Commonwealth Fusion Center
Standard Operating Procedure

Effective Date	Number
January 1, 2026	CFC-02[1]
Subject	
Commonwealth Fusion Center Privacy, Civil Rights, and Civil Liberties Policy	

Purpose

The Commonwealth Fusion Center (CFC) collects, evaluates, analyzes and disseminates information in furtherance of its mission while protecting privacy, civil rights, civil liberties, and other protected interests. This includes implementing appropriate privacy and civil liberties safeguards as outlined in the Privacy Act of 1974, as amended, to ensure that the information privacy and other legal rights of individuals and organizations are protected.

This privacy, civil rights, and civil liberties policy assists the Commonwealth Fusion Center (CFC) and its authorized users in:

- Increasing public safety and improving national security.
- Minimizing the threat and risk of injury to specific individuals.
- Minimizing the threat and risk of injury to law enforcement and others responsible for public protection, safety, or health.
- Preventing and disrupting potential terrorist and/or criminal activity.
- Protecting the privacy, civil rights, civil liberties, and other protected interests of individuals in the United States.
- Minimizing the threat and risk of damage to real or personal property.
- Protecting the integrity of the criminal investigatory process, criminal intelligence, and justice system processes and information.
- Minimizing reluctance of individuals or groups in the United States to use or cooperate with the justice system.
- Supporting the role of the justice system in society.
- Promoting governmental legitimacy and accountability.
- Not unduly burdening the ongoing business of the justice system.
- Making the most effective use of public resources.

Definitions

Primary terms and definitions are located in Appendix A.

[1] This policy supersedes all previous Commonwealth Fusion Center policies related to privacy.

Policy Applicability and Legal Compliance

All CFC personnel and non-CFC personnel assigned to the CFC shall comply with the CFC's privacy, civil rights, and civil liberties policy. This policy applies to information the CFC gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to CFC personnel, governmental agencies (including Information Sharing Environment (ISE) participating centers and agencies), participating justice and public safety agencies, private contractors, private entities, and the general public.

All CFC personnel and non-CFC personnel assigned to the CFC shall comply with applicable state and federal law protecting privacy, civil rights, and civil liberties, including, but not limited to:

- The Constitution of the United States
- The Constitution of the Commonwealth of Massachusetts
- MGL c. 22C, § 38 (Criminal Information)
- MGL c. 4, §7, cl. 26 (a)–(u) (Public Record Exemptions)
- 28 CFR Part 23 related to Criminal Intelligence Systems
- MGL c. 6, § 167 *et seq.* (Criminal offender Record Information)
- MGL c. 66, §10 (Public Records Law)
- MGL c. 66A, §1 (Fair Information Practices)
- MGL c. 272, §99 (Wiretap Law)
- MGL c. 41, §98F (Daily Logs)
- MGL c. 41, §97D (Rape and Sexual Assault Reports)
- MGL c. 265, §24C (Confidentiality of Alleged Rape Victim's name)
- MGL c. 93H, §1 *et seq*. (Security Breach/Personal Information)
- 18 USC 2722 (Federal Driver's Privacy Protection Act)
- Laws and statutes applicable to victim rights and confidentiality
- Laws applicable to juvenile confidentiality

The CFC has adopted internal operating policies and procedures that are in compliance with applicable laws protecting privacy, civil rights, and civil liberties.

Governance and Oversight

The Massachusetts State Police (MSP) oversees CFC operations. A sworn member of the MSP serving in the rank of Major is designated as the Director of the CFC (CFC Director) and supervises the overall operation of the CFC, including the implementation and enforcement of this policy.

The MSP shall designate an employee to serve as the Privacy and Civil Liberties Officer for the CFC. The Privacy and Civil Liberties Officer shall be qualified to handle complex privacy, civil rights, and civil liberty issues. The Privacy and Civil Liberties Officer is the point of contact for reporting alleged violations of this policy. The Privacy and Civil Liberties Officer is also responsible for receiving complaints and coordinating complaint resolution

pursuant to the procedures set forth in the Public's Right of Inspection and Redress section of this policy. The Privacy and Civil Liberties Officer also serves as the liaison to the Information Sharing Environment, ensuring that privacy, civil rights, and civil liberties protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies. The Privacy and Civil Liberties Officer can be contacted by sending an email to the attention of the CFC Privacy and Civil Liberties Officer to fusion@mass.gov, or by sending correspondence to the following physical address:

Commonwealth Fusion Center
470 Worcester Road
Framingham, MA 01702
ATTN: CFC Privacy and Civil Liberties Officer

The CFC shall conduct regular reviews to assess compliance with this policy. The CFC Director, the Deputy CFC Director, the Executive Officer of the CFC, the Assistant Intelligence Services Manager, the Commonwealth Watch Center Commander, the Criminal Information Section Commander, the Anti-Terrorism Unit Commander, and the CFC Privacy and Civil Liberties Officer provide continuous oversight of CFC operations and are constantly monitoring to ensure that privacy, civil rights, and civil liberties are protected in accordance with this policy. The CFC Privacy and Civil Liberties Officer is responsible for oversight of all privacy matters and works in conjunction with CFC leadership in regard to oversight.

The CFC Director and/or designee shall ensure that CFC information is maintained in a secure manner and shall establish access and dissemination guidelines. Access to CFC information shall be granted only to internal and external personnel whose position and job duties require such access; who have successfully completed a background check and obtained an appropriate security clearance, if applicable; and who have been selected, approved, and trained accordingly.

An audit mechanism shall be available relative to access history and disclosure of CFC information for databases that are actively managed.

CFC Information

The CFC has been designated by Massachusetts Executive Order 476 as the principal state repository for threat-related information, including: criminal activity, threats to public safety, and terrorist activity.

