruction** - The temporary record of any student may be destroyed no later than seven (7) years after the student transfers, graduates or withdraws from the school district, if the student and his/her parent/guardian have been given written notification that includes the approximate date of the destruction of the temporary record and indicating their right to receive the information in whole or in part at the time of the student's graduation, transfer or withdrawal from the school system or prior to its destruction. Such notice must be in addition to the annual notice issued by Boston Public Schools in the "Guide to BPS For Students & Families."

For more information about this circular, contact:

<b>Name:</b>	Catherine Lizotte
<b>Department:</b>	Office of Legal Advisor
<b>Mailing Address:</b>	2300 Washington Street, Boston, MA 02119
<b>Phone:</b>	617-635-9320
<b>Fax:</b>	617-635-9327
<b>E-mail:</b>	<a href="mailto:clizotte@bostonpublicschools.org">clizotte@bostonpublicschools.org</a>

Dr. Brenda Cassellius, Superintendent

## **Attachment 1**

### **STUDENT RECORD REQUEST PROCEDURES**

1. Parent/guardian or eligible student requests for the student's record are received, processed, and sent to the requester directly by the school. Third-party requests are received by the Office of Legal Advisor, processed by the school, and then sent back to the Office of Legal Advisor for transmission to the requester.
2. The principal/headmaster will be responsible for certifying that all portions of the student record have been copied as a response to the requestor. The principal/headmaster will complete the checklist and certification. If the request is being sent to the parent, the certification will include the date sent to the parent. A copy of the checklist will be sent with the record, and the original will be retained by the school.
3. For third-party requests, the principal/headmaster will complete the same process, but provide the copy of the entire record and the checklist to the Office of Legal Advisor for review and delivery.
4. Requests received during the Summer months: By June 1 of each year, principals must identify who to contact for each week of the summer break and provide that list to the School Superintendent. The designated individual will check for incoming mail and for parent/guardian or eligible student requests, will obtain the records (copy and/or print), complete the checklist, and deliver them to the requester. In the event of a third-party request, the same protocol will be followed but the designated individual will send the record and the completed checklist to the Office of Legal Advisor.

## Attachment 2

### NOTICE OF NON-CUSTODIAL PARENT REQUEST FOR STUDENT RECORDS

VIA REGISTERED MAIL AND FIRST CLASS MAIL

Dear Custodial Parent of \_\_\_\_\_:

This is to notify you that a request from \_\_\_\_\_ was received on \_\_\_\_\_ for the following parts of your child's student record:

\_\_\_\_\_.

In accordance with federal and Massachusetts law, non-custodial parents must be given access to their children's student records, unless the school has been given written documentation that establishes either:

1. the non-custodial parent was denied legal custody by court order based upon a threat to the student or to the custodial parent;
2. the non-custodial parent has been denied visitation or has supervised visitation;
3. access to the student or to the custodial parent has been restricted by a court-issued protective order against the non-custodial parent, provided such protective order does not specifically allow access to student record information; or
4. there is an order of a probate and family court judge which prohibits the distribution of student records to the non-custodial parent.

The requested records will be released on \_\_\_\_\_ unless the documentation indicated in the paragraph above has been received by the Building Administrator of the School. If you have any questions, you may contact

\_\_\_\_\_ at \_\_\_\_\_.  
Sincerely,

\_\_\_\_\_  
Signature of Principal or Other Authorized School Employee

Dated: \_\_\_\_\_

**NOTE: This notice must be sent in both English and the primary language of the custodial parent.**



### Attachment 3

#### NOTICE OF DISSEMINATION OF STUDENT RECORD TO THIRD PARTIES FOR WHICH CONSENT IS NOT REQUIRED OR IS ASSUMED BY OPERATION OF LAW

Dear \_\_\_\_\_:

This is to notify you that a:

- ☐ subpoena
- ☐ request from a justice
- ☐ other (specify)

\_\_\_\_\_

has been received for the following parts of your/your child's student record:

\_\_\_\_\_

The Massachusetts regulations pertaining to student records state that the school system must comply with the above request but that this notification must be provided to you prior to the release of the records. In the case of a subpoena, court order, or request from a probation officer or the Department of Youth Services, you have the right to attempt to have the subpoena, order, or request stopped by a court.

The records will be released on \_\_\_\_\_. If you have any questions, you may contact \_\_\_\_\_ at \_\_\_\_\_.

Sincerely yours,

\_\_\_\_\_  
Signature of Principal or Other Authorized School Employee

\_\_\_\_\_  
Date

**NOTE: This notice must be sent in both English and the primary language of the custodial parent.**

Attachment 4

**PARENT'S OR STUDENT'S CONSENT FOR DISSEMINATION OF  
STUDENT RECORD TO THIRD PARTY**

My name is \_\_\_\_\_.

I am:

- ☐ the parent/guardian of a BPS student named: \_\_\_\_\_  
☐ a BPS student age 14 or over and in at least ninth grade

I give permission for the following third parties to

- ☐ inspect                      ☐ secure a copy of

the parts of my/my child's student record are noted below.

