United States
Department of Justice

Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise

A collaborative effort between the U.S. Department of Justice's Global Justice Information Sharing Initiative and the DHS/DOJ Fusion Process Technical Assistance Program and Services

June 2010

About the Document

The *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise*, developed by the U.S. Department of Justice's Global Justice Information Sharing Initiative, assists law enforcement agencies in determining whether they are in compliance with applicable privacy-related policies, procedures, rules, and guidelines.

Background: The extensive growth of intelligence and information sharing has brought a renewed emphasis on the importance of protecting privacy, civil rights, and civil liberties. Compliance reviews and audits have become a necessary tool for agencies to use in order to identify high-risk operational and management issues dealing with privacy, civil rights, and civil liberties, particularly with the recent development of fusion centers. This resource was developed to assist intelligence enterprises with ensuring compliance with all applicable privacy, civil rights, and civil liberties protection laws, regulations, and policies while sharing intelligence and information needed to safeguard America.

Value to the Justice Community: Agencies should use this resource to conduct periodic assessments of their intelligence enterprise. These assessments will assist in determining whether agency policies and procedures comprehensively address and implement privacy, civil rights, and civil liberties protections. The product from such an assessment will assist law enforcement agencies in identifying weaknesses and gaps in their protections policies and procedures.

Contents: The document includes a suggested methodology for conducting the review of an agency's intelligence enterprise and identifies the high-liability areas of concern that should be included when performing the review. The document also contains a suggested list of questions to answer when conducting the compliance process but may not cover all laws, policies, and procedures that are applicable to a particular state or agency. Agencies are encouraged to add questions or enhance sections to include questions/items that may be applicable to their particular jurisdiction's rules, standards, or policies, thereby making certain that the verification is comprehensive for their intelligence enterprise.

Target Audience: The target audience for the resource is local, state, and tribal law enforcement agencies with an intelligence enterprise or fusion center.

Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise

June 2010

To request a Word version of Section 1 and 2, please submit your request to GLOBAL@iir.com.

About Global

The U.S. Department of Justice's Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee to the U.S. Attorney General on critical justice information sharing initiatives. Global promotes standards-based electronic information exchange to provide justice and public safety communities with timely, accurate, complete, and accessible information in a secure and trusted environment. Global is administered by the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance.

This project was supported by Grant No. 2008-DD-BX-K520 awarded by the Bureau of Justice Assistance, Office of Justice Programs, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative and the U.S. Department of Homeland Security. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice or the U.S. Department of Homeland Security.

Contents

Introduction

The Importance of Privacy, Civil Rights, and Civil Liberties Protections

In recent years, intelligence and information sharing has grown considerably among law enforcement and homeland security professionals nationally. These core processes underpin effective strategies aimed at safeguarding our country from criminal and terrorist threats, as well as other hazards that affect our society. Nevertheless, as the adoption of intelligence and information sharing grows, so must the importance of protecting the privacy, civil rights, and civil liberties of our citizens. A key step for agency leadership in ensuring that these protections are imbedded in their agency is to undergo a compliance verification process to review and assess the business practices of the agency's intelligence enterprise. This internal process will help identify weaknesses and gaps in the protection of privacy, civil rights, and civil liberties.[1]

Agencies undergo a compliance verification process to review and assess the business practices of the agency's intelligence enterprise. This internal process will help identify weaknesses and gaps in the protection of privacy, civil rights, and civil liberties.

For law enforcement professionals, the standards required by the Criminal Intelligence Systems Operating Policies federal regulation (28 CFR Part 23)[2] once served as the sole guideline for ensuring that the privacy and constitutional rights of individuals are protected during the collection and exchange of criminal intelligence information. The regulation specifically provides guidance to law enforcement agencies in five primary areas—submission and entry of criminal intelligence information, secure storage, inquiry, dissemination, and the review-and-purge process. The *National Criminal Intelligence Sharing Plan* (NCISP)[3] establishes 28 CFR Part 23 as the de facto national standard by recommending that law enforcement agencies adopt, at a minimum, 28 CFR Part 23 to help ensure that the submission, access, storage, and dissemination of criminal intelligence information conform to the privacy and constitutional rights of individuals, including the groups and organizations to which they may belong. Yet, as the policing environment has rapidly expanded from daily "calls for service" and crime prevention activities to now include safeguarding critical infrastructure and key

1 Though the compliance verification process identified in this document is intended for use by law enforcement agencies and entities that have an intelligence function, the concept of the assessment may possibly be expanded for other parts of the criminal justice system. Additionally, as intelligence enterprises use the document to internally assess their systems and processes, they should be cognizant of the intelligence sharing protocols in place for sharing with all criminal justice entities, including corrections, probation and parole, and prosecutors.