The CFC maintains, accesses, and/or uses different types of information from various sources. This information includes, but is not limited to: publicly available open-source information, tips and leads, FIOs, SARs, criminal intelligence information, and information contained in fact-based information databases (e.g., criminal history records, case management information, deconfliction, wants and warrants, driving records, and commercial databases).

The CFC receives information from various federal, state, and local law enforcement agencies, public safety partners, and the private sector.

The CFC shall only seek or retain information that:

- Is reasonably related to a possible threat to public safety or the enforcement of 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 and/or terrorist activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal and/or terrorist activity, or
- Is relevant to the investigation and/or prevention of suspected criminal and/or terrorist activities, the justice system response to suspected criminal and/or terrorist activities, and the enforcement of legal sanctions, orders, and/or sentences, or
- Is useful in crime analysis or in the administration of criminal justice (including topical searches), or
- Is necessary to ensure public safety and/or public order, and
- Is obtained from a reliable and verifiable source or limitations on the quality of the information are identified, and
- Was collected in a fair and lawful manner except to the extent that the CFC, as a law enforcement entity, is authorized or mandated to act upon such information.

The CFC may seek and retain information which is based on "reasonable suspicion" that an individual or organization has committed or is planning to commit a criminal offense or terrorist act, and the information is relevant to the criminal or terrorist activity. Information that meets the criteria of this paragraph may be entered into a Criminal Intelligence system or other CFC database that is maintained in accordance with 28 CFR Part 23.[2]

The CFC may seek and retain information that is based on a level of suspicion that is less than "reasonable suspicion," such as Suspicious Activity Report (SAR) information, subject to the provisions of this policy. If such information meets the criteria established in the current version of the *Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.5.5*, the CFC may disseminate the information to any law enforcement agency or official permitted by law.

If the information does not meet the criteria established in the current version of the Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.5.5, but the information still represents a serious threat to any individual, community, or the nation, the CFC may elect to enter the information into the FBI's eGuardian system without providing access to other external agencies.

[2] As of the effective date of this policy, the Commonwealth Fusion Center (CFC) does not maintain or enter information into a criminal intelligence database as defined by 28 CFR Part 23. The CFC is not subject to 28 CFR Part 23 but has voluntarily adopted the protections articulated in 28 CFR Part 23 as a matter of policy.

The CFC shall not seek, accept, or retain, and will inform originating agencies not to submit, information about individual(s) or organization(s) solely on the basis of their political, religious, or social views or activities; their participation in a lawful event; their membership in or association with an organization not involved in criminal activity; or their race, religion, ethnicity, citizenship, national origin, age, disability, gender, gender identities, or sexual orientation.

CFC personnel shall never consider a subject's race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity as factors creating suspicion. However, those attributes may be documented in specific suspect descriptions for identification purposes.

Upon receipt of information, the CFC shall assess and review the information to determine its nature, usability, reliability, veracity, and quality. This assessment shall include consideration of the following:

- Whether the information consists of tips and leads data, suspicious activity reports, criminal history, intelligence information, case records, conditions of supervision, case progress, or other information category.
- The nature of the source as it affects veracity (e.g., anonymous tip, trained investigator, public record, private sector).
- The reliability of the source (e.g., reliable, usually reliable, unreliable, unknown).
- The validity of the content (e.g., confirmed, probable, doubtful, cannot be judged).

The CFC shall keep a record of the source(s) of all information collected and retained by the CFC.

The CFC will identify and review protected information prior to sharing that information through the Information Sharing Environment (ISE). Further, the CFC will provide notice mechanisms (e.g., data field labels) that will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

The CFC will not knowingly accept any information from any source that is obtained in violation of any federal, state, or local law, ordinance, or regulation, except to the extent that the CFC, as a law enforcement entity, is authorized or mandated to act upon such information.

Suspicious Activity Report Information

CFC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips, leads, and other information related to suspicious activity that may or may not lead to the generation of a Suspicious Activity Report (SAR). Prior to allowing access to or disseminating SAR information, CFC personnel shall ensure that:

- Reasonable attempts to evaluate or screen the information have been made to assess the information's credibility and/or reliability
- The information has been analyzed for sensitivity and confidence.
- Information is marked as uncorroborated when its credibility and/or reliability is uncorroborated.
- Information is marked as invalidated when its credibility and/or reliability has been invalidated or otherwise unsubstantiated.
- Standardized reporting formats and data collection codes are utilized for SAR information.
- CFC shall store SAR 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.
- The SAR storage system shall include an audit and inspection mechanism, and the data shall be labeled to distinguish it from other information within the system.
- Access to, or dissemination of, the information shall use the same (or a more restrictive) access and dissemination standard that is used for data that rises to the level of reasonable suspicion (e.g., "need-to-know" and "right-to-know" access or dissemination of personally identifiable information).
- Immediate steps shall be taken to determine the validity of any otherwise unvalidated tip or lead[3] to determine its credibility or law enforcement value.
- The CFC's physical, administrative, and technical security measures are adhered to in order to ensure the protection and security of tips, leads, and SAR information. Tips and leads (including SAR information) will be secured in a system that is the same as or similar to the system that secures data that rises to the level of reasonable suspicion.

The CFC 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, thus leveraging existing policies and protocols to protect the information.

The CFC's SAR process provides for human review and vetting to ensure that information is gathered in an authorized and lawful manner and, where applicable, determined to have a potential nexus to terrorism or criminal activity. CFC personnel shall be trained to recognize behaviors and incidents that are indicative of potential criminal activity or terrorism. To the extent feasible, the CFC will train outside law enforcement members to recognize

[3] SAR information is a subset of tips and leads. Retention and use of a tip or a lead will be affected by whether it has been validated. See the definitions of "validated information," "invalidated information," and "unvalidated information," in Appendix A, Terms and Definitions.

those behaviors and incidents indicative of potential criminal activity or terrorism.