THIRD PARTIES:

---

---

REASONS FOR RELEASE OF RECORDS:

---

---

PARTS OF RECORD TO BE RELEASED*	PERMISSION GRANTED	PERMISSION DENIED
transcript information (includes identifying information, course titles, grades or their equivalent, and grade level completed).	<input type="checkbox"/>	<input type="checkbox"/>
disciplinary record	<input type="checkbox"/>	<input type="checkbox"/>
extracurricular activities	<input type="checkbox"/>	<input type="checkbox"/>
teacher and counselor evaluations and comments	<input type="checkbox"/>	<input type="checkbox"/>
attendance record	<input type="checkbox"/>	<input type="checkbox"/>
other (specify)_____	<input type="checkbox"/>	<input type="checkbox"/>

-----

_____ **Signature of eligible student or parent/guardian	_____ Student's Class	_____ Date
---	--------------------------	---------------

\* Before seeking the parent's or eligible student's consent, the school should cross out those items which have not been requested by the third party.

\*\* This form may be signed by a student or former student of fourteen years of age or older, or a student in the ninth grade or above, or a custodial parent or guardian.

**Attachment 5**

**CHECKLIST FOR RETRIEVAL OF COMPLETE STUDENT RECORD**

	YES	Not Applicable
PRINT ELECTRONIC STUDENT FILE from ASPEN, SNAP, and EDPLAN	<input type="checkbox"/>	<input type="checkbox"/>
Transcript information (includes identifying information, course titles, grades or equivalent, and grade level completed).	<input type="checkbox"/>	<input type="checkbox"/>
Disciplinary record	<input type="checkbox"/>	<input type="checkbox"/>
Nursing record	<input type="checkbox"/>	<input type="checkbox"/>
Special education record	<input type="checkbox"/>	<input type="checkbox"/>
ELL file	<input type="checkbox"/>	<input type="checkbox"/>
Attendance records	<input type="checkbox"/>	<input type="checkbox"/>
Physical restraint records	<input type="checkbox"/>	<input type="checkbox"/>
Counseling records	<input type="checkbox"/>	<input type="checkbox"/>
Correction of student record	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify)_____	<input type="checkbox"/>	<input type="checkbox"/>

\* The school should cross out those items which have not been requested.

**CERTIFICATION**

I, \_\_\_\_\_(PRINCIPAL/SCHOOL LEADER) of

\_\_\_\_\_School, certify that to the best of my knowledge, all of the components of the student record that are requested, applicable to this student, and maintained by the school or on an electronic BPS system have been copied and delivered to the requestor,

\_\_\_\_\_ [name], on \_\_\_\_\_ [date].

\_\_\_\_\_  
Signature

## **POLICY REGARDING PREPARING AND SHARING STUDENT INCIDENT REPORTS AND OTHER STUDENT INFORMATION WITH THE BOSTON POLICE DEPARTMENT**

The Boston Public Schools (“BPS”) is responsible for the safety and security of its students and school communities, and for ensuring that every student has the same opportunity to attend a school that is a safe place for learning. This responsibility requires BPS personnel to report school incidents to police when required by law. BPS personnel may also call police for assistance in responding to emergency situations. At the same time, BPS must abide by laws restricting the disclosure of students’ education records to non-school officials, and ensure that protected information is not improperly transmitted to third parties.

Employees in BPS’s Department of Safety Services work closely with school administrators to maintain safe learning environments for students and staff by both responding to incidents and by engaging in proactive partnerships with the schools they serve. These employees also serve as special officers licensed by the Boston Police Department (“BPD”), which supports the district by responding to incidents and investigating criminal activity. BPD employees, as non-school officials, do not have access to education records except in certain circumstances. The unique nature of Department of Safety Services employees’ dual roles requires a policy that establishes consistent standards for preparing student incident reports and for sharing those reports with non-school officials. BPS also requires a policy that describes those circumstances in which BPS personnel must report school incidents to police, and that makes clear that school administrators are solely responsible for administering and documenting discipline in accordance with the BPS Code of Conduct.

### **WHAT THIS POLICY COVERS:**

This policy covers: (1) mandatory reporting by BPS personnel to BPD for certain incidents; (2) standards for Department of Safety Services employees in preparing an incident report; (3) protocol for sharing such reports and other student information; (4) creation of a school safety working group; and (5) training and compliance requirements.

This policy addresses sharing between Safety Services employees and BPD. For requirements governing students’ education records and the legal requirements for sharing such records with families, school personnel, and other third-parties, please refer to [Superintendent Circular LGL-07, Privacy of Student Information and Student](#)

[Record Procedures: How to Respond to Student Record Requests in Compliance with FERPA and State Law.](#)

**PRINCIPLES:**

In developing this policy, The Boston School Committee and Boston Public Schools affirm the following principles:

1. All students have the right to feel safe and secure in school.
2. It is the responsibility of Boston Public Schools to provide for the safety and well-being of all students in its care and to ensure that they feel supported and secure in the learning environment.
3. It is the responsibility of the Boston Public Schools Department of Safety Services to enforce the law and to protect students, staff, guests, property, and school communities by responding to incidents as defined in section III(A) and by engaging in prevention and intervention strategies and initiatives that focus on student support.
4. It is the responsibility of school administrators to manage student conduct by implementing supports and interventions and by administering discipline in accordance with the BPS Code of Conduct.
5. Consistent with the Boston Trust Act, BPS will not cooperate with or assist in immigration enforcement activities, which include identifying, arresting, or detaining any person based solely on their immigration status or a suspected violation of federal civil immigration law, or providing personal information solely for the purpose of enforcing civil violations of U.S. immigration laws.