2 Additional information on Criminal Intelligence Systems Operating Policies is available at http://www.iir.com/28CFR/pdf/ecOrder12291_28CFRPart23.pdf.

3 The *National Criminal Intelligence Sharing Plan* is available at http://www.it.ojp.gov/documents/NCISP_Plan.pdf.

resources (CIKR) from the threats of terrorism, sharing information to aid in the prevention of widespread flu pandemics, or exchanging intelligence to assist with preparations for and the aftereffects of a natural disaster, 28 CFR Part 23 by itself does not address all the nuances inherent to practicing intelligence and information sharing in this homeland security environment. What is needed is a process to examine all the "intelligence-related" functions of an agency that go beyond the tenets of 28 CFR Part 23 in ensuring the protection of individuals' privacy and constitutional rights.

The NCISP recommends that law enforcement agencies' chief executive officers "ensure that individuals' privacy and constitutional rights are considered at all times" when performing the intelligence function within an agency. Moreover, the *National Strategy for Information Sharing* (NSIS)[4] recognizes that the need to protect the rights of Americans is a core facet of national information sharing efforts. These fundamental concerns, coupled with the expansion of intelligence enterprises nationally, both in numbers and in scope, have highlighted the importance of additional guidance in terms of addressing intelligence and information sharing for law enforcement and homeland security professionals. Agencies should consider implementing policies that not only incorporate the tenets of 28 CFR Part 23 for criminal intelligence information but also offer broader guidance that will ensure that privacy, civil rights, and civil liberties are protected for all information and intelligence sharing. Once these policies are adopted, agencies must implement them agencywide through appropriate training and practice. As a part of the implementation effort, agencies are encouraged to conduct a periodic self-assessment of their intelligence enterprise in order to determine that their agency policies and procedures covering privacy, civil rights, and civil liberties are being followed, particularly when missions expand or when new partners are added.

Compliance reviews and audits have become a necessary tool for agencies to use in order to identify high-risk operational and management issues, particularly with the recent development of fusion centers. An agency's privacy policy and associated procedures should be transparent, and agency leadership should be accountable for their privacy protection processes in all areas of the intelligence enterprise. To meet this need, the Global Justice Information Sharing Initiative's (Global) Criminal Intelligence Coordinating Council (CICC), Global Intelligence Working Group (GIWG) Privacy Committee has developed the *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise*. This compliance verification will assist intelligence enterprises with ensuring their compliance with all applicable privacy, civil rights, and civil liberties protection laws, regulations, and policies while sharing intelligence and information needed to safeguard America.

4 The *National Strategy for Information Sharing* (NSIS), issued by the White House in 2007, is available at http://georgewbush-whitehouse.archives.gov/nsc/infosharing/NSIS_book.pdf.

Background and Methodology

The GIWG Privacy Committee was formed under the CICC to identify the needs and priorities of law enforcement agencies relating to the protection of citizens' privacy and constitutional rights as agencies perform the intelligence process. The GIWG Privacy Committee and all of Global's working groups continually focus on the development and implementation of policies, templates, and guidance to ensure that these protections are in place in agencies' intelligence enterprises. Therefore, in order to assist agency executives with determining whether their intelligence enterprise is operating in a manner that provides appropriate privacy protections and to recognize the uniqueness of these systems, the GIWG Privacy Committee determined that a template or compliance verification should be developed that can be used to conduct a self-assessment privacy compliance review within a law enforcement agency.

The *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise* can assist agencies in determining whether they are in compliance with applicable policies, procedures, rules, and guidelines. The compliance verification includes a suggested methodology for conducting the review of an agency's intelligence enterprise and identifies the high-liability areas of concern that should be included when performing the review. The document also contains a suggested list of questions to answer when conducting the compliance process but may not cover all laws, policies, and procedures that are applicable to a particular state or agency. Agencies are encouraged to add questions or enhance sections to include questions/items that may be applicable to their particular jurisdiction's rules, standards, or policies, thereby making certain that the verification is comprehensive for their intelligence enterprise.

> Use the *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise* as a self-assessment tool for an intelligence enterprise.