The CFC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that are consistent with criminal and/or terrorist activity will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights (race, religion, ethnicity, citizenship, national origin, age, disability, gender, gender identities, or sexual orientation) and civil liberties (speech, assembly, religious exercise, etc.) will not be inappropriately gathered, documented, processed, and shared.

Acquiring and Retaining Information

Information gathering (acquisition) and investigative techniques used by the CFC will comply with all applicable laws and regulations, including, but not limited to:

- 28 CFR Part 23[4] regarding criminal intelligence information, as applicable.
- Constitutional provisions, applicable Massachusetts code provisions and administrative rules (including those cited in the "Compliance with Laws Regarding Privacy, Civil Rights, and Civil Liberties" section of this policy), as well as regulations and policies that apply to multijurisdictional intelligence and information databases.

The CFC will further attempt to comply with best practices, principles, and guidelines including, but not limited to:

- The OECD Fair Information Practice Principles (FIPPS) (if circumstances arise where the Fair Information Principles conflict with law, regulation, order of a court, or CFC/MSP policy, the conflicting FIPPS shall not apply).
- Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP) (Ver.2.0).

Information gathering and investigative techniques used by the CFC will be the least intrusive necessary, given the particular circumstances, to gather information it is legally authorized to seek, collect, and retain.

The CFC will contract only with commercial database entities that provide an assurance that their methods for gathering personally identifiable information

[4] The operating principles of 28 CFR Part 23 provide guidance to law enforcement regarding how to operate criminal intelligence information systems effectively while safeguarding privacy and civil liberties. The regulation applies, as a matter of law, to state, local, tribal, or territorial agencies if they are operating interjurisdictional or multijurisdictional criminal intelligence systems that are supported with Omnibus Crime Control and Safe Streets Act funding. See 28 CFR § 23.3. For participating or member agencies, the intelligence project's operating policies, as set forth in a participation or membership agreement, govern their submission, access, use, retention/destruction, and any third-party dissemination of criminal intelligence information received from the intelligence project. For further information, see https://28cfr.iir.com/Resources/Executive-Order.

comply with applicable law and that their methods are not based on misleading collection practices.

External agencies that access the CFC's information or share information with the CFC are governed by the laws and rules governing those individual agencies, including applicable federal and state laws.

Classification of Information

At the time of entry and subsequent retention, if applicable, into the appropriate CFC system, information received by the CFC will be reviewed to determine its veracity and reliability. This review, to the maximum extent possible, shall include an evaluation of:

- The veracity of the source (e.g., anonymous tips, trained investigator, public record, private sector);
- The validity of the content (e.g., verified, partially verified, unverified, or unable to verify); and
- The reliability of the source (e.g., completely reliable, usually reliable, unreliable, reliability unknown).

The CFC will re-evaluate the classification of new or existing information whenever new information is received or added. The purpose of the evaluation will be to determine what impact or effect, if any, additional information has on the reliability and/or veracity of previously received and/or retained information.

At the time a decision is made by the CFC to enter new or retain existing information, CFC personnel shall take all necessary steps, to the maximum extent feasible and pursuant to applicable limitations on access and disclosure, to:

- Protect confidential sources and law enforcement undercover techniques and methods.
- Not interfere with or compromise pending criminal investigations.
- Protect the privacy, civil rights, and civil liberties of all involved.
- Ensure that confidentiality restrictions based on an individual's status (e.g., as a child, sexual abuse victim, or resident of a domestic abuse shelter, etc.) are complied with in accordance with applicable law.

The access classifications established under applicable guidelines shall determine the user's access authority level. The access authority level controls the range and scope of information to which authorized CFC personnel have access and what information authorized CFC personnel can add, change, remove, or print. The access authority level shall determine to whom CFC information can be disclosed and under what circumstances.

Data Quality Assurance

The CFC shall make reasonable efforts to ensure that information retained is accurate, relevant, complete, and derived from dependable and trustworthy sources of information. The CFC shall also make reasonable efforts to ensure

that information is only merged with other information about the same individual or organization when the applicable criteria in the "merging of information" section is met.

The CFC shall promptly investigate alleged errors and deficiencies in information received (or refer them to the originating agency for investigation) and will make reasonable efforts to correct, remove, or refrain from using information that is determined to be erroneous, deficient, misleading, obsolete, or otherwise unreliable.

If the CFC determines that it did not have authority to collect certain information, the CFC shall immediately remove or refrain from using the information in question.

Originating agencies external to the CFC are responsible for reviewing the quality and accuracy of their information prior to providing the information to the CFC. The CFC will review the quality of information it receives from originating agencies. The CFC shall promptly notify the originating agency in writing if information received is alleged, suspected, or found to be inaccurate, incomplete, unsubstantiated, or otherwise unreliable.

If information previously provided to a recipient agency is determined to be deficient, erroneous, incorrectly merged, out of date, or lacking adequate context, the CFC shall promptly notify the recipient agency in writing.

Analysis of Information

Information received by the CFC will only be analyzed by qualified individuals who have successfully passed a background check, possess the appropriate security clearance, and have been properly trained to provide tactical and/or strategic intelligence analysis on criminal and/or terrorism related matters.

Information acquired or received by the CFC, identified in "CFC Information," or accessed from other sources will only be analyzed to further crime and terrorism prevention, public safety, law enforcement resource deployment, or prosecution objectives.

Information received by the CFC will not be analyzed or combined in an unlawful manner or for an unlawful purpose.

The CFC requires that all analytical products are reviewed and approved by the CFC Director or designee prior to dissemination to ensure that they provide applicable privacy, civil rights, and civil liberties protections.

Merging of Information

Information will be merged only by qualified individuals who have successfully completed a background check, possess the appropriate security clearance, and have been trained accordingly.

Records pertaining to an individual or organization from two or more sources will not be merged unless there is sufficient identifying information to clearly

establish that the information pertains to the same individual or organization. The CFC shall utilize reasonable steps when determining whether information is sufficient to permit merger.

