



Commonwealth Fusion Center Standard Operating Procedure

Effective Date	Number
July 1, 2006	CFC - 05

Subject:
Commonwealth Fusion Center Privacy Policy

Purpose

The primary goal of the Commonwealth Fusion Center (CFC) is to facilitate the gathering and sharing of information across the public safety spectrum. Integral to this effort is the realization that the privacy concerns of individuals and issues of data quality must be balanced against the intelligence and information sharing goals of the CFC.

The purpose of this policy is to ensure safeguards and sanctions are in place to protect personal information as information and intelligence are developed and exchanged. It is the policy of the CFC to protect the legitimate privacy concerns of citizens while conducting its mission.

Fair Information Practices

This policy embraces the eight Privacy Design Principles developed by the Organization of Economic Cooperation and Development's *Fair Information Practices* and shall be used to guide the policy wherever applicable. The eight Privacy Design Principles are:

1. **Purpose Specification-** Define agency purposes for information to help ensure agency uses of information are appropriate.
2. **Collection Limitation-** Limit the collection of personal information to that required for the purposes intended.
3. **Data Quality-** Ensure data accuracy.
4. **Use Limitation-** Ensure appropriate limits on agency use of personal information.
5. **Security Safeguards-** Maintain effective security over personal information.
6. **Openness-** Promote a general policy of openness about agency practices and policies regarding personal information.
7. **Individual Participation-** Allow individuals reasonable access and opportunity to correct errors in their personal information held by the agency.
8. **Accountability-** Identify, train, and hold agency personnel accountable for adhering to agency information quality and privacy policies.

Purpose Specification

CFC personnel have developed databases by using existing data sources from participating entities to integrate data with the goal of identifying, developing, and analyzing information and intelligence related to terrorist activity and other crimes for investigative leads. This capability will facilitate integration and exchange of information between the participating agencies.

CFC intelligence products and services will be made available to law enforcement and criminal justice agencies, and homeland security entities. All agencies who contribute staff to the CFC will be subject to a Memorandum of Understanding and will be required to adhere to all CFC policies and security requirements.

CFC personnel develop information and intelligence provided by participating agencies. Collection of personal information will be limited to that data necessary for the information sharing and intelligence purposes for which it is intended.

**Collection
Limitation**

Limitations on the collection of data concerning individuals are the responsibility of the collector of the original source data. Each contributor of information is to abide by the collection limitations applicable to it by reason of law, rule, or policy.

Data Quality

The CFC is committed to protecting individual privacy through policies, procedures, and business processes that ensure data accuracy. Participating agencies remain the owners of the data contributed and are, therefore, responsible for the quality and accuracy of the data accessed by the CFC. Inaccurate personal information can have a damaging impact on the person concerned and on the integrity and functional value of the CFC, and any information obtained through the CFC must be independently verified with the original source from which the data was extrapolated before any official action (e.g., warrant or arrest) is taken. User agencies and individual users are responsible for compliance with respect to use and further dissemination of such information and the purging and updating of the data.

Use Limitation

Information obtained from or through the CFC can only be used for lawful purposes. A lawful purpose means the request for data can be directly linked to a law enforcement agency's active criminal investigation or is a response to a confirmed lead that requires follow-up to prevent a criminal act.

CFC personnel will take necessary measures to make certain that access to the CFC's information and intelligence resources is secure and will prevent any unauthorized access or use. The CFC reserves the right to restrict the qualifications and number of personnel allowed access and to suspend or withhold service to any individual violating this policy. The CFC further reserves the right to conduct audits concerning the proper use and security of the information received from the CFC.