As a part of this initiative, two pilots were conducted at the Florida Fusion Center, a component of the Florida Department of Law Enforcement, and the Georgia Information Sharing and Analysis Center, a component of the Georgia Bureau of Investigation. As a result of these two pilots, the following suggested plan of action was developed to assist agencies as they conduct the compliance verification for their intelligence enterprise.

Agency leadership should remain attentive to other processes and procedures that could affect the intelligence and information sharing environment, such as the pending changes to the Controlled Unclassified Information[5] (CUI) designation currently being undertaken by the federal government. Current efforts include standardizing procedures for designating, marking, and handling CUI information among the different federal agencies.

5 For additional information on Controlled Unclassified Information, please visit http://www.archives.gov/cui/.

Implementation of the CUI Framework should take place within the next five years and will affect the dissemination of information between the federal government and state, local, and tribal agencies.

As part of the national fusion center initiative, the joint DHS/DOJ Fusion Process Technical Assistance Program partnered with Global and the CICC in the development and delivery of the *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise*. As fusion centers develop and implement their privacy protections, it is imperative that a regular examination of the center's operations occur to ensure that the tenets of the privacy protections have been implemented. The *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise* can serve this function by assisting centers in reviewing and assessing their policies and procedures related to privacy, civil rights, and civil liberties protections. As fusion centers undergo the compliance verification process, the DHS/DOJ Fusion Process Technical Assistance Program's Fusion Center Exchange Service provides a valuable opportunity to incorporate peer-to-peer exchanges between centers as they undergo the compliance verification process. This peer-to-peer exchange will help fusion centers ensure that their compliance verification process is comprehensive and it will assist in the identification of any gaps or deficiencies in policies, procedures, and protocols; provide promising practices to mitigate these gaps; and assist in developing a corrective action plan.

How to Use the Privacy, Civil Rights, and Civil Liberties Compliance Verification Tool

The *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise* was designed to be utilized as a self-assessment tool for an intelligence enterprise. It is recommended that random and periodic (at least annual) internal or external compliance verification be conducted on an agency's intelligence enterprise in order to provide the needed transparency as well as guard against punitive ramifications. Individuals conducting the verification should review and assess the business practices of the intelligence enterprise in order to help identify weaknesses and gaps in the protection of privacy, civil rights, and civil liberties. A random sample of data should be reviewed to ensure that the agency's policies and procedures have been implemented and are being followed. The document is divided into two sections. The first section focuses on the intelligence enterprise as a whole, and the second section focuses on the intelligence enterprise's criminal intelligence system. Appendix A provides agencies with a sample method for conducting the compliance verification. Appendix B defines various terms used within the verification document, although some states might have different definitions of the terms used.

There are several different options presented regarding the composition of the compliance verification team. Agency leadership might want to consider a team made up of internal staff members, or they might want to reach out to other intelligence enterprises for assistance—or they could choose to include both internal and external individuals to build the compliance verification team. Recommendations for compliance team members should include subject-matter experts from the security and information technology area, as well as managers

or senior supervisors, and an attorney knowledgeable in privacy, civil rights, and civil liberties laws applicable to intelligence functions.

It is recommended that the compliance verification team request and examine copies of any relevant documents, such as governance legislation, privacy policies/procedures, interagency sharing agreements, and retention policies/procedures. As part of the process, the compliance team should also include interviews with intelligence enterprise managers and employees and user agency representatives and examine random samples of the information being stored and shared.

Once the compliance verification process is completed, agency leadership should examine and analyze any deficiencies that are noted during the verification process and develop a corrective action plan to mitigate these deficiencies. The end result of this comprehensive process is an intelligence enterprise that has broad privacy, civil rights, and civil liberties protections in place through its policies, procedures, and operating guidelines.

Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise

Intelligence Enterprise: _____

Date of Review: _____

Names, Titles, and Contact Numbers of Reviewers: _____

_____

_____

_____

Names, Titles, and Contact Numbers of Employees Interviewed: _____

_____

_____

_____

Overview of the Intelligence Enterprise (attach additional pages if needed):[6] _____

_____

_____

_____

_____

_____

_____

_____

6 The intelligence enterprise overview may include authority(ies), location (state/local agency), crime focus (all-crimes/terrorism-focused), established date, participating agencies, and hours of operation.

Section I: Intelligence Enterprise Operations

This section addresses the intelligence enterprise's overall operation, focusing on how the protection of privacy, civil rights, and civil liberties has been developed and implemented into the enterprise's daily operations.