In most cases, sufficient identifying information for an individual will include a name (full or partial), and one or more of the following: date of birth; social security number; driver's license number; fingerprints; photographs; physical description; scars, marks, or tattoos; DNA; retinal scan; or facial recognition.

In most cases, sufficient identifying information for an organization will include a name (full or partial), and one or more of the following: physical address; telephone number; email address(es); federal or state tax ID number; website; and public facing social media account(s).

If matching requirements are not fully met but there is reason to believe the records are about the same individual or organization, the information may be associated if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.

Sharing and Disclosure of Information

Credentialed, role-based access criteria will be used, as appropriate, to control:

- the information a particular group or class of users can access;
- the information a class of users can add, change, remove, or print; and
- to whom information can be disclosed and under what circumstances.

Access to information that the CFC retains shall be provided only to authorized personnel and only for the following purposes: law enforcement, public protection, public prosecution, and/or public health purposes.

The CFC adheres to the current national standards, including the current version of the ISE-SAR Functional Standard relative to the processing of suspicious activity reports (SAR). The CFC utilizes a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially related to criminal activity or terrorism.

Agencies external to the CFC may not disseminate information received from or through the CFC without approval from the originator of the information. If the originator of the information is not the source agency, the originator is responsible for notifying the external agency seeking permission to disseminate the information.

Nothing in this policy prohibits the dissemination of criminal intelligence and information to a government official or to any other individual when necessary to avoid imminent danger to life or property.

The CFC shall not confirm the existence or nonexistence of information to any person or agency who would not be eligible to receive the information, unless otherwise required by law.

Disclosure of Information to the Public

Information gathered and retained by the CFC may be disclosed to a member of the public only if the information is a public record as defined by G.L. c. 66, §10, or is not otherwise exempt from public disclosure by statute or law.

Subject only to the mandates of the CFC to comply with the Massachusetts Public Records Law or other applicable laws, the CFC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself unless otherwise required by law.

If a member of the public submits a request under the Massachusetts Public Records Law (G.L. c. 66, §10), the CFC reserves the right to assert any exemption contained in G.L. c. 4, §7, cl. 26 (a) – (u) or assert any Massachusetts statute or law prohibiting the public disclosure of requested CFC documents.

Categories of records that are ordinarily exempt from public inspection and/or not otherwise subject to public disclosure include, but are not limited to, the following records:

- Records which are, expressly or by implication, statutorily confidential or not subject to public disclosure. See M. G. L. ch. 4, §7, cl. 26 (a).
- Records related to any ongoing investigation or prosecution. See M. G. L. ch. 4, §7, cl. 26 (f).
- Investigatory materials, that if disclosed, would so prejudice the possibility of effective law enforcement that such disclosure would not be in the public interest. See M. G. L. ch. 4, §7, cl. 26 (f).
- 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. See also, M. G. L. ch. 66, §10.
- Records relating to security measures, emergency preparedness, threat assessments, or any other records related to the security or safety of persons, structures, utilities, transportation, cyber security and other critical infrastructure. See M. G. L. ch. 4, §7, cl. 26 (n).
- Records that would reveal scientific and technological secrets or the security plans of military and law enforcement agencies, the disclosure of which would endanger the public welfare and security. M. G. L. ch. 4, §7, cl. 26 (a), (f), (n).
- Records containing information of specifically named individuals, the disclosure of which would constitute an unwarranted invasion of personal privacy. M. G. L. ch. 4, §7, cl. 26 (c).

- A record or part of a record, that if disclosed, would have a reasonable likelihood of threatening public safety by exposing a vulnerability to a terrorist attack. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism, including but not limited to: vulnerability assessments, risk planning documents, needs assessments, and threat assessments. See M. G. L. ch. 4, §7, cl. 26 (f) and (n).
- Information in a criminal intelligence system or other CFC database subject to 28 CFR Part 23, or information that is otherwise required to be kept confidential by federal law, federal regulation, state law, state regulation, or rule of court. See M. G. L. ch. 66, §10, M. G. L. ch. 4, §7, cl. 26 (f) and 6 U.S.C. 482.
- Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot, under the Access to Public Records Act, Massachusetts General Laws, or applicable Federal Law, be shared without permission. See 6 U.S.C. 482.
- A record, or part of a record, that constitutes trade secrets, competitively sensitive information, proprietary information, or is subject to a nondisclosure agreement. See M. G. L. ch. 4, §7, cl. 26(s).

The Massachusetts State Police shall maintain a record of all public records requests for CFC information. The Massachusetts State Police shall also maintain a record of any information disclosed in response to public records requests.

The CFC reserves the right to charge a fee for costs associated with researching or otherwise responding to a public record request in accordance with M. G. L. ch. 66, §10 and 950 CMR 32.06.

Public's Right of Inspection and Redress

Upon satisfactory verification of identity, any individual ("data subject") may access and review any of their personal data, as defined by M. G. L. ch. 66A, §1 *et seq.*, that is in the possession of the CFC and not exempt from disclosure pursuant to M. G. L. ch. 4, §7 or other applicable public records law. In accordance with M. G. L. ch. 66A, §1 *et seq.*, the data subject may access his or her personnel data for the purposes of challenging or contesting the accuracy or completeness of the information in accordance with M. G. L. ch. 66A, §1 *et seq.*

To track all requests and information disclosed, subjects requesting information shall be directed to the Massachusetts State Police public records request portal located at:

https://massstatepolice.govqa.us/WEBAPP/_rs/(S(kcevvjcan4zpsredhcnxag52))/supporthome.aspx

The CFC's response to the request for information shall be made within a reasonable time as required by law. Subject to the CFC's lawful discretion, the existence, content, and source of information shall not be made available

to an individual unless required under M. G. L. ch. 66, §10 or any other public records law, when:

- disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution;
- disclosure would endanger the health or safety of an individual, organization, or community;
- disclosure would likely jeopardize public safety or cybersecurity;
- the information is in a criminal intelligence information system or other CFC database subject to 28 CFR Part 23 [see 28 CFR § 23.20(e)];
- the information is classified or otherwise not subject to disclosure under federal or state law;
- the CFC did not originate and/or does not have the right to disclose the information; or
- other authorized basis for denial.

