ATTACHMENT 6
Table of Contents

1. Introduction 3
2. Staffing and Organizational Structure 11
3. Planning and Direction 13
4. Collection 16
5. Processing and Collation 23
6. Analysis and Production 29
7. Dissemination 32
8. Review and Reevaluation 36
9. Commonwealth Fusion Center Security 39
10. Commonwealth Fusion Center Databases and Data Sources 47
Chapter 1

Introduction

The Fusion Concept

Law enforcement has always been aware of the key role that information and intelligence play in prevention and response. Although it is impossible to protect every potential target from every conceivable method of attack, there are a number of strategies that can be implemented to maximize this ability. In addition, further refinement in the intelligence and information sharing arena will maximize the ability to respond quickly and efficiently if an incident occurs.\footnote{Global Justice Information Sharing Initiative (2005) Fusion Center Guidelines Developing and Sharing Information and Intelligence in a New World: Guidelines for Establishing and Operating Fusion Centers at the Local, State, Tribal and Federal Level.}

Effective terrorism-related detection, prevention, intelligence analysis, information sharing, preparedness, and response depend on timely and accurate information about the enemy, their ideology, operations, support mechanisms, structure, targets, and attack methods. This information should serve as a guide for efforts to\footnote{Ibid}:

- rapidly identify both immediate and long-term threats;
- identify persons involved in terrorism-related and criminal activities; and
- guide the implementation of information-driven and risk-based prevention, response, and consequence management efforts.

Fusion in this context refers to the overarching process of managing the flow of information and intelligence across levels and sectors of government. The fusion concept supports the development of intelligence-led policing and the implementation of risk-based, information-driven prevention, response, and consequence management programs. Data fusion blends data from different sources including law enforcement, public safety, and the private sector, resulting in meaningful and actionable intelligence and information. The fusion process turns information and intelligence into knowledge. The primary emphasis of fusion is to identify emerging terrorism-related threats and risks, as well as to support ongoing efforts to address criminal activities. It is anticipated that the fusion process will\footnote{Ibid}:

- Allow local and state entities to better forecast and identify emerging crime, public health, and quality of life trends.
- Support multidisciplinary, proactive, risk-based, and community-focused problem solving activities.
- Provide a continuous flow of information and intelligence to officials to assist in developing a depiction of evolving threats.
- Improve the delivery of emergency and non-emergency services.
Moving from a functional model to a working implementation in a real environment involves a number of design considerations, including what information sources to use, what fusion architecture to employ, and communication protocols.

For purposes of this initiative, the following steps are offered as a foundation to illustrate the fusion process: data input, data merging, correlation and association, data extraction, deconfliction, data refinement based on system results/user query, human analysis, and dissemination. Information and intelligence should be validated as to credibility and reliability. Commonwealth Fusion Center (CFC) personnel will utilize fused and analyzed information to provide value-added intelligence products that support the development of performance-driven, risk-based prevention, response, and consequence management programs.

To illustrate the fusion process within a conceptualized fusion center model, Figure 1 depicts a distributed capability, populated by multiple and diverse data sources. Data is blended or “fused.” Users access the data via a common interface, extracting, analyzing, and disseminating information based on need and current demands. Although it is anticipated that fusion centers will primarily be used for preventive and proactive measures, the process will also be critical if an incident occurs, providing information to responders as well as officials, media, and citizens.

Fusion Process

---

4 Global Justice Information Sharing Initiative (2005) Fusion Center Guidelines Developing and Sharing Information and Intelligence in a New World: Guidelines for Establishing and Operating Fusion Centers at the Local, State, Tribal and Federal Level
Terrorism-related intelligence is derived by collecting, blending, analyzing, and evaluating relevant information from a broad array of sources on a continual basis. There is no single source for terrorism-related information. It can come through the efforts of the intelligence community; Federal, State, tribal, and local law enforcement authorities; other government agencies (e.g., fire services, transportation, healthcare, general government), and the private sector (e.g., energy, transportation, healthcare, financial, Internet/information technology). In Massachusetts, there are a substantial number of criminal justice and public safety databases and data sources, many of which are not integrated across agencies. The Commonwealth Fusion Center is a significant effort to identify those sources and maximize their utility for our counterterrorism goals.

The Commonwealth Fusion Center Operations Manual describes goals, objectives, and the general operating environment for information sharing and intelligence analysis in Massachusetts. The Operations Manual further identifies and delineates the roles, tasks, and responsibilities necessary in each segment of the intelligence cycle.

The Fusion Center has established a set of standard operating procedures that explain information sharing and intelligence gathering processes. These operating procedures are necessary to achieve policy goals and objectives. That is, establish plans to gather information from all sources, formal and informal, conduct analysis deriving pertinent information in order to document and share with those in law enforcement requiring such products on identified law enforcement targets.

For agency information to be useful requires utilizing and evaluating specific guidelines and procedures on a daily basis. A distinction and understanding between general record information and intelligence file products are delineated in the following sections. This is necessary to mitigate misunderstanding between the two areas and their effective utilization.

Both the general records and the intelligence systems require exacting controls relating to input, processing, storage, retrieval, purging, dissemination, and security. The latter part of this manual addresses these issues which are key components of a strong administrative and monitoring data system.
Definitions$^5$


28 Part 23 contains implementing standards for operating federally grant-funded multi-jurisdictional criminal intelligence systems. It specifically provides guidance in five primary areas: submission and entry of criminal intelligence information, security, inquiry, dissemination, and review-and-purge process.

Account
An area of specialization in which analysts have subject matter expertise such as crime types, critical infrastructure sectors and or criminal or terrorist groups.

Actionable Intelligence (see Tactical Intelligence)

Analysis
Analysis is the review of information and its comparison to other information to determine the meaning of the data in reference to a criminal investigation or assessment. That activity whereby meaning, actual or suggested, is derived through organizing and systematically examining diverse information and applying inductive or deductive logic for the purposes of criminal investigation or assessment.

Asset
An asset is a taskable collector of intelligence. Assets include informants, police officers, police agencies, public safety agencies, analytical units (in their collection role), private sector partners and public information systems. Assets may include anonymous callers, police officers from other agencies, other agency personnel, etc.

Criminal Information Section (CIS)
The State Police Criminal Information Section is the statutorily-designated intelligence collection authority for crime information in the Commonwealth.

Commonwealth Fusion Center (CFC)
The Commonwealth Fusion Center is the information sharing and intelligence gathering hub for the Commonwealth designated through executive-mandate.

Criminal Information
Raw data as it pertains to criminal activity.

Criminal Intelligence
Information collection and analysis process conducted to support the anticipated need for decision making and action.

---

Collection
The process which involves the identification, gathering, and documentation of actual or planned criminal or terrorist activity, as well as information about those suspected of involvement in the criminal or terrorist activity.

Collection Management
The process of converting intelligence needs into collection or intelligence production requirements, establishing priorities, tasking or coordination, monitoring status and re-tasking as required.

Collection Plan
A plan that directs the collection of data on a particular topic with a specific objective, a list of potential sources of that data, and an estimated time frame.

Commonwealth Fusion Center Information Management System (CFC-IMS)
The IMS will be the primary CFC electronic database to record and store information having potential intelligence value. It will be available to all Massachusetts law enforcement agencies.

Dissemination
Dissemination is the distribution of information and intelligence in accordance with governing rules and laws.

Emergency Support Function - 18 (ESF-18)
The Massachusetts Emergency Management Agency (MEMA) has eighteen emergency support functions in place. ESF-18 is the Business and Industry Emergency Support Function that coordinates the emergency activities of private sector owner/operators and organizations in support of disaster efforts in the Commonwealth.

Essential Elements of Information
These are the bits of information (who, what, where, why and how) required by analysts and investigators to be able to answer an intelligence collection requirement.

General Records
Include arrest records, crime reports, booking forms, personnel records, communications, and all other documents flowing in and out of Department of State Police information channels.

Informant
An individual who agrees to provide information or perform tasks in lieu of prosecution for criminal offenses or as a result of a plea bargain; who agrees to provide information or perform services in the furtherance of a criminal investigation which could result in monetary payment; or a civic minded, non-criminal individual who provides information, but prefers not to testify in court, and wishes to remain anonymous.