**LEGAL FRAMEWORK:**

The preparation and sharing of student education records and other student information by BPS personnel is governed by federal and state laws and local regulations. The Family Educational Rights and Privacy Act, [20 U.S.C. § 1232g](#); [34 CFR Part 99](#) (“FERPA”), and Massachusetts student records laws, [G.L. c. 71, § 34D](#); [603 CMR 23.00, et seq.](#) restrict access to a student’s education record (any information that identifies a student and is maintained by the school) (“education record”) to the eligible

student, parent, and authorized school personnel, unless a legal exemption applies. As BPS employees, Department of Safety Services employees are required to adhere to FERPA's disclosure restrictions with respect to education records, even when the disclosure is to other city departments, including BPD. Department of Safety Services employees, however, also qualify as a BPS ["law enforcement unit"](#) under FERPA. [Records created and maintained by a law enforcement unit](#), such as incident reports, are not considered education records under FERPA and therefore are not subject to disclosure restrictions. Department of Safety Services employees are also special officers licensed by BPD pursuant to [BPD Rule 400A](#), and are required to comply with BPD rules and directives. Finally, there are several Massachusetts laws that either require school officials to report certain incidents to police, or provide BPD with the exclusive authority to investigate and report on certain crimes.

## **I. DEFINITIONS**

For purposes of this policy, the following terms shall have the following meanings:

**BPD** means the Boston Police Department, which includes the Boston Regional Intelligence Center (BRIC).

**BPD 1.1** means the Incident Report that is prepared by officers and special officers of the Boston Police Department and is filed with and maintained by the Boston Police Department.

**Code of Conduct ("COC")** means the Boston Public Schools Code of Conduct.

**Crimes** means all criminal and delinquency offenses.

**Incident Report** means a written record created by a Department of Safety Services employee that pertains to student or school activity, in the form of an SSR1 or a BPD 1.1. These reports, because they are created by Safety Services and are maintained by either BPS or BPD are typically not considered educational records and are thus not protected under FERPA, unless they are used for school disciplinary purposes.

**Intelligence Report** means any written report or narrative created by a Department of Safety Services employee that pertains to student activity other than the activity permitted to be documented in an Incident Report by this policy, including activity that is

documented for intelligence gathering purposes or for the sole purpose of reporting observations.

**School Safety Report or SSR1** means the Incident Report that is prepared by Safety Services employees and is filed with Safety Services.

**Safety Services** means the Boston Public Schools Department of Safety Services.

**Safety Services employees** means employees in Safety Services who are employed by BPS and licensed as special officers by BPD.

**School Administrator** means the school leader, building administrator, or other school official who is responsible for overseeing discipline in the school.

**Student Activity** means any activity involving one or more BPS students occurring on BPS property, on BPS buses, at or near school bus stops, while BPS students are on their way to and from school, and while BPS students are participating in any school-sponsored activities, whether on or off school grounds.

## II. REPORTING ACTIVITY TO THE BOSTON POLICE DEPARTMENT

Several Massachusetts laws require BPS personnel to notify police about certain incidents and to provide information necessary for police to investigate:

- Missing child - [G.L. c. 22A, § 4](#);
- Student in possession of a dangerous weapon at school - [G.L. c. 71, § 37L](#);
- Incident of bullying or retaliation when there is a reasonable basis to believe that criminal charges may be pursued against the aggressor, unless the principal determines that the bullying and retaliation can be handled appropriately within the school or district - [G.L. c. 71, § 37O](#); [603 CMR 49.06\(2\)](#).

Other laws establish BPD's authority to investigate and document certain incidents:

- Incidents of rape or sexual assault - [G.L. c. 41 § 97D](#) (please refer to [Superintendent's Circular EQT-3, Sexual Misconduct Towards Students](#), for BPS protocol for reporting these incidents);
- Incidents involving stalking or harassment or a violation of a restraining order - [G.L. c. 258E, § 8](#).

BPS has also established a protocol for reporting certain incidents to police. Please refer to [Superintendent's Circular SAF-04, Incident Data--Reporting and Release](#).

### **III. REQUIREMENTS FOR SAFETY SERVICES EMPLOYEES - PROCEDURES FOR PREPARING AND SHARING INCIDENT REPORTS**

#### **A. INCIDENT REPORT PREPARATION BY SAFETY SERVICES EMPLOYEES**

Safety Services Employees may only document Student and non-Student Activity pursuant to the provisions of sections 1 and 2 below. As described in section 3 below, activity that is not listed in sections 1 or 2 may only be documented by the School Administrator, if the School Administrator determines that such activity may qualify as a violation of the Code of Conduct.

##### **1. CRIMINAL ACTIVITY**

Safety Services employees may document only the following Student Activity by preparing and filing a BPD 1.1:

- (a) All felony Crimes;
- (b) Non-felony Crimes of assault and battery, hazing, those involving stalking behavior or sexual behavior, and threats that could have caused the person to whom they were conveyed to fear that the speaker had both the intention and ability to carry them out;
- (c) Possession of and possession with intent to distribute controlled substances as defined in [G.L. c. 94C](#) (other than possession of 2 ounces or less of marijuana, pursuant to G.L. c. 94C, §§ [32L](#) and [32M](#));
- (d) Possession of dangerous or electrical weapons;
- (e) Other non-felony Crimes where a victim or victim's parent or guardian requests a report.