If the information did not originate with the CFC, the requestor will be referred to the originating agency, if appropriate or required. Otherwise, the CFC will notify the source agency of the request and its determination that disclosure by the CFC or referral of the requestor to the source agency was neither required nor appropriate under applicable law.

Information gathered or collected, and records retained by the CFC shall 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 originating agency's normal operations or specifically authorized by the originating agency; or
- disseminated to persons not authorized to access or use the information.

If an individual has a complaint regarding the accuracy or completeness of information that originated with the CFC, the individual shall be directed to submit their complaint to the CFC's Privacy and Civil Liberties Officer. The CFC's Privacy and Civil Liberties Officer will review all complaints and bring all requests to the attention of the CFC Director in a timely manner. The individual will be notified in writing of all decisions and will be provided with an explanation if their request to correct information is denied. The individual will also be informed of a procedure for appeal when the CFC has declined to correct challenged information to the satisfaction of the complainant. A record shall be kept of all requests for corrections, responses, and resulting action, if any.

Complaints regarding the accuracy or completeness of CFC information should be forwarded either by sending an email to the attention of the CFC

Privacy and Civil Liberties Officer to fusion@mass.gov, or by sending correspondence to the following physical address:

Commonwealth Fusion Center
470 Worcester Road
Framingham, MA 01702
ATTN: CFC Privacy and Civil Liberties Officer

All complaints regarding information that is retained by the CFC and originated with the CFC shall be acknowledged with an assurance that the complaint will be reviewed. The CFC will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. All complaints will be resolved within 30 days of receipt, except in unusual circumstances with the authorization of the CFC Director. After reviewing the challenged information, the CFC Privacy and Civil Liberties Officer and the CFC Director will determine if the challenged information is accurate or inaccurate. If the information is determined to be inaccurate, incomplete, or out-of-date, the information will be corrected or purged. The CFC will not share information that is subject to an unresolved complaint, except when specifically authorized in writing by the CFC Director. A record will be kept by the CFC of all complaints, findings, and any action taken in response to the complaint.

If the information subject to the complaint did not originate with the CFC, the CFC Director or designee shall notify the originating agency in writing within 10 days and, upon request, assist such agency in verifying, correcting, and/or purging the information in question.

Information Retention and Destruction

All criminal intelligence information, as that term is defined in 28 CFR § 23.3, shall be reviewed for record retention in accordance with 28 CFR Part 23 (at least every five (5) years) and/or as specified by applicable state law pertaining to records retention.

For other information or intelligence, record retention will be established by state law, local ordinance, or in accordance with a retention schedule established by the CFC.

The agency shall remove information when the information has no further value or meets applicable criteria for removal according to 28 CFR Part 23 and/or applicable state records retention schedules.

The CFC shall delete information or return it to the originating agency once its retention period has expired or as otherwise agreed upon with the originating agency in a participation or membership agreement.

Permission to destroy or return information or records will be presumed if in accordance with applicable state retention schedule(s) and will be subject to review by the CFC Privacy and Civil Liberties Officer.

The CFC shall notify the submitting agency at least 30 days prior to the validation/purge date of all information contained in a criminal intelligence

information system. The CFC shall notify the submitting agency of all information that has been purged from a criminal intelligence information system maintained by the CFC. The CFC may notify originating agencies of proposed destruction or return of records not contained in a criminal intelligence information system but is not required to do so unless such notification is mandated by agreement with the originating agency.

A record that information has been purged or returned shall be maintained by the CFC.

Security Safeguards

The CFC Security Officer is designated by the CFC Director and shall be trained to serve as the CFC Security Officer. The CFC Security Officer has primary responsibility for ensuring the security of CFC data and information systems.

The CFC will comply with generally accepted industry or other applicable standards for security, in accordance with MSP and CFC Security Policies and Procedures. Security safeguards will cover any type of medium (printed and electronic), or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related CFC activity.

The CFC shall use software, information technology tools, and physical security measures that protect information from unauthorized access, modification, theft, or sabotage. The CFC shall only use information systems that can withstand most manmade and natural disasters without risking alteration or destruction of data. The security methods and techniques used shall be consistent with the National Criminal Intelligence Sharing Plan and 28 CFR Part 23.

The CFC will operate in secure facilities 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.

The CFC shall secure tips, leads, and SAR information in a 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.

The CFC shall store information so that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.

Access to CFC information will be granted only to center personnel whose positions and job duties require such access; who have successfully completed a background check and possess an appropriate security clearance, if applicable; and who have been selected, approved, and trained accordingly.

Queries made to CFC data applications shall be logged into the data system identifying the user initiating the query. The CFC shall utilize database audit

mechanisms to track all types of information accessed, requested, and disseminated.

Risk and vulnerability assessments shall be stored separately from publicly available data to prevent public records disclosure.

All CFC personnel shall immediately report a suspected or confirmed breach of CFC data to the CFC Security Officer, the CFC Privacy and Civil Liberties Officer, and the CFC Director. The CFC will follow the data breach notification guidance set forth in M. G. L. ch. 93H, §1 *et seq*. (Security Breach/Personal Information).

To the extent required by M. G. L. ch. 93H, §1 *et seq*., the CFC shall immediately notify originating agencies when a suspected or confirmed data breach might have involved data that originated from their agency.