Information
Unevaluated and untested facts and data obtained from observations, comments, reports, and pictures regarding people, places, things, and events, as a prelude to a decision or action by law enforcement, managers, or policy makers.
Intelligence
The product of systematic gathering, evaluation, and synthesis of raw data on individuals or activities suspected of being, or known to be, criminal in nature.

Intelligence Collection
The gathering of information, through approved methods, to satisfy intelligence collection requirements, goals, and gaps.

Intelligence Collection Requirement
The document that identifies a specific target for collection efforts and includes all the Essential Elements of Information needed for collection.

Intelligence Gap
Unknown information or assets about a target or priority information/intelligence requirement.

Intelligence-Led Policing
The collection and analysis of information to produce an intelligence end product designed to inform police decision-making at both the tactical and strategic levels.

Need to Know
The requirement that the information requested is both pertinent and necessary for the requesting individual or agency to initiate, further, or complete an assigned law enforcement task.

Open Source Information and Intelligence
Open source information is any type of lawfully and ethically obtainable information that describes persons, locations, groups, events, or trends.

Operation
The planned police activity which involves the direct or indirect contact with the subjects of an investigation. Examples are tactical operations, search warrants, warrant sweeps, routine license inspections, roadblocks, or raids.

Operational Intelligence
Information which is evaluated and systematically organized on an active or potential target including individuals, organizations, or specific crimes.

Priority Information / Intelligence Requirements (PIIR)
The details of what an end-user needs from the intelligence function in broad terms.

Reasonable Suspicion
Established when information exists which provides sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.

Right to Know
Requestor has official capacity and statutory authority to the information being sought.
SCIF (Sensitive Compartmented Information Facility)—An accredited area, room, group of rooms, buildings, or an installation where SCI may be stored, used, discussed, and/or processed.

Source
The originator of information. The source of the information should be contacted to confirm veracity prior to using the information for intelligence or operational purposes.

Strategic Intelligence
Information on patterns and trends which are collected, evaluated, and analyzed for resource management and policy planning.

Tactical Intelligence
Evaluated information on which short term enforcement action can be based. Also may be referred to as actionable intelligence.

Target
The identity of a specific individual(s) or group(s), location(s) or event(s) that is suspected of involvement in or planning criminal activity.

Task
An intelligence collection requirement becomes a task when levied on a bureau or squad for action.

Threat Assessment
A report that looks at a criminal group or criminal activity and assesses the threat that activity or group poses to a jurisdiction, either at present or in the future, and recommends ways to lessen the threat.

Vulnerability Assessment
A report that looks at an individual, location, or event and assesses the vulnerability of that individual, location, or event to a criminal act and recommends ways to lessen or eliminate the vulnerability.

Watch Officer
The function of the Watch Officer is to provide real-time support and information services, maintain situational awareness at all times, make appropriate log entries, and issue alerts as required by policy.
The Intelligence Process

The intelligence process involves the following series of steps which ensures a professional and dynamic approach to identify and counter threats utilizing intelligence assets and functions. The process must be objective, unbiased and without prejudice. It must be based on accurate and relevant facts with due consideration for the privacy and constitutional rights of individuals, groups and organizations.

- Planning and Direction
- Collection
- Processing and Collation
- Analysis and Production
- Dissemination
- Feedback/Reevaluation

Intelligence Cycle

---

Chapter 2

Staffing and Organizational Structure

SWORN OFFICER PERSONNEL FUNCTIONS

The Director of the Commonwealth Fusion Center (CFC) shall be directly responsible to the Colonel/Superintendent of the Massachusetts State Police (MSP). The Director will be responsible for the proper and efficient administration of personnel assigned to the CFC. This officer will be the point of contact for other intelligence/fusion centers. The Director, or his official designee, can initiate strategic intelligence studies of major public safety problems (crime, disorder, public health, social service and other emerging problems) affecting the Commonwealth of Massachusetts.

The Executive Officer of the Commonwealth Fusion Center shall be directly responsible to the Director of the Commonwealth Fusion Center. The Executive Officer will function in the role of Director when so designated. The Executive Officer will be responsible for coordinating the activities of both the Commanding Officers of the Analytical Section and the Investigative Section. The Executive Officer shall be responsible for the logistical needs of the CFC. This officer will also be responsible for ensuring that the procedures as contained in Policy guidelines are properly adhered to.

The Commanding Officer of the Anti-Terrorism Unit shall be directly responsible to the Executive Officer. This officer will be responsible for the direct supervision of the investigative personnel under their command. In this role, s/he will insure that proper investigative procedures are followed and that only information allowed by law is collected. This officer will be responsible for the facilitation and collection of raw data for submission to the CFC from other law enforcement agencies. This officer will ensure investigators adhere to the policies and procedures, and rules and regulations of the MSP, as well as the CFC.

The Commanding Officer of the Analytical Unit shall be directly responsible to the Executive Officer. This officer will be responsible for the direct supervision of all the analytical personnel under their command. In this role, s/he will insure that the activities of the section strictly adhere to all relevant federal, state, and constitutional restrictions. This officer will insure that the privacy rights of citizens are not violated in the normal course of the section's analytical activities. This officer will be responsible for ensuring that analytical personnel adhere to all policies and procedures, and rules and regulations of the MSP, as well as the CFC.

Intelligence Officers / Investigators shall be directly responsible to sworn supervisors within the Anti-Terrorism Unit. Officers will be responsible for collecting intelligence, conducting investigations that have a nexus to terrorism and conducting homeland security-related objectives as issued. Investigators will also conduct threat and vulnerability assessments and other critical infrastructure protection functions as needed.
NON-SWORN PERSONNEL – DUTIES

Intelligence Analysts (Research Analyst I & II) will be responsible for understanding the criminal intelligence process, intelligence-led policing, and their roles in enhancing public safety. Analysts will understand the importance of the National Criminal Intelligence Sharing Plan, the Global Justice Fusion Center Standards, and other nationally recognized best business practices. Analysts will perform research on assigned criminal and terrorist related accounts, as well as support the critical infrastructure protection programs through interactions with subject matter experts in assigned sectors. Analysts will become familiar with the range of data sources used in their assigned areas for information sharing and intelligence gathering.

Analysts will gain an understanding of the proper handling of criminal intelligence information, including file management and information evaluation. They will be responsible for the development of intelligence products using critical thinking, logic, inference and recommendations development. CFC analysts will be familiar with legal, privacy, and ethical issues related to information sharing and intelligence gathering. Analysts will adhere to all CFC policy and procedures, as well as applicable state and federal regulations and laws.

Senior Intelligence Analysts (Research Analyst III) will be responsible for understanding the criminal intelligence process and intelligence-led policing, and their roles in enhancing public safety. Analysts will understand the importance of the National Criminal Intelligence Sharing Plan, the Global Justice Fusion Center Standards and other nationally recognized best business practices. Analysts will perform research on assigned criminal and terrorist related accounts, as well as support the critical infrastructure protection through interactions with subject matter experts in assigned sectors. Analysts will become familiar with the range of data sources used in their assigned areas for information sharing and intelligence gathering.

Senior analysts will manage CFC projects, develop project proposals, grants, and implementation plans and will be responsible for the Intelligence Analysts assigned to their respective tasks. They will be responsible for advising the Command Staff, the Executive Office of Public Safety, the Homeland Security Advisor, Homeland Security Regional Councils and other state policy makers on information sharing and intelligence processes. They will assist CFC stakeholders with the ongoing development of the CFC’s information sharing and intelligence capacity. They report directly to the Analytical Unit Commander (AUC).

The Security/Compliance Officer shall be directly responsible to the AUC. This officer will be responsible for compliance with information access policies, submission criteria, file maintenance and data and intelligence file audits. S/he will ensure that all Federal, state and local laws regarding privacy, security, and criminal intelligence systems are adhered to by participating agencies and individuals. This position will ensure that the CFC complies with 28 CFR part 23 Criminal Intelligence Systems and the Fair Information Practices including collection limitation, data quality, limited disclosure, and security safeguards.
Chapter 3
Planning & Direction

PLANNING AND DIRECTION

The intelligence cycle guides the Commonwealth Fusion Center and its public and private partners. During the planning process, these core stakeholders present general intelligence requirements. The CFC will then develop and prioritize collection requirements to support those objectives. Those requirements will be referred to appropriate agencies/entities.