In determining whether Student Activity falls within the above classifications, Safety Services employees must adhere to the provisions of G.L. c. 71, § 37P which in part require that "SROs [school resource officers] shall not serve as school disciplinarians, as enforcers of school regulations or in place of licensed school psychologists, psychiatrists or counselors and that SROs shall not use police powers to address traditional school discipline issues, including non-violent disruptive behavior."



## 2. NON-CRIMINAL ACTIVITY

Safety Services employees may document only the following Student Activity using a School Safety Report (SSR1):

- (a) missing child ( BPD may also write a BPD 1.1., see above);
- (b) sick/injury assist;
- (c) medical evaluation or other medical emergency (BPD also responds to medical-related incidents when an ambulance is called and completes a BPD 1.1).

SSR1s may also be prepared for non-Student Activity, including but not limited to (i) found property or evidence; (ii) found needles/syringes; (iii) found weapons; (iv) found controlled substances; (v) found property damage/graffiti; (vi) hazardous material incident; (vii) safe mode/containment drill; (viii) trespass.

## 3. OTHER ACTIVITY NOT LISTED ABOVE

- a. If an activity is not listed above, it shall not be documented in a Incident Report. Student Activity that occurs in school and that may qualify as a violation of the Code of Conduct must be documented by the School Administrator or designee in the BPS Student Information System (SIS).
- b. When a Safety Services employee is the first to respond to or witness such activity, the Safety Services employee must report such activity to the School Administrator, but may not prepare an Incident Report. If the School Administrator determines that such activity may qualify as a violation of the Code of Conduct, the School Administrator must document such activity in the BPS Student Information System (SIS).
- c. Safety Services employees shall not prepare Intelligence Reports.

## **B. INFORMATION CONTAINED IN AN INCIDENT REPORT**

- 1. Because Safety Services employees may be considered school officials with access to students' education records, they may not redisclose information obtained from those education records to non-school officials without consent or pursuant to an exemption to FERPA or state law, such as in the event of a health or safety emergency. Therefore, Incident Reports may not be prepared using information

obtained from an education record, except for “Directory Information,” as defined by BPS in its annual Guide to the Boston Public Schools.<sup>1</sup>

2. Where FERPA and state student records laws only apply to the disclosure of education records, they do not prohibit the preparation of an Incident Report based on a Safety Services employee’s personal knowledge or observations. However, Safety Services employees shall not use personal knowledge or observations to prepare an Incident Report if:

- (a) the knowledge was originally obtained from an education record;
- (b) the knowledge or observations are not directly related to the explicit situation for which the Incident Report is prepared.

3. In no event shall an Incident Report contain the following information:

- (a) Immigration status
- (b) Citizenship
- (c) Neighborhood of residence
- (d) Religion
- (e) National origin
- (f) Ethnicity
- (g) Students’ native or spoken language
- (h) Suspected or alleged gang involvement, affiliation, association, or membership
- (i) Participation in school activities, extracurricular activities outside of school, sports teams, or school clubs or organizations
- (j) Degrees, Honors, or Awards
- (k) Post-high school plans

#### **IV. PROTOCOL AFTER AN INCIDENT REPORT IS PREPARED**

Safety Services employees are required by BPD to prepare and file BPD 1.1s at the BPD district station on the same day the incident occurs. Once filed, the BPD 1.1 is a BPD record.

Prior to preparing a BPD 1.1, a Safety Services employee shall inform the School Administrator. Within 24 hours of receiving notification of an Incident Report, the School Administrator shall communicate with affected students and their families to discuss the

---

<sup>1</sup> For the 2020-2021 school year, “Directory Information” shall be limited to: student’s name, age, grade level, and dates of enrollment.

incident resulting in the BPD 1.1 or SSR1. The School Administrator shall also notify their supervisor or school superintendent. Families shall be notified that they may request a copy of the SSR1 from the school in the student's or family's native language or a copy of the BPD 1.1. from the BPD district station.

## **V. SHARING INCIDENT REPORTS AND STUDENT INFORMATION WITH THE BOSTON POLICE DEPARTMENT**

### **A. SHARING INCIDENT REPORTS**

1. When a BPD 1.1 is filed, it is a BPD report.
2. Safety Services employees may not share any other Incident Report with any individual or entity other than the BPS Chief of Safety Services or Deputy Chief of Safety Services. The Chief and Deputy Chief shall only share Incident Reports with the liaison from the BPD School Unit, except if disclosure to other individuals or entities is required by court order or subpoena or pursuant to the public records law .

### **B. SHARING STUDENT INFORMATION NOT CONTAINED IN AN INCIDENT REPORT**

1. Safety Services employees may only share information obtained from an education record pursuant to an exception to FERPA or state law (such as providing Directory Information, responding to a subpoena or court order, or in the event of a health or safety emergency), or when such information is based on an employee's personal knowledge, subject to the limitations of section III(B)(2) above, which include that the knowledge or observations must be directly related to the explicit situation for which the information is sought.
2. Even when such sharing is permitted, Safety Services employees may not share any information concerning a student with any individual or entity other than the BPS Chief of Safety Services or Deputy Chief of Safety Services. The Chief and Deputy Chief shall only share information concerning a student with the liaison from the BPD School Unit. Immigration status or citizenship of a student, even if known based on an employee's personal knowledge, may not be shared. Other information listed in III(B)(3) above that is known based on an individual's personal knowledge may only be shared subject to the limitations in section III(B)(2) above and if determined by the Chief or Deputy Chief to be relevant to the request for such information. The

only exceptions to these rules are situations where it is necessary for Safety Services employees to transmit student information to non-school officials in order to respond to an immediate health or safety emergency.