Accountability and Enforcement

The Commonwealth Fusion Center Privacy, Civil Rights, and Civil Liberties Policy shall be made available upon request and posted on the Massachusetts State Police website.

The CFC Privacy and Civil Liberties Officer, in consultation with the CFC Director, shall be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the CFC's information system.

The CFC shall adopt and follow procedures and practices by which it can ensure and evaluate compliance with the provisions of this policy and applicable law. This will include logging access to CFC systems and periodic random auditing of these systems. A compliance verification review shall be completed at least annually, and the Privacy and Civil Liberties Officer shall author an annual report regarding compliance with this policy. Privacy and Civil Liberties Officer shall provide the annual compliance report to the CFC Director.

The CFC Privacy and Civil Liberties Officer shall provide an electronic copy of this policy to all CFC personnel and non-CFC personnel assigned to the CFC. The CFC shall require written acknowledgment of receipt of this policy and agreement to comply with applicable provisions.

The CFC shall annually conduct audits and inspections of any information and intelligence contained in a criminal intelligence database maintained by the CFC. The audits shall be conducted randomly by a designated representative of the CFC. The audits shall be conducted in such a manner that the confidentiality, sensitivity, and privacy of CFC information is protected.

CFC personnel shall report suspected or confirmed violations of CFC policies relating to protected information to the CFC Privacy and Civil Liberties Officer and the CFC Director. Suspected or confirmed violations shall be reported regardless of whether the violation was intentional or unintentional.

If an individual is determined to have violated the provisions of this policy, the following action(s) may be taken:

- the individual's access to CFC information may be suspended or terminated;
- the individual may be suspended, demoted, transferred, or terminated, as permitted by applicable personnel policies and/or collective bargaining agreements;
- the individual may be subject to other sanctions or administrative actions as provided in agency personnel policies and/or collective bargaining agreements;
- the CFC may request the individual's employer to initiate disciplinary proceedings and/or mandate that the individual adhere to the provisions of this policy; or,
- if appropriate, the CFC may refer the matter to appropriate authorities for criminal/administrative investigation and possible criminal prosecution.

The CFC reserves the right to suspend or withhold service and/or deny access to any individual or participating agency that violates this policy.

An audit mechanism shall be available to identify all persons who have accessed or disseminated CFC database information. This audit mechanism shall be sufficient to allow for the identification of every individual who has accessed or disseminated a particular piece of information retained in CFC databases that are actively managed.

Training

To the maximum extent feasible, the CFC shall require the following individuals to participate in annual training regarding the implementation of and adherence to this policy:

- CFC personnel and non-CFC personnel assigned to the CFC.

Annual training shall include instructions on:

- The purpose of the Commonwealth Fusion Center Privacy, Civil Rights, and Civil Liberties Policy.
- The substance, intent, and implementation of the provisions of the Commonwealth Fusion Center Privacy, Civil Rights, and Civil Liberties Policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the CFC.
- Originating and participating agency responsibilities and obligations under applicable law and policy.
- Mechanisms for reporting violations of the Commonwealth Fusion Center Privacy, Civil Rights, and Civil Liberties Policy.
- Potential negative effects that could result from violations of the Commonwealth Fusion Center Privacy, Civil Rights, and Civil

Liberties Policy.

- How to identify, report, and respond to a suspected or confirmed data breach.
- Possible penalties for violations of the Commonwealth Fusion Center Privacy, Civil Rights, and Civil Liberties Policy.
- Legal updates related to privacy, civil rights, and civil liberties.
- ISE Core Awareness Training.

The CFC Director reserves the right to require any CFC employee or authorized user to attend appropriate training.

Official:
Maj. Eric J. Benson #3389

APPENDIX A
(Primary Terms & Definitions)

28 CFR Part 23 – United States Department of Justice regulation that governs federally funded, multijurisdictional criminal intelligence systems. The regulation applies, as a matter of law, to state, local, tribal, or territorial agencies if they are operating interjurisdictional or multijurisdictional criminal intelligence systems that are supported with Omnibus Crime Control and Safe Streets Act funding (See 28 CFR § 23.3). The operating principles of 28 CFR Part 23 provide guidance regarding how to operate criminal intelligence information systems effectively while safeguarding privacy and civil liberties. The regulation mandates a reasonable suspicion standard for collecting information on individuals involved in criminal activity, restricts collecting data on political or religious views, and requires regular review and purging of outdated or unreliable information. It addresses five main areas: submission/entry, security, inquiries, dissemination, and review/purge.

Access – Information access is the ability of an individual to navigate to particular information on a computer or in a computer system. Web access means having a connection to the internet through an access provider or an online service provider.

Agency – See Originating Agency, Participating Agency, or Source Agency.

Analysis (law enforcement) – The review of information and its comparison to other information to determine its meaning in reference to a criminal investigation or assessment.

Assessment – An estimate, evaluation, or appraisal of information and its possible impact.

Audit Mechanism – A computer database feature that provides a comprehensive chronological record of all activities and transactions within a digital system, documenting who did what, when, and how. Its purpose is to provide a tamper-proof history for accountability, enable investigation of security breaches or system issues, and satisfy regulatory compliance by ensuring data integrity and transparency.

Authentication – The process of validating the credentials of a person, computer process, or 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 usernames and passwords.

Authorization – The process of granting a person, computer process, or device with access to certain information, services, or functionality. Authorization is verified through authentication.

Civil Liberties – Civil liberties are fundamental personal freedoms that protect individuals from improper government action and arbitrary governmental interference. Civil liberties are freedoms that are guaranteed by the Constitution of the United States, particularly the Bill of Rights. Civil liberties include freedom of speech, press, and religion. Civil liberties are freedoms from government action, while civil rights are actions the government must take to ensure equal treatment and opportunity.

