Model Policy

Privacy Policy

D R A F T

Table of Contents

Section 1: Purpose

The _____ has developed an intelligence fusion center whose services will be made available to law enforcement agencies via user authentication based on user roles, through stand-alone workstations specifically designed for accessing the fusion center databases. All access will be provided through secure law enforcement network connectivity. The fusion center project was initiated in response to the increased need for timely information sharing and exchange of crime-related information among members of the law enforcement community.

Fusion Center Databases

The center has developed databases by using existing data sources to integrate disparate data from many types of storage systems to identify, develop, and analyze information related to terrorist activity and other crimes for investigative leads. This capability will facilitate integration and exchange of information between the participating agencies, including criminal history, driver license data, vehicle registration records, and incarceration/corrections records with significant amounts of public data record entries. None of the data sources accessed are recognized as intelligence databases as defined by the criminal intelligence systems operating policies contained in 28 CFR Part 23. The use of data from existing data nonintelligence sources will save countless investigative hours and significantly improve the opportunity for successful conclusion of investigations.

Section 2: Collection Limitation

The Fusion Center is maintained for the purpose of sharing information by agencies participating in the project. The center operates applications that contain copies of the original source data provided by other systems, periodically refreshed, in an efficient and automated environment. The decision of the agencies to participate in the center and about which databases to provide is voluntary and will be governed by the laws and rules governing the individual agencies respecting such data, as well as by applicable federal law such as the Driver's Privacy Protection Act of 1994.

Because the laws, rules, or policies governing information that can be collected and released on private individuals will vary from agency to agency, limitations on the collection of data concerning individuals is 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. Information contributed to the center should be that which has been collected in conformance with those limitations.

Section 3: Data Quality

The agencies participating in the center remain the owners of the data contributed and are, therefore, responsible for the quality and accuracy of the data accessed by the center.

Inaccurate personal information can have a damaging impact on the person concerned and on the integrity and functional value of the center. In order to maintain the integrity of the center, any information obtained through the center 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.

Section 4: Use Limitation

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

The Executive Board of the Fusion Center will take necessary measures to make certain that access to the center's information and intelligence resources are secure and will prevent any unauthorized access or use. The Board reserves the right to restrict the qualifications and number of personnel who will be accessing the center and to suspend or withhold service to any individual violating this *Privacy Policy*. The Board, or persons acting on behalf of the Board, further reserves the right to conduct inspections concerning the proper use and security of the information received from the center.

Security for information derived from the center will be provided in accordance with applicable laws, rules, and regulations. Furthermore, all personnel who receive, handle, or have access to criminal history records or other sensitive information will be trained as to those requirements.

All personnel having access to the center's data agree to abide by the following rules:

(a) The center's data will be used only to perform official law enforcement investigative-related duties in a manner authorized by the user's employer.

(b) Individual passwords will not be disclosed to any other person except as authorized by agency management.

(c) Individual passwords will be changed if authorized personnel of the agency or members of the center suspect the password has been improperly disclosed or otherwise compromised.

(d) Background checks will be completed on personnel who will have direct access to the center.

(e) Use of the center's data in an unauthorized or illegal manner will subject the user to denial of further use of the center, discipline by the user's employing agency, and/or criminal prosecution.

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

Section 5: Security Safeguards

Information obtained from or through the center 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 center's data is limited to those individuals who have been selected, approved, and trained accordingly. Access to information contained within the center will be granted only to law enforcement agency personnel who have been screened with a state and national fingerprint-based background check, as well as any additional background screening processes using procedures and standards established by the Fusion Center Executive Board of Directors. Each individual user must complete an Individual User Agreement in conjunction with training provided by a certified center trainer.

Access to the center's databases from outside of the center will only be allowed over secure network lines.

Section 6: 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 (e.g., a participating state's motor vehicle department) 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 center will make this *Privacy Policy* available for public review or to any interested party. The center will post this *Privacy Policy* on its public Web site and make it available to any interested party.

Section 7: Individual Participation

The data maintained in the center's data applications is provided, on a voluntary basis, by the participating agencies or is information obtained from other sources by the center. The data is made available "as-is" and is not to be viewed as necessarily accurate, complete, or current until verified with the original source. The process of using each contributor's data against the information contained in the center's databases will involve comprehensively comparing and cross-referencing the former for any matches, similarities, or points of commonality with the latter, without limitation or restriction as to the kind or quantity of information thereby derived or produced.

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 which results from the search process and is responsible for assuring 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 center'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. For example, each participating agency must provide a means for an individual to review and challenge the accuracy and completeness of his or her criminal history record, as authorized and required by 28 CFR section 20.21(g).

Section 8: Accountability

When a query is made to any of the center'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 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 provide by law. The agency *from* which the information is requested will maintain a record (log) of any secondary dissemination of information when it includes criminal history information, personal information obtained in connection with a motor vehicle record as defined in 18 U.S.C. section 2721 (Driver's Privacy Protection Act), or data designated by the Board, for at least five years. This record will reflect as a minimum:

(a) Date of release;
(b) To whom the information relates;
(c) To whom the information was released (including address and telephone number);
(d) The State Identification (SID) and/or the FBI number(s) or other information that clearly identifies the data released; and
(e) The purpose for which the information was requested.

Original source data must be used for any official action. Such records will be maintained for a minimum of five years for audit purposes to ensure compliance with this *Privacy Policy* and with other applicable laws, policies, and regulations. The Executive Board will be responsible for conducting or coordinating audits and investigating misuse of the center's data or information. All violations and/or exceptions shall be reported to the Board.

Individual users of the center'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 center's data may result in the suspension or termination of use privileges, discipline sanctions imposed by the user's employing agency, or criminal prosecution. Each user and participating agency in the center is required to abide by this *Privacy Policy* in the use of information obtained by and through the center.