Collection management planning is an ongoing process. Analysis and effective coordination among all stakeholders ensures that the CFC will achieve its desired mission, goals and objectives. The planning should attempt to identify and task other public safety and private partner assets to provide accurate, reliable data, and ensure overlapping coverage and verification of information.

CFC planning and direction activities include:

- Conduct and update comprehensive risk, threat, and vulnerability assessments.
- Identify patterns and trends reflective of emerging threats.
- Define collection requirements based on results of risk assessments.
- Identify the circumstances or events (crime, public health) that represent indicators and/or precursors of threats.
- Identify the sources and/or repositories of data and information regarding indicators and precursors.
- Identify the existing capacity to collect key information from existing sources.
- Identify collection gaps and mitigate them.

COLLECTION MANAGEMENT STRUCTURE

Commonwealth Fusion Center Advisory Council

The Commonwealth Fusion Center Advisory Council, in conjunction with the CFC leadership team, will provide leadership on collection management goals. The CFC Director will draft recommended collection requirements and meet with core stakeholders and public safety partners to discuss priority information/intelligence requirements (PIIR) and essential elements of information to determine the collection requirements. The deliverables from these meetings will include an updated collection plan and priority information/intelligence requirements, essential elements of information and supplemental guidance documents for field collection efforts. The core stakeholders will meet on a quarterly or biannual basis to continuously assess the viability of these collection requirements.

---

8 The composition of the Council is determined by the Executive Office of Public Safety

This document is exempted from Public Disclosure under M.G.L. chapter 4 §7, clause 26 (n)
This Advisory Council ensures that collection management occurs within the intelligence and operations cycles. The Council can establish responsibility for priority areas of interest and provide leadership for collection efforts outside the structure of the CFC. It can lead collection efforts across the range of state and local police agencies, public safety agencies, and private sector partners.

The Advisory Council, in conjunction with CFC leadership, will determine new tactical and strategic requirements and the need to prepare a new or updated PIIR to meet the current threat. They will examine the validity and necessity of current intelligence collection requirements.

**Intelligence Services Management**

The Analytic Unit Commander (AUC) is responsible for the research and analytical support to investigators and intelligence representatives of public safety agencies. The research function assists in collecting data from databases and data sources to answer intelligence collection requirements. The analytical function is the focus point for all information relating to an intelligence collection requirement. This function analyzes all information and prepares tactical and strategic intelligence briefings, and along with supervisory personnel, prepares and disseminates specific bulletins (officer safety, intelligence, criminal information, crime analysis, and requests for information, etc.) The CFC intelligence analyst will normally be the in-house subject matter expert on a specific issue or target. The AUC and intelligence analyst supervisors monitor entry of information into the Information Management System (IMS), Homeland Security Information Network (HSIN) and other CFC data applications from various intelligence and investigative units and other public safety partners. The CFC is the center for intelligence collection management in the Commonwealth and provides leadership by establishing collections requirements and monitoring subsequent collection efforts on assigned requirements.

One aspect of this leadership will be ongoing efforts to conduct outreach to the five regional homeland security councils, the major cities and our private sector associates. The CFC plans to establish focus groups with public safety organizations through the homeland security councils and major cities to review intelligence collection requirements prior to issuance. We strive to achieve buy-in across the wide spectrum of public safety agencies in order to mitigate traditional barriers to information and intelligence collection.

As part of our Private – Public Sector partnership (ESF-18), we plan to review collection requirements aimed at private sector security professionals. The attached collection requirements for critical infrastructure sectors, contained in the current plan, represent one form of information outreach to private partners. By harnessing the capacity of private sector partners, the CFC can greatly enhance its network of information sources that will highlight any potential nexus to terrorism crimes, pre-attack planning, and surveillance.
PRIORITY INFORMATION
INTELLIGENCE REQUIREMENTS
FLOWCHART

FBI/DHS
Priority Information
Intelligence Requirements
(PIIR)

Commonwealth Fusion Center
Priority Information
Intelligence Requirements
(PIIR)

Homeland Security
Regions
Priority Information
Intelligence Requirements
(PIIR)
Chapter 4

Collection Process

INTELLIGENCE INFORMATION

Collection

Collection is the gathering of raw information based on the information requirements needed to produce intelligence products. The collection process involves the identification, gathering, and documentation of actual or planned criminal or terrorist activity, as well as information about those suspected of involvement in the criminal or terrorist activity.

Information is gathered from all possible sources, according to the requirements of a particular project or mission. Data can be collected from a variety of sources including investigative files, public records, field interviews, tip lines, incident reports, periodicals, confidential sources, and the Internet. All legal and ethical sources will be used to further the public safety goals of the Commonwealth.

CFC collection activities include:

- Communicating collection requirements to relevant state, local, and private-sector partners.
- Implementing situational awareness activities such as training and public education.
- Mitigating impediments to collection.
- Compiling classified and unclassified data, information, and intelligence generated by people and organizations.
- Serving as the 24/7 initial point of contact for information provided by the U.S. Department of Homeland Security, Department of Defense, Department of Justice, FBI, and other Federal entities (via telephone calls, HSIN, LEO, e-mail bulletins, VTC and Fax) for the receipt of the following classified and unclassified:
  - Immediate threat-specific information
  - Long-term threat information
  - Terrorist tactics and methods
- Integrating with other reporting systems such as 911 and 311, and, in conjunction with the Joint Terrorism Task Force, establishing and maintaining easy-to-use methods for the public reporting of suspicious activity using:
  - Internet
  - Toll-free tip line
- Establishing a process to identify and track reports of suspicious circumstances indicating pre-operational surveillance, acquisition of items used in an attack or false documentation.

Collection Assets and Resources

The CFC is a multi-jurisdictional, multi-disciplinary intelligence center that focuses on terrorism, as well as intelligence-led policing and takes an all-crimes approach. It strives to maximize the public safety and private sector partnerships that exist to build new relationships with organizations that share its mission of information sharing and intelligence analysis.

Among the many resources that exist are the thousands of first responders across the police, fire, emergency management, and emergency medical services disciplines. Further, there are thousands of private sector employees that can contribute to the public safety community effort’s to monitor critical infrastructure in Massachusetts.

The CFC will leverage technology to support its mission. Through the development of a formalized information and intelligence gathering system within public safety, the CFC can task first responders with collecting relevant information and sharing that information with its partners. Police intelligence liaison officers will have the ability to directly enter and access criminal intelligence as needed to support their individual agency’s missions through the CFC’s Information Management System via COPLINK.

Information collection and sharing will be further enhanced through the use of DHS’s Homeland Security Information System Massachusetts (HSIN-MA). HSIN-MA will be the core of information sharing among Massachusetts’ public safety agencies and their private sector partners. HSIN-MA is a secure website designed to facilitate the sharing of information among local, regional, state, and federal agencies.

Existing Data Sources

Another objective is the identification of existing data sources and databases that can inform strategic and tactical decision makers regarding existing or potential crime and terrorism issues. Massachusetts public safety agencies have a range of existing data sources such as Computer Aided Dispatch/Records Management Systems (CAD/RMS), automated booking systems, investigative case management systems, hazardous materials databases, and incident reporting systems. Partner agencies such as the Department of Public Health have collection efforts such as the Weapons Related Injury Surveillance System (WRISS) and Emergency Room admissions data that also can provide indicators of terrorist or criminal events. Through the assessment of each data source, the CFC can identify critical information streams that will assist in the detection and prevention of criminal and terrorist acts. The challenge will be to examine these data sources, assist with improvements that support the homeland security mission, and establish protocols to access this information in support of the fusion process.