Civil Rights – Civil rights are legal guarantees of fair treatment and protection from discrimination. Civil rights are actions the government must take to ensure equal treatment and opportunity for all people. Civil rights largely stem from federal laws, such as the Civil Rights Acti of 1964. Civil rights focus on protecting groups and individuals from discrimination based on factors such as race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, or other characteristics unrelated to the worth of the individual. Protection of civil rights means that government entities will take action to ensure that individuals are not discriminated against on the basis of any federal or state protected characteristic. Civil rights include the right to vote, access to public facilities, and equal employment opportunities. Civil rights are actions the government must take to ensure equal treatment and opportunity, while civil liberties are freedoms from government action.

Classification – A rating given to stored information.

Confidentiality – Confidentiality is closely related to but is not synonymous with privacy. It refers to 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.

Credentials – Proof of identification that is used to gain access to computer systems and resources. Examples of credentials are usernames, passwords, smart cards, and certificates.

Criminal Intelligence Information or Data – Information and data about individuals and organizations suspected of criminal activity. The information must meet at least a reasonable suspicion standard to be collected and maintained. Criminal intelligence information must be maintained in accordance with 28 CFR Part 23.

Data Breach – The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or other protected information, or (2) an authorized user accesses or potentially accesses PII or other protected information for a purpose other than the authorized purpose. Data breaches may include, but are not limited to, incidents such as:

- Theft or loss of unencrypted digital media (laptop computers, hard drives, USB drives, etc.) containing PII or other protected information.
- Unauthorized employee access to information containing PII or other protected information.
- Moving information containing PII or other protected information to a computer that is accessible from the internet without first taking proper information security precautions.
- Intentional or unintentional transfer of information containing PII or other protected information to a system that is not appropriately accredited for security at the approved level, such as unencrypted email.
- Transfer of information containing PII or other protected information to the information systems of a possibly hostile agency or an environment where it may be exposed to more intensive decryption techniques.

Data Protection – 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 PII or other protected information to an individual, agency, or organization outside the agency that collected the information. Although disclosure and dissemination are similar concepts, disclosure typically refers to the release of sensitive and protected information to an individual or entity upon request or out of obligation, while dissemination typically refers to the release of information in the course of day-to-day operations for the benefit of public safety/law enforcement.

Dissemination – The transmission of criminal intelligence or information orally, in writing, electronically, or by any other means, from the person having custody of the intelligence or information to another person. Although dissemination and disclosure are similar concepts, dissemination typically refers to the release of information in the course of day-to-day operations for the benefit of public safety/law enforcement, while disclosure typically refers to the release of sensitive and protected information to an individual or entity upon request or out of obligation.

Electronically Maintained – Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer. Electronic mediums include but are not limited to: electronic memory chips, magnetic tape, magnetic disks, CD/DVDs, USB drives, hard drives, or cloud storage technologies.

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 by transmission over the internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, and/or faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voicemail.

Evaluation – An assessment of the reliability of the source and the accuracy of the raw data.

Fair Information Practice Principles (FIPPs) – FIPPs are a set of eight internationally recognized principles that inform information privacy policies in both the public and private sector. Because of operational necessity, it may not always be possible to apply all eight FIPPs principles equally. The following are the eight FIPPs principles that fusion centers and other integrated justice systems should endeavor to apply where practicable:

1. Purpose Specification
2. Data Quality/Integrity
3. Collection Limitation/Data Minimization
4. Use Limitation
5. Security Safeguards
6. Accountability/Audit
7. Openness/Transparency
8. Individual Participation

Fusion Center – A collaborative effort of two or more federal, state, local, tribal, or territorial (SLTT) government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal and terrorist activity. State and major urban area fusion centers serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and both SLTT and private sector partners.

Homeland Security Information – 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.

Information Quality – Information quality refers to various aspects of information: the accuracy and validity of the actual values of the data, data structure, and database/data repository design. The basic elements of information quality have traditionally been identified as accuracy, completeness, currency, reliability, and context/meaning. The definition of information quality is evolving and expanding to include considerations of accessibility, security, and privacy.

Information Sharing Environment (ISE) – The ISE is a conceptual framework composed of the policies, procedures, and technologies linking the resources (people, systems, databases, and information) of SLTT agencies, federal agencies, and the private sector to facilitate terrorism-related information sharing, access, and collaboration.

Information Sharing Environment (ISE) Suspicious Activity Report (SAR) (ISE-SAR) – A SAR that has been determined to have a potential nexus to terrorism or other criminal activity (i.e., to be reasonably indicative of criminal activity associated with terrorism or other criminal activity)

Intelligence – Information that has been processed (i.e., collected, evaluated, collated, analyzed, and reported).

Invalidated Information – A tip or lead (including a SAR) that has been determined to be false or inaccurate or otherwise determined to not warrant additional action and/or maintenance. If additional information is received to warrant further analysis, information that has been deemed invalidated can be re-examined through an analytical process and subsequently deemed validated.

Joint Terrorism Task Forces (JTTFs) – Joint Terrorism Task Forces (JTTFs) are interagency task forces managed by the Federal Bureau of Investigation that are designed to enhance communication, coordination, and cooperation in countering terrorist threats. JTTFs execute the FBI's lead federal agency responsibility for investigating terrorist acts and terrorist threats against the United States.

Law – As used by this policy, law includes any local, state, or federal statute, ordinance, regulation, executive order, policy, or court rule.

Logs – Computer logs are files or records containing information about activities in a computer system. This can include information such as who accessed the system, when it was accessed, what files were opened, and what changes were made. Logs are important for keeping track of user activity, ensuring adequate security, and troubleshooting computer systems.

Need-to-Know – An individual has a need-to-know sensitive information or intelligence if the information is necessary for them to conduct their official duties as part of an organization that has a right-to-know the information.