1. Governance and Authorities

The purpose of the governance area is to determine who has the primary responsibility for the intelligence enterprise's overall operation, including who will ultimately be held accountable for the operation of the intelligence enterprise and for any problems or errors.

a) Enabling legislation or executive order

i) Does the intelligence enterprise have legislation, an executive order, or other authority establishing the center/unit?

_____ State law. Cite: _____

_____ Local ordinance. Cite: _____

_____ Other. Explain: _____

Comments: _____

_____

ii) Does the authority clearly define the goals and scope of the intelligence enterprise?

Yes ____ No ____

Comments: _____

_____

b) Oversight mechanisms (functions)

i) Does the intelligence enterprise have an oversight mechanism?

Internal: Yes ____ No ____

External: Yes ____ No ____

Comments: _____

_____

ii) Does the oversight mechanism have access to conduct a regular review to assess whether privacy policies are being followed?

Yes ____ No ____

Comments: _____

_____

1) If yes, does the oversight mechanism regularly review whether privacy policies are being followed?

Yes ____ No ____ N/A _____

Comments: _____

_____

c) Does the intelligence enterprise have bylaws and/or policies and procedures that are compliant with legal requirements, including but not limited to the U.S. Constitution; the state's constitution; and applicable laws, executive orders, and agency regulations?

Yes ____ No ____

Comments: _____

_____

d) If applicable, do the policies and procedures of the intelligence enterprise provide for a process to assess new and/or revised laws for those issues that pose a significant risk to privacy?

Yes ____ No ____ N/A ____

Comments: _____

_____

2. Privacy, Civil Rights, and Civil Liberties Policy

A privacy, civil rights, and civil liberties policy is a written, published statement that articulates the intelligence enterprise's position on how it handles the personally identifiable information and other personal, sensitive information it seeks or receives and uses in the normal course of business. The purpose of a privacy policy is to articulate within the intelligence enterprise, to external agencies that access and share information with the intelligence enterprise, to other entities, and to the public that the intelligence enterprise will adhere to legal requirements and intelligence enterprise policy and procedural provisions that enable gathering and sharing of information in a manner that protects constitutional rights, including personal privacy and other civil liberties and civil rights. There are legal consequences for violations of citizens' rights, as well as a loss of the public's trust.

a) Does the intelligence enterprise have a written privacy, civil rights, and civil liberties policy?

Yes ____ No ____

Comments: _____

_____

b) Has the policy been approved by an oversight mechanism?

Yes ____ No ____

Comments: _____

_____

i) If yes, what mechanism has approved the policy?

_____ Governance board

_____ Executive order

_____ Legislation

_____ Other (e.g., agency leadership, other advisory bodies)

_____ N/A

Comments: _____

_____

c) If the intelligence enterprise is a fusion center, was the privacy policy submitted for review through the approved Fusion Center Management Group review process?

Yes ____ No ____ N/A ____

Comments: _____

_____

i) If yes, has the policy been determined to be at least as comprehensive as the Information Sharing Environment (ISE) Privacy Guidelines?

Yes ____ No ____ N/A _____

Date of DHS notification to the fusion center: _____

Comments: _____

_____

d) Does the intelligence enterprise's privacy policy include documentation on how the policies and procedures meet the following ISE Privacy Guidelines requirements:

i) Limiting the sharing of information through the ISE to terrorism, homeland security, and law enforcement (terrorism-related) information?

Yes ____ No ____

Comments: _____

_____

ii) Identifying protected information to be shared through the ISE?

Yes ____ No ____

Comments: _____

_____

e) Does the intelligence enterprise have a designated privacy official?

Yes ____ No ____

Comments: _____

_____

f) Does the privacy official have access to legal counsel to help clarify laws, rules, regulations, and statutes governing the collection, maintenance, and dissemination of information and assist with the development of policies, procedures, guidelines, and operation manuals?

Yes ____ No ____

Comments: _____

_____

g) Is the privacy policy reviewed annually for possible revision?

Yes ____ No ____

Comments: _____

_____

h) Does the intelligence enterprise require personnel and participating users (as applicable) to acknowledge receipt of the privacy policy and agreement to comply with the policy in writing?

Yes ____ No ____

Comments: _____

_____

i) Is the intelligence enterprise's privacy policy available to the public?