Taking advantage of citizen awareness can be accomplished through use of the Commonwealth Fusion Center Terrorism Tip line, our Public Safety Access Points (PSAP), State Police cellular 911 technologies, and police and other public safety call centers throughout the state.
INFORMATION SOURCES

All information sources will be utilized within legal statutes, ethical standards, best business practices, and CFC policy & procedure requirements. Information from a variety of sources will be needed to combat terrorism and criminal activity in Massachusetts. The CFC collects information pertinent to crime, terrorism, and quality of life issues, and processes information into intelligence for use by law enforcement, regulatory, public health and safety, and security personnel. The CFC will make every effort to collect information from all available legitimate sources which will help to achieve CFC goals.

Open Source Information and Intelligence

Open source information is any type of lawfully and ethically obtainable information that describes persons, locations, groups, events, or trends. Open source information is overt and public and includes the following:

- All types of media
- Public data sources and databases
- Directories
- Open discussions such as bulletin boards, forums, online discussions, classes, seminars or presentations
- Government documents and publications
- Scientific and academic research, treatises or reports
- Statistical databases and sources
- Commercial information vendors
- Public and commercial websites
- Search engines of Internet content

Reasonable Suspicion Standard

The CFC will use the reasonable suspicion standard to guide intelligence collection activities. That is, information collectors must have sufficient facts to give a trained law enforcement officer, investigator, or analyst a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise in order to collect and process that information.

Target Identification

Targets of intelligence information collection and/or investigative actions will be identified by a reasonable suspicion standard associated with a criminal organization or criminal activity.

Intelligence information collection and/or investigations will not be based upon a person, organizations, religious, cultural, or political affiliation where there is no reasonable suspicion of criminal activity.
Legal Requirements

The intelligence information collection process will be conducted according to applicable federal and state statutes. The controlling federal mandate, Criminal Intelligence Systems, 28 CFR part 23, as well as state public records laws, impact the information sharing and intelligence process. All applicable information gathering policies and procedures of the CFC will also apply.

If there is a legal question regarding information sharing or intelligence gathering, the CFC will consult the State Police Legal Counsel and/or Office of the Attorney General as circumstances dictate.

Collection Management Planning

All investigative methods will be utilized to collect criminal intelligence information. This will include the use of technology, physical resources, and human assets. The utilization of investigative collection methods will be governed by appropriate federal and state statutes and applicable policy & procedures.

Collection management planning is an ongoing process. Analysis and effective coordination among all public safety partners ensures that the CFC’s intelligence analytical support function can achieve its desired mission, goals and objectives. Collection planning will identify and task public safety and private sector assets to provide accurate, reliable data, and will strive to ensure overlapping coverage and verification of information.

[Diagram of Information Collection Planning Cycle]

This document is exempted from Public Disclosure under M.G.L. chapter 4 §7, clause 26 (n)
Threat, Vulnerability and Risk Assessment and Trends Analysis

The first stage of collection management planning entails developing a risk-based information gathering strategy. The CFC will conduct and continuously update a comprehensive and compatible risk assessment involving aspects of threat, vulnerability, and consequence. These assessments will identify patterns and trends reflective of emerging threats throughout the state. The CFC will assume a leadership role in defining the collection requirements based on the results of risk assessments conducted on critical infrastructure and high profile events throughout the Commonwealth.

In addition, the CFC will work with public safety partners to identify the circumstances or events such as crime, suspicious activity, or public health incidents that represent indicators and/or precursors of threats. This information, in addition to information provided by national threat, vulnerability, and risk assessments, form the basis for the Fusion Center's Priority Information and Intelligence Requirements (PIIR).

Priority Information and Intelligence Requirements Development

The CFC will develop PIIRs by using a 360 degree development process, involving national, state, and local policymakers, public safety practitioners, and private sector partners. The CFC’s intent is to undertake a general assessment based upon threat, vulnerability, and risk assessments conducted in a number of areas, and generated at the national level through federal information and intelligence gathering agencies such as the Department of Homeland Security (DHS) and the FBI. Utilizing their PIIRs will provide a nationally-recognized benchmark for the development of statewide requirements.

From that assessment, the CFC will examine information collection requirements generated from executive level public safety officials from the various disciplines. For instance, Massachusetts Police Chiefs identified street gangs as a significant public safety issue, which required a shift in information collection activities.

This process will be further enhanced by reviewing the collection needs of officers and investigators at the practitioner level. First responders working in certain jurisdictions each day have not only gathered a great deal of valuable information, but have also identified information gaps and barriers that the CFC can help address. These street level intelligence gatherers offer a different perspective for the development of information and intelligence requirements.

Finally, the CFC will leverage the knowledge and experience of our private sector partners to glean information from the various critical infrastructure sectors that they represent. The private sector represents a substantial untapped resource, therefore Massachusetts policy makers and CFC officials will use existing partnerships as a path to share information and gather additional data.

DATA SOURCE IDENTIFICATION

Once Fusion Center PIIRs have been developed, the next step is to identify existing data sources to address these information needs. The goal of this phase is to identify the sources and/or repositories of data and information regarding indicators and precursors to criminal or terrorist events. Data sources could include, among others, agency records management systems, investigative reports, licensing data, emergency room admission records, and trial transcripts.
Agency and Information Source

One challenge that confronts collection planning is the identification of agencies and information sources that routinely collect information that can be of value in the identification of crime and terrorist threats. There are a number of agencies, such as the Department of Fire Services and the Department of Public Health, that collect relevant information as part of their mission. In the past, these sources may have been overlooked. As our partnerships expand, the Fusion Center will identify additional information sources to accomplish our intelligence-led policing mission.

Counterterrorism and Public Safety Awareness Training

A key element of gathering information and intelligence to accomplish the CFC’s homeland security and intelligence-led policing goals is to improve the awareness of public safety information gatherers through continuous education and training. In order to connect the dots, public safety officers must understand the dots. Development of public safety awareness training that outlines pre-attack planning, terrorism indicators, precursor chemicals for improvised explosive devices, or other weapons of mass destruction, as well as identification of crimes that have a nexus to terrorism, will greatly augment public safety data gathering.

Legal / Privacy / Civil Liberties / Technical Requirements Review

Once data sources have been identified, the CFC and its partner agencies must assess the legal, privacy and civil liberties issues surrounding the collection of certain data. In some cases, certain public and private organizations are legally prohibited from passing information to public safety agencies.

In other cases, the collection of information from certain data sources is limited due to technical barriers. Various agencies have data in isolated, stand-alone databases or in some cases in paper records. An analysis of these limitations will assist the CFC in developing recommendations for data enhancement and data source improvement.

Priority Information and Intelligence Requirements Dissemination

As the CFC matures, the methods to disseminate PIIRs will evolve as well. The CFC will rely primarily upon the Homeland Security Information System-Massachusetts (HSIN-MA) secure website to publish PIIRs to a wide audience. Using HSIN-MA provides an opportunity to meet our mutual goals of information sharing with key leaders and planners at all levels of government while also reaching out to interact and share information with our private sector critical infrastructure partners. This website can assure secure dissemination to a key group of public safety decision makers, as well as intelligence and access officers in various agencies.

The development of an information sharing working group at the state level will also serve as a vehicle to disseminate information requirements. The working group consisting of Fusion Center staff, the State Police, regional homeland security councils, the Massachusetts Chiefs of Police Association, the Major City Chiefs Association, and the Massachusetts Fire Chiefs Association will assist in the dissemination of requirements. This working group can provide a realistic state and local perspective on information gathering and sharing which will enlighten Fusion Center decision makers.
Feedback and Reevaluation

As information is received, processed, and analyzed, it must be critiqued to assure that collection and other operational requirements are being met. The intelligence cycle is not complete until a review of the information or intelligence product is completed, ensuring the requesting consumer has received it, and, importantly, verifying that the consumer feels the requirement has been met. If the requirements have not been met, the process must be restarted to target new assets and collection requirements.

One aspect of this final stage is to update threat, vulnerability, and consequence assessments so as to stay apprised of the current risk environment facing the Commonwealth. Terrorists in particular are highly adaptive; therefore it becomes important to continually reexamine the threats posed to various critical infrastructure sectors.

Another portion of this feedback stage is to assess the effectiveness of national intelligence and information collection requirements which the CFC receives from the FBI and DHS.