Originating Agency – The agency or organizational entity that analyzes, documents, disseminates, and/or publishes information or data that is collected by a source agency. In some circumstances the originating agency and the source agency may be the same. (e.g., if Townville PD sends a missing person report to the CFC and the CFC incorporates information from that report into a bulletin for distribution to CFC partners, Townville PD would be the Source Agency and the CFC would be the Originating Agency for that information. See below for Source Agency definition.)

Participating Agency – An agency or organizational entity that is authorized to access receive, and/or use fusion center information and/or databases through its authorized individual users.

Personal Information – Personal Information is defined in M.G.L. ch. 93H, §1 as an individual's first and last name or first initial and last name in combination with any one or more of the following data elements that relate to the individual:

(a) Social Security number;

(b) driver's license number or state-issued identification card number; or

(c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Personally Identifiable Information – Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information, that is linked or linkable to a specific individual.

Privacy – Privacy refers to individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable information, including records that can be accessed by or are attached to an individual's personally identifiable information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the capacity to be physically left alone; to be free from physical interference, threat, or unwanted touching; or to avoid being seen or overheard in particular contexts.

Privacy, Civil Rights, and Civil Liberties Policy – A privacy, civil rights, and civil liberties policy is a written, published statement that articulates an organization's policy on the handling of records that contain personally identifiable information. The policy is likely to be informed by the Fair Information Practice Principles (FIPPs) and should include procedures relating to information collection, analysis, maintenance, dissemination, and access. The purpose of a privacy, civil rights, and civil liberties policy is to articulate that the agency/center will adhere to those legal requirements and agency/center policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests.

Privacy Protection – A process of maximizing the protection of privacy, civil rights, and civil liberties when collecting and sharing information.

Protected Information – Protected information is information about individuals or organizations that is subject to information privacy or other protections by law or regulation. Protection may be extended to other individuals and organizations by fusion center or originating/participating/source agency policy.

Public – The public includes all persons, media outlets, and for-profit or nonprofit entities, organizations, and associations. The public also includes any governmental entity for which there is no existing specific law authorizing access to CFC information.

The public does not include personnel assigned to the CFC, persons or entities that assist the CFC in the operation of the justice information system, and public agencies whose authority to access information gathered and retained by the CFC is specified in law.

Public Access – Information that is not subject to privacy interests or rights and can be viewed by the public.

Purge – A term that is commonly used to describe methods that destroy data in a manner that prevents it from being recovered. Purging data is different than deleting data. Deleting data makes the data inaccessible except to system administrators or other privileged users, while purging data completely destroys/erases the data.

Reasonably Indicative – The reasonably indicative standard is met when observed behavior, when considered in context by a reasonable person, creates an articulable concern that the behavior may indicate preoperational planning associated with terrorism or other criminal activity. When the reporting party is a law enforcement officer, this standard takes into account the training and experience of a reasonable law enforcement officer. Information documented in a SAR must meet this standard.

Redress – Internal procedures to address complaints from individuals regarding protected information that pertains to them and is under the CFC's control.

Retention – ***(Refer to Storage)***

Right-to-Know – A requirement for access to specific information to assist in a lawful and authorized governmental function. Right-to-know is determined by the mission and functions of a law enforcement, homeland security, counterterrorism, or other lawful and authorized government activity. Right-to-know is also determined by the roles and responsibilities of particular personnel in the course of their official duties.

Right to Information Privacy – The legal and ethical right of individuals to control their personal information and determine who can collect, use, and share their information. This right applies unless a legal or reasonable public interest exists that warrants collecting, accessing, retaining, and disseminating information about an individual's activities.

Security – Security refers to 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 also aims to ensure the accuracy and timely availability of data for the legitimate user set and promote failure resistance in electronic systems overall.

Source Agency – Source agency refers to the agency or entity that reports suspicious activity or other information to the CFC (examples include a local police department, a private

security firm handling security for a power plant, and a security force at a military installation). In some circumstances the originating agency and the source agency may be the same.

Storage: In the context of the ISE, storage (or retention) refers to the storage and safeguarding of terrorism-related information – including 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.

Suspicious Activity – Observed behavior reasonably indicative of preoperational planning associated with terrorism or other criminal activity. Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyber-attacks, testing of security, expressed-implied threats, etc.

Suspicious Activity Report (SAR) – Documentation of observed behavior reasonably indicative of preoperational planning associated with terrorism or other criminal activity. Suspicious activity reports are 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 – According to Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), terrorism information is all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign/international terrorist groups/individuals, or domestic groups/individuals involved in transnational terrorism; (b) threats posed by such groups/individuals to the United States, United States persons, United States interests, or interests of other nations; (c) communications of or by such groups/individuals; or (d) other groups/individuals reasonably believed to be assisting or associated with such groups/individuals.

Terrorism-related Information – In accordance with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended by the 9/11 Commission Act (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 the 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 may include intelligence information.

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. SAR information should be viewed, at most, as a subcategory of tips or leads information. Tips and leads information does not include criminal history records or incidents that do not have a criminal offense attached or indicated. Tips and leads information should be maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

Unvalidated information – A tip or lead (including a SAR) received by the CFC that has not yet been reviewed to determine further action or maintenance, or information undergoing an analytical process that has not yet determined to be validated or invalidated information.

User – An individual representing a participating agency who is authorized to access, receive, and/or use the CFC's information, information databases, and/or resources for lawful purposes.

U.S. Persons – A "U.S. person" is generally defined as a United States citizen, a United States permanent resident alien, an unincorporated association substantially composed of United States citizens and/or permanent resident aliens, or a United States corporation.

Validated Information – A tip or lead (including a SAR) that has been thoroughly evaluated and confirmed for accuracy, reliability, and relevance. Validated information has passed through a rigorous process of verification and analysis to ensure it is trustworthy and fit for its intended use. If additional information is received to warrant further analysis, information that has been deemed validated can be re-examined through an analytical process and subsequently deemed invalidated.