3. Under the health or safety emergency exception, sharing information obtained from an education record is permitted when necessary to protect the health or safety of students or other individuals in connection with an actual, impending, or imminent emergency, and is limited to the period of the emergency. In making their determination of whether a situation rises to the level of a health or safety emergency, School Administrators may rely on BPD's assessment of a particular situation or incident.

## **VI. REPORTING AND AUDIT PROCEDURES**

### **A. MONTHLY REPORTING**

1. At the end of each month, Safety Services shall submit data for the preceding month to the superintendent. The data shall include: (i) number of Incident Reports written; (ii) for each Incident Report, the date of the incident, the nature of the activity, student age, grade, school, and whether the report was written in connection with an arrest; (iii) for each Incident Report shared externally, when and to whom it was shared; and (iv) a log of information shared pursuant to the health or safety exception. Specifically for SSR1s, the data shall also include why the data was shared and who authorized the sharing.

### **B. AUDITS**

1. No less frequently than twice per school year, the superintendent shall direct a central office audit of Incident Reports and other communications prepared or transmitted by Safety Services employees. At the superintendent's request, Safety Services shall provide the superintendent with copies of Incident Reports or other communications prepared or transmitted during a 30 day period as determined by the superintendent. The superintendent or designee shall audit such Incident Reports to determine whether they were prepared in compliance with this policy, and shall prepare a report summarizing the findings to share with the School Safety Working Group, described below.

## **VII. SCHOOL SAFETY WORKING GROUP**

A. The superintendent shall establish a School Safety Working Group (“Working Group”) that will be charged with further discussing issues related to this policy, receiving reports from the superintendent about the district’s implementation of this policy, and making recommendations to the School Committee.

B. The Working Group shall be composed of 12 members, representing the following groups: (i) a BPS student, nominated by the immigration, youth or community advocacy organization noted in (vi) below, with preference given to a student who attends a school that has historically experienced a high volume of arrests or Incident Reports; (ii) a parent or guardian chosen by the Citywide Parent Council; (iii) a member of the Boston Special Education Parents Advisory Council (SpEdPAC); (iv) a teacher chosen by the Boston Teachers Union (BTU); (v) a school leader, assistant principal or dean from a school with an assigned Safety Services employee, chosen by the superintendent; (vi) a representative from an immigration, youth, or community advocacy organization chosen by the School Committee; (vii) a representative from the BPS Office of Opportunity Gaps; (viii) a representative from the BPS operational leader team, or other BPS central office representative with responsibility for advising School Administrators on the Code of Conduct; (ix) a representative from the BPS Department of Safety Services; (x) an individual, who is not an employee of the City of Boston, with expertise in law enforcement and school safety laws and regulations, chosen by the School Committee; and (xi) two representatives from the superintendent’s student data working group (which made recommendations on this policy), nominated by the working group.

C. The Working Group shall meet with the superintendent or her/his designee on a quarterly basis for a presentation of the monthly data reports described in section VI(A)(1) for the past quarter. After the first year of the implementation of this policy, the Working Group shall meet with the superintendent or her/his designee on a semi-annual basis. The Working Group shall be provided with the data to be presented no later than 5 business days prior to each meeting. The Working Group may make recommendations to the superintendent during these meetings. The superintendent may choose to publish additional data related to this policy.

D. The Working Group shall make an annual presentation to the School Committee on its findings and recommendations.

E. Any records or data shared with the Working Group shall not contain identifying information about students, victims, witnesses, or other individuals, including details of incident narratives that may allow such individuals to be identified.

## **VIII. TRAINING AND COMPLIANCE**

### **A. ANNUAL ACKNOWLEDGMENT**

1. All BPS employees will sign an acknowledgment of responsibility for safeguarding student information under this policy, FERPA, and state student records laws.

### **B. TRAINING**

1. BPS shall design and provide training on this policy pursuant to the provisions below.
2. Safety Services employees shall receive training on this policy upon hire and every three years thereafter. Safety Services employees may also receive training pursuant to Rule 400A, as determined by BPD.
3. School Administrators shall receive training on this policy upon hire and every three years thereafter.

### **C. COMPLIANCE**

1. Violations of this policy may subject BPS employees to discipline, up to and including termination.

## **IX. PUBLICATION**

A summary of this policy shall be included in the annual BPS Guide to the Boston Public Schools, and shall be made available translated in BPS's nine major languages. The superintendent may issue a circular that further directs the implementation of this policy.

## **X. ANNUAL REVIEW**

In order to periodically assess this policy's effectiveness, the School Committee shall review this policy on an annual basis and determine whether any revisions are

necessary. The annual review may occur in conjunction with the Working Group's annual presentation to the Committee.