The collection management planning process must be a dynamic one in order to meet the changing nature of crime and terrorism. Through the development of ongoing working relationships with all interested public safety partners, the CFC can gather relevant and timely information and intelligence to accomplish the Commonwealth's public safety goals. Maximizing the resources of the CFC, the State Police, the regional homeland security councils, federal, state and local public safety agencies will improve the readiness posture as we move forward.
Chapter 5
Processing and Collation

PROCESSING AND COLLATION

Processing and Collation involves converting the vast amount of information collected into a form usable by analysts. This involves sorting, combining, categorizing, and arranging data in a manner which assists in determining relationships and patterns. Processing includes the entering of raw data into databases where it can be used in the analysis process. The goal is to ensure timely processing to present a complete picture of the emerging threat situation to investigative or operational units, as well as key government officials.

CFC processing and collation activities include:

- The integration and quality control of data from disparate sources.
- The development of new data sources to fill in information gaps.
- The classification of information and intelligence data.

Data Integration

Criminal justice data has only recently begun to be standardized across diverse agencies. More often, data from disparate sources must be integrated and or modified to a format that is usable for analytical purposes. In some cases, data fields must be recoded to enable analysts to conduct research and associate like data from different data sources.

Data Quality Control

Criminal justice data is of varying quality, therefore it is extremely important to assure quality control before analysis takes place. Implementing a process of that includes error checking, checks for missing data, and the standardization of data elements will enhance the value of this data for analytical purposes. The CFC will strive to ensure that its data sources contain complete, accurate, and verifiable information.

Data Source Development

New data sources will be created on the fly to address an information and intelligence gap. For example, the CFC may develop a lead tracking database for a specific investigation to record the influx of calls received through its tip line. While our preference is to utilize existing data sources when feasible, new databases will be needed to accomplish our goals and objectives.

When these situations occur, the CFC will leverage existing Global Justice XML Data Model (GJXDM) standards to assure seamless data integration and information exchange. The GJXDM is a nationally recognized data standard for public safety and homeland security agencies, and will greatly enhance data source development. It is a universal translation language that enables disparate databases to interact.
Information Evaluation

In order to utilize and act upon information received through various sources, it is critical to evaluate not only the information, but also the source as to its reliability and validity.

<table>
<thead>
<tr>
<th>Source Reliability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reliable</td>
</tr>
<tr>
<td>Usually reliable</td>
</tr>
<tr>
<td>Unreliable</td>
</tr>
<tr>
<td>Unknown</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Content Validity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confirmed</td>
</tr>
<tr>
<td>Probable</td>
</tr>
<tr>
<td>Doubtful</td>
</tr>
<tr>
<td>Cannot be judged</td>
</tr>
</tbody>
</table>

Information Classification Guidelines

All intelligence products to be disseminated from the CFC must be labeled with a classification in the footer of the document. The Security Chapter outlines the federally recognized intelligence classifications in detail. The majority of CFC products will be of the Unclassified and Sensitive But Unclassified nature. Within the Sensitive But Unclassified classification are subsets such as For Official Use Only and Law Enforcement Sensitive.

**Unclassified:** Information and intelligence contained is not of a sensitive nature. Information was collected from open source documentation, and methods of collection and corroboration are not sensitive. Dissemination is not restricted.

**Sensitive but Unclassified:** Information and intelligence is of a sensitive nature. Information was collected from law enforcement or other restricted access sources. Methods of collection and corroboration, as well as recommendations therein, may be sensitive. Dissemination is limited to those with a need to know, right to know.

**Law Enforcement Sensitive:** Information and intelligence is for law enforcement use only. Information was collected from law enforcement or other restricted access sources, methods of collection and corroboration, as well as recommendations therein, are considered sensitive. Dissemination is limited to law enforcement entities with a need to know, right to know.

Any questions on these classifications should be directed to Fusion Center supervisors or commanders.
SUBMISSIONS & REQUESTS

Submissions and requests to the CFC may be made by:

1. Authorized law enforcement agencies at the federal, state and municipal levels that agree to comply with rules, regulations, policies and procedures as set forth in the memorandum of understanding (MOU) signed by the individual agencies wishing to participate in the CFC.

2. Public and Private sector entities associated with critical infrastructure environments at the federal, state, and municipal levels that agree to comply with rules, regulations, policies and procedures as set forth in the memorandum of understanding (MOU) signed by the individual agencies wishing to participate in the CFC.

3. Individual citizens wishing to provide information or needing to request information may do so according to pertinent Massachusetts law and/or CFC guidelines.

Submissions and requests to the CFC may be made via telephone, HSIN-MA, in person, U.S. mail, computer disk or tape, e-mail, and Information Management System (IMS) – COPLINK.

Law Enforcement Agency Submission Requirements

The following information fields are required of the submitting agency when submitting information to the CFC, regardless of submission method.

1.) Full name, rank, ID, and telephone number of submitting officer
2.) Submitting agency name
3.) Submitting agency case number
4.) Type of criminal activity
5.) Source Reliability
6.) Content validity
7.) Dissemination code
8.) Primary subject information:
   a) Subject name plus two identifiers (DOB, SSN, address, physical description, etc.)
   b) Organization/Gang name (if applicable)
   c) Location (if available)
   d) Vehicle (if available)
   e) Telephone/s (if available)
   f) Email (if available)
   g) Weapon/s (if available)
CFC Personnel Submission Procedures

The following procedures will be adhered to when information is being submitted by law enforcement entities, except if through the IMS.

The Watch Officer will:

1.) Date and time stamp when information received
2.) Verify all required data fields as described in Submission Procedure for LE Agencies is complete
3.) Verify access officer information and CFC PIN#
4.) If submission made in person, complete visitor log listing:
   a) Date, time in, name, agency, purpose, time out

CRIMINAL INTELLIGENCE FILES

A criminal intelligence file consists of stored information on the activities and associations of:

A. Individuals where:

1. There is reasonable suspicion of being or of having been involved in the actual or attempted planning, organizing, financing, or commission of criminal acts; or

2. There is reasonable suspicion of being or of having been involved in criminal activities with known or suspected crime figures.

B. Organizations, businesses, and groups where:

1. There is reasonable suspicion of being or of having been involved in the actual or attempted planning, organizing, financing, or commission of criminal acts; or

2. There is reasonable suspicion of being or of having been illegally operated, controlled, financed, or infiltrated by known or suspected crime figures.

Information Evaluation

Information to be stored in a CFC criminal intelligence system such as the IMS or Hsin-MA must first undergo review for relevancy and an evaluation for source reliability and information validity prior to filing. Evaluating information source and content informs future users of the information’s worth and usefulness.
File Content

Only information that meets the CFC’s criteria for file input and has a criminal predicate should be stored in the criminal intelligence file.

Exclusions to Criminal Intelligence File

Specifically excluded material includes:

(a) Information on an individual or group merely on the basis:
   - that such individual or group supports unpopular causes.
   - of ethnic background.
   - of religious or political affiliation.
   - of non-criminal personal habits.

(b) Criminal Offender Record Information (CORI). This is because CORI may be subject to specific audit and dissemination restrictions which are designed to protect an individual’s right to privacy and to ensure accuracy.

(c) Associations with individuals that are not of a criminal nature.

File Criteria/Categories

All information to be retained in the criminal intelligence file must meet the stated guidelines for file definition and file content. Information will only be retained in one of three file categories as set forth below:

A. Permanent File:

1. This file includes individuals, groups, businesses, and organizations which have been positively identified by criminal involvement and one or more distinguishing characteristics.

2. The retention period for all documents will be in accordance with Commonwealth of Massachusetts – Secretary of State Guidelines. Information will be evaluated within the specified period for its file acceptability.

3. Modus Operandi File Exclusion: The exception to this rule involves modus operandi (MO) files. MO files describe a unique method of operation for a specific type of crime (homicide, fraud) and may not be immediately linked to an identifiable suspect. MO files may be retained indefinitely while additional identifiers are sought.
B. Temporary File:

1. The temporary file includes individuals, groups, businesses, and organizations whose criminal involvement is questionable and which have not been positively identified by one or more distinguishing characteristics.