**Security
Safeguards**

Security for information derived from the CFC will be provided in accordance with applicable laws, rules, and regulations. Furthermore, all personnel who receive, handle, or have access to CFC data and/or sensitive information will be trained as to those requirements. All personnel having access to the CFC's data agree to abide by the following rules:

1. The CFC's data will be used only to perform official law enforcement investigative-related duties in a manner authorized by the user's employer.
2. Individual passwords will not be disclosed to any other person except as authorized by agency management.
3. Individual passwords will be changed if authorized personnel of the agency or CFC personnel suspect the password has been improperly disclosed or otherwise compromised.

-
4. Background checks will be completed on personnel who will have direct access to the CFC.
 5. Use of the CFC's data in an unauthorized or illegal manner will subject the user to denial of further use of the CFC and/or criminal prosecution.

Each authorized user understands that access to CFC data can be denied or rescinded for failure to comply with the applicable restrictions and use limitations.

Information obtained from or through the CFC will not be used or publicly disclosed for purposes other than those specified in the Memorandum of Understanding that each participating agency must sign. Information cannot be (1) sold, published, exchanged, or disclosed for commercial purposes; (2) disclosed or published without prior approval of the contributing agency; or (3) disseminated to unauthorized persons.

Use of the CFC's data is limited to those individuals who have been selected, approved, and trained accordingly. Access to information contained within the CFC will be granted only to law enforcement agency personnel who have successfully passed a criminal background check, as attested to by their agency head. Each individual user must complete an Individual User Agreement in conjunction with training.

CFC personnel shall take every possible and responsible action to maintain confidentiality and to secure personal information they may encounter in the course of their duties.

Openness

It is the intent of the participating agencies to be open with the public concerning data collection practices when such openness will not jeopardize ongoing criminal investigative activities. Participating agencies will refer citizens to the original collector of the data as the appropriate entity to address any concern about data accuracy and quality, when this can be done without compromising an active inquiry or investigation.

All agencies participating in the CFC will make this privacy policy available for public review. The CFC will make this policy available to any interested party upon request.

Individual Participation

The data maintained by the CFC is provided, on a voluntary basis, by the participating agencies or is information obtained from other sources by the CFC. Each individual user searching against the data as described herein will be required to acknowledge that he or she remains solely responsible for the interpretation, further dissemination, and use of any information that results from the search process. Additionally, he or she is responsible for ensuring that any information relied upon is accurate, current, valid, and complete, especially before any official action is taken in full or partial reliance upon the information obtained.

Members of the public cannot access individually identifiable information, on themselves or others, from the CFC's applications. Persons wishing to access data pertaining to themselves should communicate directly with the agency or entity that is the source of the data in question.

Participating agencies agree that they will refer requests related to privacy or sunshine laws back to the originator of the information.

Accountability

When a query is made to any of the CFC's data applications, the original request is automatically logged by the system identifying the user initiating the query. When such information is disseminated outside of the agency from which the original request is made, a secondary dissemination log must be maintained by both the CFC and the originating agency in order to correct possible erroneous information and for audit purposes, as required by applicable law. Secondary dissemination of information can only be to a law enforcement agency for a law enforcement investigative purpose, or to other agencies as provided by law. This record will reflect as a minimum:

1. Date of release.
2. To whom the information relates.
3. To whom the information was released (including address and telephone number).
4. An identification number or other indicator that clearly identifies the data released.
5. The purpose for which the information was requested.

The CFC Security Officer will be responsible for conducting or coordinating audits and investigating misuse of the CFC's data or information. All violations and/or exceptions shall be reported to the CFC Director. Individual users of the CFC's information remain responsible for their legal and appropriate use of the information contained therein. Failure to abide by the restrictions and use limitations for the use of the CFC's data may result in the suspension or termination of use privileges and/ or criminal prosecution. Each user and participating agency in the CFC is required to abide by this policy in the use of information obtained by and through the CFC.

References

M.G.L. c.22C §38 – Criminal Information Section; Duties and Functions
Organization of Economic Cooperation and Development's *Fair Information Practices*
28 CFR Part 23 – Criminal Intelligence Systems
Justice Information Privacy Guideline -National Criminal Justice Association