# **Critical Infrastructure Monitoring System Policy**

## **Metro Boston Homeland Security Region**



**Boston • Brookline • Cambridge • Chelsea • Everett • Quincy • Revere • Somerville • Winthrop**





## Contents

1. Introduction .....	2
1.1 Purpose .....	2
1.2 Historical Context.....	2
1.3 Assumptions .....	3
2. Organization.....	4
2.1 Participating Organizations .....	4
3. Operations and Management.....	5
3.1 Authority to Operate.....	5
3.2 External Users.....	5
3.3 24/7 Recording .....	6
3.4 Camera Capabilities.....	6
3.5 Camera Inventory .....	6
3.6 No Sound Recordings.....	6
4. Documentation of Access.....	6
4.1 Documenting Cross Jurisdictional Camera Access .....	6
4.2 Request Process .....	7
5. Oversight .....	7
5.1 CIMS Oversight.....	7
5.2 Ensuring Transparency and Protection of Civil Liberties.....	7
6. Administrator .....	8
6.1 Policy Approval.....	8
6.2 Policy Maintenance .....	8



# 1. INTRODUCTION

## 1.1 PURPOSE

The purpose of this Metro Boston Homeland Security Region (MBHSR) Critical Infrastructure Monitoring System (CIMS) Closed Circuit Television (CCTV) Policy is to: 1) identify an overarching organizational construct and organizing principles for a regional CIMS network; 2) delineate specific roles and responsibilities of individual jurisdictions, and; 3) ensure a process for information sharing that aligns with the protection of civil liberties of residents and visitors to the region.

Goal 2 of the MBHSR *Homeland Security Strategy (2022 – 2027)*, “Strengthen the Region’s capabilities to protect its Critical Infrastructure and Key Resources (CIKR),” includes *Objective 2.3: Strengthen infrastructure systems*, which identifies the need to enhance monitoring of infrastructure, as well as maintain and improve existing infrastructure systems such as law enforcement analytics tools and gunshot detection. Critical infrastructure includes those assets, systems, networks, and functions—physical or virtual—so vital to the United States that their incapacitation or destruction would have a debilitating impact on security, national economic security, public health or safety, or any combination of those matters. Key resources are publicly or privately controlled resources essential to minimal operation of the economy and the government.

The CIMS program may also be used to deter criminal activity and public disorder, reduce fear of crime, identify criminal activity and suspects, identify and gather possible evidence for use in criminal and civil court actions, document police actions, safeguard citizen and police officer rights, aid in Amber alerts or in the search for lost/missing children or elderly people, assist emergency services personnel when responding to incidents, assist with the monitoring of traffic conditions, evacuation route status, monitor transportation networks (airports, waterways, highways, tunnels, transit, intermodal), events and attractions, government facilities, severe weather events and otherwise assist officials with the provision of municipal services in order to enhance overall municipal efficiency, and assist with the training of department personnel.

## 1.2 HISTORICAL CONTEXT

The purpose of the CIMS program is to enhance the management of emergency situations, detect and deter terrorism, and otherwise protect the health, safety and welfare of those who live and work in, visit, and transact business with the Region.

The MBHSR CIMS network was launched in 2003 in preparation for the Democratic National Convention (DNC) in Boston in July of 2004. This network was made possible with the awarding of the Urban Areas Security Initiative (UASI) grant to the City of Boston and 8 surrounding cities and towns. The purpose of this project was to enhance collaboration and information sharing amongst law enforcement agencies in the region in order to keep residents safe, and more effectively and efficiently investigate crimes, with a focus on critical infrastructure within the region.



#### CIMS Successful Use Cases:

##### **Boston Marathon Bombing, April 2013**

During the 2013 Boston Marathon, two terrorists planted and detonated two homemade pressure cooker bombs near the finish line on Boylston Street in Boston. The resulting blast left 3 individuals dead and hundreds more injured. During the subsequent investigation, the CIMS cameras in Boston were utilized by local, state, and federal law enforcement agencies to help in the identification of the two terrorists responsible as officials were able to share images of the suspects just 3 days later.

##### **Winthrop Shooting, June 2021**

In June of 2021, a man shot and killed two Winthrop residents in a race-fueled attack. He had stolen a box truck and crashed into a home before going on foot and began shooting. CIMS camera usage in the area allowed Winthrop Police to determine the suspect's intent based on the video footage of the route he took.

Emerging and unique threats facing the Nation and the MBHSR have created significant challenges that support the need for a collaborative and interoperable camera network.

### **1.3 ASSUMPTIONS**

The following planning assumptions underpin the MBHSR CIMS Policy:

- This policy refers only to UASI-funded cameras within the region.
- The MBHSR CIMS Policy is the baseline agreed upon set of guiding principles that all jurisdictions will adhere to. Individual jurisdictions may choose to enact more strict policies at the local level.
- Jurisdictions are responsible for identifying critical infrastructure within their municipality.
- As technology continues to improve and become more advanced, the region must ensure it is updating its plans and policies in order to ensure the protection of civil liberties for citizens and visitors to the MBHSR.
- The MBHSR will routinely conduct audits to study funding decisions and their impact in order to better improve the CIMS program and make fiscally sound decisions.
- Some cameras may be located in a location where two jurisdictions share a border. These instances are left to those jurisdictions to decide how to proceed with regards to shared (or not shared) access to said cameras.
- While Cambridge is a part of the MBHSR, they do not participate in the CIMS program.