2. Individuals, groups, and organizations are given temporary file status only in the following situations:

   a. The subject is unidentifiable because there are no physical descriptors, identification numbers, or distinguishing characteristics available.

   b. The subject's involvement in criminal activities is questionable due to either:

      * Possible associations with a known criminal and appears to be jointly involved in illegal activities

      * The subject has a history of criminal conduct, and the circumstances afford him an opportunity to again become active.

   c. The reliability of the information source and/or the validity of the information content cannot be determined at the time of receipt. However the information appears to be significant and merits temporary storage.

3. The retention period is one year, during which time effort is made to secure additional data verification. If the information still remains in the temporary file at the end of one year with no updated information, and no further information is available, the information is purged and destroyed.

C. Working File:

1. The working file category is the receiving phase of newly acquired raw data. The CFC staff review the new materials for its acceptability to the CFC criminal intelligence system.

2. The retention period for newly received raw data documents is 180 days, during which effort is made to determine the value of raw data and its acceptability to the CFC criminal intelligence system.
Chapter 6

Analysis and Production

ANALYSIS AND PRODUCTION

Analysis and production is the converting of raw information into intelligence. It includes integrating, evaluating, and analyzing available data, and preparing intelligence products. The information's reliability, validity, and relevance is evaluated and weighed. The information is logically integrated, put in context, and used to produce intelligence. This includes both “raw” and “finished” intelligence. Raw intelligence is often referred to as “the dots”. … “Finished” intelligence reports “connect the dots” by putting information in context and drawing conclusions about its implications.

CFC analytical activities include the following:

- Blending data, information, and intelligence received from multiple data sources.
- Reconciling, deconflicting, and validating the credibility of data, information, and intelligence received from collection sources.
- Evaluating and analyzing data and information using subject matter experts.
- Identifying and prioritizing the risks faced by the Commonwealth, regions, cities, and towns within it.
- Producing value-added intelligence products that can support the development of performance-driven, risk-based prevention, response, and consequence management programs.
- Identifying specific protective measures to discover and disrupt potential terrorist attacks during the planning and early operational stages.

INVESTIGATIVE SUPPORT

CFC staff provides research and analytical support to criminal justice agencies throughout the Commonwealth. Our analysts process and disseminate information related to crime trends, possible solutions, and potential criminal activity. Analysts conduct case workups to support active investigations by using data from State Police databases, CJIS, III, RMV, etc. as needed. Among the services our analysts provide in this area are the following:

Case Analysis

Case analysis is an approach used to manage the analysis of diverse data to support active or re-opened investigations.

Business/Bank Record Analysis

Business/Bank Record Analysis involves a review of business or bank records to look for inconsistencies, anomalies, or evidence of criminal activity. Business or bank records could include ledgers, invoices, orders, travel records, or bank statements.
Pictometry

The CFC has an advanced imaging system using up-to-date satellite photography for locations across the state. Pictometry can assist with case investigations, special events planning and critical infrastructure security planning.

Information Validation

CFC analysts can use a range of resources to validate information about individuals, businesses, and organizations. Some of these services include public databases such as Choicepoint, Locate Plus, and motor vehicle files.

Deconfliction

Deconfliction is designed to identify and coordinate concurrent investigations, and effectively allocate resources toward the agency that is closest to arrest and prosecution. This ensures that one agency is not targeting another and provides a safe work zone for enforcement activities. The CFC does not control or dictate actions in this regard, but can assist in deconflicting cases. Agencies should be directed to request coordination of this service through NESPIN, for investigations, or the New England High Intensity Drug Trafficking Area Task Force (NE HIDTA) for illicit drug investigations.

INTELLIGENCE ANALYSIS

Link Analysis

Link or network analysis looks at relationships among individuals, locations, groups, businesses or other entities involved in criminal activity. Link analysis products include link charts, biographical profiles, chart summaries, conclusions, and recommendations for further action.

Data Mining

The CFC will provide a data mining resource through Raytheon’s Information Management System – COPLINK application. Individuals, organizations, locations, vehicles, and businesses can be examined through the artificial intelligence algorithms built into this analytical product.

Event-Flow Analysis

Event-Flow Analysis develops event flow and timelines to examine incidents over time. This type of analysis includes flow charting as well.

CRIME ANALYSIS

Crime Pattern Analysis

Crime pattern analysis examines the characteristics of criminal acts to determine patterns among various incidents. The patterns involved may be based upon time, day of week, geography, suspects, victim types, modus operandi, or targets.
Market Profiles
Market profiles are assessments of the state of the criminal market around a particular illicit good or service such as drugs, stolen or counterfeit merchandise.

Hot Spots Analysis
This technique involves the geographic analysis of crime or incident data assessing clusters of activity. The CFC has a robust geographic information system that forms the backbone of its mapping capability.

SP Oliver
The Fusion Center’s Crime Reporting Unit has developed a web-based crime statistical analysis tool in conjunction with MassGIS. Using a twenty-year set of crime data for Massachusetts, this tool allows the general user to examine crime data or statewide crime patterns.

CRITICAL INFRASTRUCTURE PROTECTION AND ASSESSMENT

Statewide Threat and Vulnerability Assessment
This assessment is a compilation of critical infrastructure sector-specific threats, vulnerabilities, and security improvements collected annually. This analysis provides an overview of strengths, weaknesses, opportunities, and threats to critical infrastructure across the Commonwealth.

Buffer Zone Protection Program (BZPP)
This U.S. Department of Homeland Security-sponsored program emphasizes the development of threat and vulnerability assessments on selected critical infrastructure sites throughout the Commonwealth.
Chapter 7

Dissemination

The CFC strives to deliver timely intelligence products in the most appropriate form to users. The form may include bulletins, briefings, reports, or assessments. Intelligence customers make decisions – operational, strategic, and policy – based on the information.

CFC dissemination activities include:

- Identification of those entities and personnel (e.g., officials, executives) responsible for developing and implementing prevention, response, and consequence management (public and private) efforts.
- Provision of relevant and actionable intelligence in a timely manner to those entities responsible for implementing prevention, response, and consequence management efforts (public and private sector).
- Archiving all data, information, and intelligence to support future efforts.
- Supporting the development of performance-based prevention, response, and consequence management measures.
- Providing feedback to information collectors.

There are a myriad of ways intelligence can be disseminated throughout the Commonwealth. The user’s ability to receive secure or non-secure information is a factor in the dissemination process.

Need to Know, Right to Know Rule

The Need to Know Rule establishes the requirement that the information requested is both pertinent and necessary for the requesting individual or agency to initiate, further, or complete an assigned law enforcement task. Commensurate with this is the Right to Know Rule, where the requestor has an official capacity and/or statutory authority to receive the information being sought. This rule seeks to limit sharing of sensitive intelligence to entities that will use it for necessary policy and/or investigative decisions. This is a fundamental guideline for all dissemination activities at the CFC. The Need to Know, Right to Know rule can be controversial in that it will, at certain times, restrict information to relatively small groups of individuals and agencies, often causing distress among stakeholders who are outside of that group. Nevertheless, this rule is vital to maintaining the privacy and security of raw intelligence and sensitive investigative and intelligence data.

Third Agency Rule

The recipient of information and intelligence is prohibited from sharing that information or intelligence with another agency or entity without an explicit waiver from the originating agency.

---

No "original document" which has been obtained from an outside agency is to be released to a third agency. Should such a request be received, the requesting agency will be referred to the submitting agency for further assistance. This is also a critical guideline for the CFC because it protects original information and sensitive investigations. In order to build credibility among diverse public safety agencies, it is imperative that the CFC maintain a high level of trust and security in the information that it has received from other partners. The most appropriate means to share much of this third party information is to refer those requesting said information to the originating agency.

**REPORT TYPES**

The CFC will distribute four types of intelligence products:

- **Bulletins:** of an immediate nature, such as an officer safety issue, be on the lookout (BOLO), or some other tactical information. The intent is to disseminate information (all sources having been contacted to confirm facts) or request responses. These also include recommendations for action when appropriate.

- **Briefs:** a summary of recent events, which have been researched and validated by CFC analysts. The analyst must add value to the collected information, and not just forward information collected.

- **Reports:** A substantive analysis of a topic of concern to the Commonwealth.

- **Assessments:** A long term strategic overview addressing a threat to the Commonwealth. This will be the culmination of research and information collection analyzed over the breadth of one topic, and may address an individual, a group, a place, or an event.

**CLASSIFICATION OF REPORTS**

The CFC will classify every intelligence product it disseminates. The purpose of classification is to guide dissemination of information and intelligence; however, it is acknowledged that we should not over-restrict information when dealing with our private and public sector partners. The CFC Security Officer will be responsible for overseeing the classification of documents released by the CFC. The following are classifications to be used by the CFC until further notice:

- **Unclassified (U):** Dissemination has no restrictions

- **Sensitive but Unclassified (SBU):** Dissemination has restrictions to those who need to know, and have a right to know, which would include any intelligence geared to critical infrastructure partners. Specific dissemination issues should be resolved by the CFC command staff.

- **Law Enforcement Sensitive (LES):** Dissemination is restricted to law enforcement only. This may have to do with the conclusions reached by analysts, or may involve CORI.
As a general principle, the CFC will ensure that as much information as possible is released to our public and private sector partners. It may be possible to summarize a report considered LES whereby certain details are redacted, but the gist of a product is available to all concerned parties.

**DISSEMINATION METHODS**

**Dissemination Lists**

The CFC must coordinate the dissemination of intelligence to critical policy makers, public safety officials and our private sector partners who have a need to know and right to know certain information and intelligence. The lists will include:

- Law enforcement personnel
- Key policy makers
- General criminal justice and public safety personnel
- Private Sector partners

**E-Mail Dissemination**

The CFC will continue to utilize e-mail notification for intelligence bulletins and alerts to authorized recipients as needed and feasible.

**Notification Policy**

Dissemination of time sensitive, emerging events will be accomplished through a variety of means such as pagers, telephone calls, e-mail and fax transmission. The CFC is tasked with immediate notification of significant events through our notification policy. Leveraging emerging technologies such as the Homeland and Health Alert Network (HHAN), the CFC will endeavor to use best practices to reach a wide audience of public safety and private sector partners.

**Homeland Security Information Network – Massachusetts (HSIN-MA)**

The CFC will leverage information and intelligence dissemination using the DHS-supplied HSIN. Information sharing activities will include the posting of our collection requirements, requests for information, and intelligence products, as well as a document library for dissemination of other homeland security documents. HSIN-MA enables the CFC to develop a multi-layered dissemination system through various communities of interest such as law enforcement and general criminal justice communities. This enables wide dissemination of information and intelligence but restricts it to relevant communities of interest.

HSIN-MA will enable the CFC to implement the need to know, right to know and third agency rules in a secure web environment. Information will be pushed to relevant public safety entities and private sector partners within the parameters of these guidelines.

HSIN-MA requires user registration and vetting to control access to critical information and intelligence. The CFC has developed a number of communities of interest, each with different access rights based upon their need to know, right to know requirements.
Crime Reports

The CFC's Crime Reporting Unit is the state repository for FBI Uniform Crime Reporting (UCR) and National Incident Based Reporting System (NIBRS) data from participating agencies. It has a large repository of crime information which is used to provide local, regional, statewide, and national assessments of crime trends. The Crime Reporting Unit produces a series of annual crime reports, such as the yearly UCR report. It uses traditional dissemination methods such as hard copy reports and mass mailings to police agencies. It will implement web-based reports with the development of HSIN-MA.
Chapter 8

Review and Reevaluation

REVIEW AND REEVALUATION

As information is received, processed, and analyzed, it must be critiqued to see if collection and other operational requirements are being met. The information sharing and intelligence process is not complete until a review is performed of the information or intelligence product to ensure the requestor has received it and to verify that the requirement has been met. If the requirement has not been met, the process must be modified with a focus on new assets and collection requirements and re-activated.

CFC review and reevaluation activities include the following\(^{11}\):

- Review and re-evaluate intelligence documents stored in intelligence files or the IMS.
- Update threat and vulnerability assessments so as to update the risk environment.
- Assess effectiveness of national (Federal, state and local) information and intelligence collection requirements process.
- Modify requirements as necessary.
- Communicate modifications in a timely manner.

COLLECTION REQUIREMENTS REVIEW

Collection requirements should be reviewed at least annually to assure that they are collecting the most relevant information to fit the information sharing and intelligence goals and objectives of the CFC. This review should include examination of priority information and intelligence requirements, information and data sources and methods to retrieve information.

To assess the collection function of the CFC, the following evaluation criteria will be used to determine if the CFC:

- receives as part of its normal information flow, investigative information from the State Police and partner law enforcement agencies,
- coordinates information collection among the MSP Anti-Terrorism Unit,
- tasks out information appropriately to other public safety agencies,
- maintains a field interview and observation system to channel data from uniformed troopers and patrol officers in police agencies,
- receives information from other state and federal investigative sources, and
- has a plan for developing new data sources.

Review Information Sharing and Intelligence Collection Efforts

Another area of review and feedback involves information sharing and intelligence collection efforts. The CFC must conduct ongoing assessments of initiatives such as ESF-18 Public-Private Partnership and HSIN-MA portal. Generating user feedback and commentary is a key aspect of this review. For example, future efforts will focus on the development of enhanced processes for collecting and integrating private sector incident reports.

Review and Purge of Intelligence Records

Information stored in the criminal intelligence file or the Information Management System (IMS) should be reviewed periodically for reclassification or purging in order to:

- ensure that a file is current, accurate, and relevant to the needs and objective of the agency and its partners;
- safeguard every individual's privacy rights as guaranteed under federal and state laws; and
- ensure that the security classification level remains appropriate.

Partner law enforcement agencies have an obligation to keep stored information on subjects current and accurate. Reviewing of criminal intelligence should be done on a continual basis as agency personnel use the material in carrying out day-to-day activities. In this manner, information that is no longer useful or that cannot be validated can immediately be purged or reclassified where necessary.

To ensure that all files are reviewed and purged systematically, agencies should develop purge criteria and schedules which are compliant with Criminal Intelligence Systems 28 CFR 23. Operational procedures for the purge and the method of destruction for purged materials should be established.

Purge Criteria:

General considerations for reviewing and purging of information stored in the criminal intelligence file are as follows:

**Utility**

- How often is the information used?
- For what purpose is the information being used?
- Who uses the information?

**Timeliness and Appropriateness**

- Is this investigation still ongoing?
- Is the information outdated?
- Is the information relevant to the needs and objectives of the agency?
- Is the information relevant to the purpose for which it was collected and stored?
Accuracy and Completeness

- Is the information still valid?
- Is the information adequate for identification purposes?
- Can the validity of the data be determined through investigative techniques?

Review and Purge Time Schedule

Reclassifying and purging information in the CFC intelligence file, IMS or other application should be done on an ongoing basis as documents are reviewed. In addition, a complete review of the criminal intelligence file for purging purposes shall be undertaken periodically. This review and purge schedule varies from once each year for documents with temporary status to once every five years for permanent documents. Documents stored in the CFC intelligence file or IMS which have not been queried or accessed for five years will be purged from those systems.

Participating agencies should develop similar policies and a schedule best suited to their needs and should contact their legal counsel for guidance.

Manner of Destruction

Material purged from the criminal intelligence file or IMS shall be destroyed. Disposal is used for all records or papers that identify a person by name. Paper documents and other storage media such as videos or cassette tapes shall be shredded or similarly destroyed.

It is the responsibility of each participating agency to ensure that their obsolete records are destroyed in accordance with applicable laws, rules, and state or local policy.
Chapter 10

Commonwealth Fusion Center Databases and Data Sources

What follows is an overview of the databases and data sources available to the CFC. The CFC is constantly searching for data that will fulfill its analytical mission; therefore this is not a complete inventory.