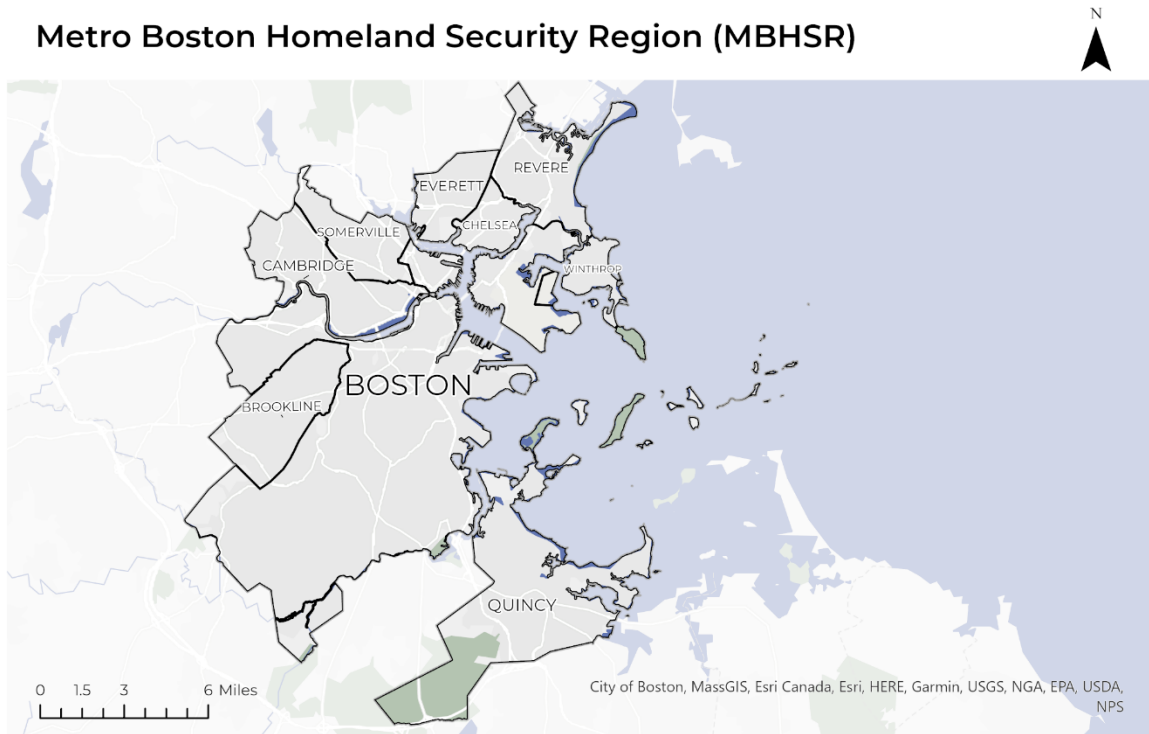


## 2. ORGANIZATION

### 2.1 PARTICIPATING ORGANIZATIONS

The MBHSR is comprised of nine (9) communities: Boston, Brookline, Cambridge, Chelsea, Everett, Quincy, Revere, Somerville, and Winthrop. All communities **except for Cambridge** participate in the CIMS program.

Metro Boston Homeland Security Region (MBHSR)



The following table depicts the number UASI CIMS cameras located within each MBHSR jurisdiction as of January 2022.

Boston	996
Brookline	12
Cambridge	<i>Does not participate in the CIMS program</i>
Chelsea	175
Everett	100
Quincy	115
Revere	69
Somerville	46
Winthrop	75



## 3. OPERATIONS AND MANAGEMENT

### 3.1 AUTHORITY TO OPERATE

The Commissioner/Chief or his/her designee within each jurisdiction will designate the number of System Administrators allowed to grant and oversee access to the CIMS network. Those designated System Administrators have the ability to create groups within their jurisdiction and assign permissions based upon job function or assignment.

Permissions are determined by the System Administrator and include the capabilities to view, rewind, download, or restrict camera footage. System Administrators are designated based upon their subject matter expertise to the MBHSR CIMS program and do not hold operational functions that would create a conflict of interest.

Jurisdictions may utilize the CIMS camera network at local dispatch areas, the front desk of public safety buildings, jurisdictional Emergency Operation Centers (EOCs), or where deemed necessary consistent with the purposes of the CIMS set forth in Section 1.1 above.

When authorized to do so by a jurisdiction, a requesting jurisdiction within the MBHSR will have the ability to view images/video produced by the CIMS cameras of the jurisdiction that has authorized and granted such access. MBHSR jurisdictions will designate that the Police Commissioner/Chief or their designee shall have exclusive authority to authorize other jurisdictions within the MBHSR to view, on an ongoing or time-limited basis and in real time only, footage recorded by the CIMS cameras. Other jurisdictions within the MBHSR may request a copy of archival footage produced by a jurisdiction's CIMS cameras pursuant to the procedures set forth in Section 5.2 of this policy.

### 3.2 EXTERNAL USERS

The Commissioner/Chief or his/her designee will review requests made for archived CIMS camera footage or requests for 'real time' viewing of specific cameras and approve based on the nature of the request. (See Section 5.2) When authorized to do so by a jurisdiction, a requesting jurisdiction within the MBHSR or external agency will have the ability to view images/video produced by the CIMS cameras of the jurisdiction that has authorized and granted such access.

MBHSR jurisdictions will designate that the Police Commissioner/Chief or their designee shall have exclusive authority to authorize partners outside of their own jurisdiction the ability to view, on an ongoing or time-limited basis and in real time only, footage recorded by the CIMS cameras. Outside agencies to a jurisdiction may request a copy of archival footage produced by a jurisdiction's CIMS cameras pursuant to the procedures set forth in Section 5.2 of this policy.