National Law Enforcement Telecommunications System (NLETS)
The National Law Enforcement Telecommunications System (NLETS) provides two basic capabilities:

- A computer-based message switching system linking together state, local and federal law enforcement and justice agencies for the purpose of information exchange, and
- Information services support for justice-related applications

NLETS supports data communications links to state networks using a commercial frame relay service, not the Internet. Within each state, all agencies receive NLETS service through the state interface, in Massachusetts this is the Criminal Justice Information System (CJIS) operated by the Criminal History Systems Board.

NLETS include all of the states and territories, all federal agencies with a justice component, and some international agencies. Data that are shared through NLETS transactions range from motor vehicle and driver records, HAZMAT, Canadian "Hot File" records and INS databases to state criminal history records. Over 40 million messages are transacted each month.

Violent Gang and Terrorist Organization File (VGTOF)

One part of NLETS is the NCIC 2000 Violent Gang and Terrorist Organization File (VGTOF). VGTOF has been designed to provide identifying information about violent criminal gangs and terrorist organizations and members of those gangs and organizations to law enforcement personnel. This information serves to warn law enforcement officers of the potential danger posed by violent individuals and to promote the exchange of information about these organizations and members to facilitate criminal investigations.

- The Group Reference Capability (GRC) provides information about gangs and terrorist organizations. This capability can be accessed by a QGG inquiry.
- The Group Member Capability (GMC) provides information on individual members of gangs or terrorist organizations. This capability can be accessed by a QGM inquiry.

Homeland Security Information Network (HSIN)
The Homeland Security Information Network (HSIN), which is available in all 50 states, makes real-time threat-related information available to law enforcement and emergency managers on a daily basis through a Web-based system. Members of the private sector, including owners and
operators of critical infrastructure, now also receive threat-related information through the HSN system. In addition, members of 35 different Federal agencies are now all collocated in DHS’ 24-hour Homeland Security Operations Center (HSOC), which allows the information coming from various sources to be synthesized together and then shared with other federal partners such as the FBI and the Department of Defense (DOD).

The system is encrypted at the most secure levels, ensuring the safest delivery of real-time interactive connectivity among state and local partners through the HSOC using the Joint Regional Information Exchange System (JRIES), a secure network and a suite of applications including mapping and imaging capabilities. It is centered on addressing four basic needs, including planning and preparedness, emergency response, threat awareness and vulnerability identification, and basic information sharing. Major features include broadcasting and "narrowcasting" of warnings and threats from DHS, user access to sensitive documents that enables real-time analysis of data, secure e-mail, and provision of peer-to-peer collaboration technology allowing real-time dialogue among members.

Each state and major urban area's participants includes governors, mayors, Homeland Security Advisor, state National Guard offices, Emergency Operations Centers, First Responder and Public Safety departments, and other key homeland security partners.

Joint Regional Information Exchange System (JRIES)

Originating as a pilot project by the DOD's Defense Intelligence Agency (DIA) aimed at improving the exchange of counterterrorism information between local and state law enforcement and components of DOD and DIA, JRIES is an Internet-based counterterrorism communications initiative. Now managed as an application on HSN, the JRIES target audience includes state and local governments, counterterrorism and intelligence agencies, and law enforcement agencies. Operating at the sensitive but unclassified (SBU) level, JRIES facilitates collaboration among its members by providing a secure environment for exchanging e-mails and peer-to-peer collaboration allowing real-time dialogue, and also provides access to data visualization software and analysis tools. It has also provided real-time links between the HSOC and counterterrorism teams at high-profile events such as the Super Bowl.

Information Management System (IMS) - COPLINK

The CFC is using COPLINK, a web-based law enforcement data mining tool to assist with the analysis of crime and homeland security information. COPLINK provides a platform for the integration of data from disparate information systems. A number of criminal justice databases are linked to the Fusion Center COPLINK node. In addition, a Direct Data Entry module allows investigators and analysts to enter information directly into COPLINK.

The integrated data is refreshed (updated) on a schedule determined by the contributing agencies. This integrated data allows for advanced analysis using artificial intelligence-based searches. Once this data is integrated, COPLINK utilizes a built-in link analysis tool, COPLINK® Visualizer, to display the links and associations among individuals, locations, incidents and other case information.
This application allows investigators to share information and post requests for information regarding certain investigations. COPLINK® Active Agent is a tool that allows investigator collaboration and notification to assist on-going investigations.

COPLINK is available to law enforcement agencies who have investigative and intelligence responsibilities.

Regional Information Sharing System (RISS)

The Regional Information Sharing System (RISS) links law enforcement agencies throughout the nation, providing secure communications, information sharing resources, and investigative support to combat multi-jurisdictional crime and terrorist threats. RISS is a national program made up of six centers that operate in geographic regions of varying size, serving the unique needs of law enforcement in each region while fostering information sharing among all levels of law enforcement across the country. RISS serves over 7,000 local, state, federal, and tribal law enforcement member agencies in all 50 states, the District of Columbia, U.S. territories, Australia, Canada, and England. The New England State Police Information Network (NESPIN) is the regional RISS site for Massachusetts and is headquartered in Franklin, MA.

The RISS secure intranet — RISSNET— serves as the communications backbone for the secure exchange of sensitive information and also allows instant electronic access to RISS services by RISS member agencies. Resources available for access on RISSNET include:

- RISS Investigative Leads Bulletin Board;
- RISSLive;
- RISS criminal intelligence databases (RISSIntel);
- RISS Anti-Terrorism Information Exchange (ATIX);
- RISS National Gang Database;
- RISS search engine (RISSSearch);
- RISSLinks—a data visualization and link analysis tool;
- Various state, regional, federal, and specialized criminal intelligence databases;
- RISS center Web sites.

ATF Bomb and Arson Tracking System (BATS)

The CFC has developed a partnership with the Bureau of Alcohol, Tobacco, Firearms, and Explosives to share the ATF's Bomb Arson Tracking System (BATS 2.0). It is the first web-based intelligence database that will allow federal, state, and local law enforcement and bomb scene commanders to share crucial information about arson and explosives incidents around the nation. BATS is an arson and explosives incident database for the entire U.S. Department of Justice, developed to achieve an unprecedented degree of information sharing among law enforcement agencies and fire service organizations at every level of government.
The BATS database improves coordination and cooperation in the fight against terrorism. It will allow images of arsons, improvised explosives devices, and crime scenes to be shared online with law enforcement partners anywhere in the United States. Investigators and analysts will be able to track trends and compare incidents for similarities in motives, leads, and potential suspects.

National Incident Based Reporting System (NIBRS)
The National Incident-Based Reporting System (NIBRS) is the replacement data collection system developed by the FBI to take the place of the older Uniform Crime Reporting (UCR) system. NIBRS collects standardized data from over 270 Massachusetts police agencies. NIBRS collects detailed information on the criminal incident, as well as demographics of victims, offenders, and arrestees. NIBRS collects data on 46 different offense types. There are a total of 53 data elements in the complete FBI data set.

SP Oliver
The CFC’s Crime Reporting Unit has collaborated with MassGIS to develop an online crime mapping application called SP Oliver. This application consists of a web-based geographic information system used to analyze crime trends from a data set of 20 years of FBI Uniform Crime Reporting data. Leveraging existing technology and crime reporting databases, this project provides an analytical tool to examine crime data along with U.S. Census data.

Financial Crimes Enforcement Network (FinCEN)
FinCEN supports law enforcement investigative efforts and fosters interagency and global cooperation against domestic and international financial crimes to provide United States policymakers with strategic analysis of domestic and worldwide money-laundering developments, trends, and patterns. FinCEN controls over 150 million reports filed under the Bank Secrecy Act and other similar laws.

Law Enforcement Online (LEO)
The FBI’s Law Enforcement Online (LEO) is a national interactive computer communications system and information service, an Intranet exclusively for the law enforcement community. It can be accessed by any approved employee of a duly constituted local, state, or federal law enforcement agency, or approved member of an authorized law enforcement special interest group. LEO is intended to provide a state-of-the-art communication mechanism to link all levels of law enforcement throughout the United States. Online services available to members include special interest group bulletin-boards, customized web-pages focused on law enforcement subjects, chat, email, electronic calendar, topical electronic library, and distance learning services.