Traditionally, requests for archived or real time CIMS footage will be made in advance in order to allow for proper review of the request. However, in the event of a major incident with regional significance, a Commissioner/Chief or his/her designee may allow external authorization to view, in real time, cameras on the CIMS network. In order for this to occur, the two parties must both be operating on a compatible version of their viewer system.



### **3.3 24/7 RECORDING**

The CIMS network is active twenty-four (24) hours a day, seven (7) days a week ("24/7"). No personnel are assigned specifically to observe video monitor screens. Jurisdictions shall maintain a list of locations where monitors shall be located.

The network servers shall be maintained in a secure environment. Recording shall be stored in such a manner that the particular images can be identified by camera location and by the date and time recorded. Unless requested through the process outline in section 5.1, camera footage will be overwritten after no more than thirty (30) days.

### **3.4 CAMERA CAPABILITIES**

Cameras deployed as part of the MBHSR CIMS may have pan-tilt-zoom ("PTZ") or thermal capability. Cameras that are part of the CIMS network shall not utilize facial recognition capabilities if available.

Except during an active investigation, jurisdictions shall not utilize automatic identification or automatic tracking capabilities with CIMS cameras.

### **3.5 CAMERA INVENTORY**

Jurisdictions shall create and maintain a camera inventory of all cameras placed into service as part of the CIMS. This inventory will include installation date, location, brand/model, and dates out of service.

### **3.6 NO SOUND RECORDINGS**

The CIMS shall not monitor or record sound unless appropriate court orders are obtained.

## **4. DOCUMENTATION OF ACCESS**

### **4.1 DOCUMENTING CROSS JURISDICTIONAL CAMERA ACCESS**

A jurisdiction within the MBHSR may request archived camera footage from another jurisdiction in the event of a criminal investigation or access to live camera footage in instances such as preplanned major events (ie; Boston Marathon). In the event that access is granted to an outside jurisdiction (in accordance with section 4.1), the record of access will be documented and stored to capture the incident number, name of requestor, as well as the location and time of the requested video evidence. This will help support audits of the CIMS network and be used to impact future strategic decision making with regards to the CIMS program.



## 4.2 REQUEST PROCESS

In order to make a request to an MBHSR jurisdiction, the following form will be utilized. This process is currently utilized in Boston by Boston Police with the link to this form located here:

All other (8) jurisdictions will utilize a form that will be initially hosted by Boston OEM until individual jurisdictions are able to get a similar version of this form hosted and owned by their own agencies. Once completed, forms will be sent to a jurisdiction's Commissioner/Chief or his/her designated System Administrators to review and either approve or deny the request. Requests made from other law enforcement agencies will be handled by the system administrator themselves, while all requests made from civilians will be sent to a local jurisdiction's legal department for review and input on the request.

# 5. OVERSIGHT

## 5.1 CIMS OVERSIGHT

The CIMS project is overseen and managed by the MBHSR JPOC Committee. The Critical Infrastructure and Key Resources (CIKR) Subcommittee will support the JPOC Committee with recommendations based upon subject matter expertise.

## 5.2 ENSURING TRANSPARENCY AND PROTECTION OF CIVIL LIBERTIES

To ensure transparency and communication with local governments, the Boston Office of Emergency Management will provide an annual report compiled from audits performed by individual jurisdictions. These reports will identify the number of CIMS cameras within a jurisdiction, the number of users on the network and their permission levels, the number of archived video requests that were approved for footage on CIMS cameras, as well as the amount of instances where real-time camera access was granted by a jurisdiction to a requesting agency.

Anyone who engages in an impermissible use of the MBHSR CIMS may be subject to criminal prosecution per M.G.L., civil liability, and/or administrative sanctions, including termination, pursuant to and consistent with the relevant collective bargaining agreements and Department policies.

Violations of this Policy occur when an individual utilizes the MBHSR CIMS network for purposes including but not limited to;

- **Invasion of Privacy.** Except pursuant to a court order, it is a violation of this Policy to observe, or record footage of, locations except those that are in public view from a vantage point that is accessible to the general public and where there is no reasonable expectation of privacy. Areas in which there is a reasonable expectation of privacy include the interior of private premises such as a home.



- **Harassment / Intimidation.** It is a violation of this Policy to use the MBHSR CIMS to harass and/or intimidate any individual or group.
- **Use / Observation Based on a Protected Characteristic.** It is a violation of this Policy to use the MBHSR CIMS to observe individuals solely because of their race, gender, ethnicity, sexual orientation, disability or other classification protected by law.
- **Personal Use.** It is a violation of this Policy to use the CIMS for any personal purpose.
- **First Amendment Rights.** It is a violation of this Policy to use the MBHSR CIMS for the purpose of infringing upon First Amendment rights.

## 6. ADMINISTRATOR

### 6.1 POLICY APPROVAL

The MBHSR CIMS Policy is effective upon approval from the MBHSR Jurisdictional Points of Contact (JPOCs). Boston Office of Emergency Management (OEM) shall maintain the official copy of the approved policy.

### 6.2 POLICY MAINTENANCE

Under the direction and oversight of the Boston Office of Emergency Management (OEM), the JPOC Committee shall be responsible for the revision, update, and distribution of the MBHSR CIMS Policy. The JPOC Committee will ensure that the Policy is reviewed on an annual basis, at a minimum, so that it remains current and operative.