Yes ____ No ____

Comments: _____

_____

3. Collection

This section refers to the collection of information by the intelligence enterprise. This collection of information may include the identification, location, and recording/storing of information, typically from an original source and using both human and technological means, for input into the intelligence cycle for the purpose of meeting a defined tactical or strategic intelligence goal. There are applicable laws, regulations, and policies that apply to the gathering of information to ensure that there is a legitimate law enforcement or homeland security purpose for the information. These questions were designed to determine whether the intelligence enterprise meets those requirements.[7]

a) Does the intelligence enterprise give other agencies (user agencies) access to collected information?

Yes ____ No ____

Comments: _____

_____

i) If yes, does the intelligence enterprise have a user (or participation) agreement or Memorandum of Understanding (MOU) with those entities that addresses which agency's privacy, civil rights, and civil liberties policy applies to users?

Yes ____ No ____ N/A _____

Comments: _____

_____

7 Questions regarding the collection of information for an intelligence system are located in Section II.

b) In instances in which user agencies are authorized to have direct access to intelligence enterprise information, are user agreements or MOUs in place that cover all areas of the intelligence enterprise's privacy, civil rights, and civil liberties policy?

Yes ____ No ____

Comments: _____

_____

c) If information is rejected for not meeting input standards established by the intelligence enterprise, is the submitting agency or officer notified?

Yes ____ No ____

Comments: _____

_____

d) Are audit trails maintained that track usage of the system and dissemination of information?

Yes ____ No ____

Comments: _____

_____

e) If nonintelligence information is stored at the intelligence enterprise along with criminal intelligence, are there written standards or criteria for collecting such information?

Yes ____ No ____

Comments: _____

_____

f) Is there a process for the regular review of information as it is being collected to ensure compliance with laws or policies restricting collection?

Yes ____ No ____

Comments: _____

_____

g) Is written notification given of potential errors or deficiencies to the privacy official of the source agency when it is determined that protected information received may be erroneous, includes incorrectly merged information, or lacks adequate content such that the rights of the individual may be affected?

Yes ____ No ____

Comments: _____

_____

h) Have criteria been adopted and promulgated for types of information that partners can and cannot submit to the intelligence enterprise?

Yes ____ No ____

Comments: _____

_____

i) Is there a process for the regular review of information as it is being collected by the intelligence enterprise to ensure compliance with laws or policies restricting collection?

Yes ____ No ____

Comments: _____

_____

j) Is there a practice of providing information updates or training about changes in the laws or policies applicable to collection to agency staff responsible for collecting information?

Yes ____ No ____

Comments: _____

_____

k) Are there written policies and business practices in place regarding the acceptance of information from third parties?

Yes ____ No ____

Comments: _____

_____

4. Validation/Retention/Destruction/Purge

The questions listed in this section address both electronic and paper files and how the information is reviewed, validated, or removed if the information is deemed to be of no further value.

a) Does the agency have a written record retention policy that covers all types of data being stored by the intelligence enterprise?

Yes ____ No ____

Comments: _____

_____

i) If yes, does the record retention policy define specific time periods that data is to be retained by the intelligence enterprise before it must be validated or destroyed/purged?

Yes ____ No ____ N/A _____

Comments: _____

_____

b) Is there a policy in place that assigns responsibilities regarding correction or destruction/purge of information which is determined to be inaccurate, misleading, obsolete, or otherwise unreliable?

Yes ____ No ____

Comments: _____

_____

c) Are all agencies that have received inaccurate information notified in writing?

Yes ____ No ____

Comments: _____

_____

d) Are there business practices that reasonably ensure that records are reviewed for validation/ destruction/purge in a timely manner?

Yes ____ No ____

Comments: _____

_____

e) Is there an internal audit of review practices to ensure compliance with validation/purge/retention policies?

Yes ____ No ____

Comments: _____

_____

5. Sharing/Dissemination

Dissemination is the process of effectively distributing intelligence utilizing certain protocols in the most appropriate format for those in need of the information to facilitate their accomplishment of organizational goals. The intelligence enterprise's policy on dissemination should be reviewed prior to completing this area.

a) Are there written policies covering the dissemination process for information?

Yes ____ No ____

Comments: _____

_____

b) Does the intelligence enterprise have written definitions of the need-to-know and right-to-know standards for information dissemination?

Yes ____ No ____

Comments: _____

_____

c) Does the intelligence enterprise have a process established to determine an inquirer's need to know and right to know the information in the performance of a law enforcement activity?

Yes ____ No ____

Comments: _____

_____

d) Are written/electronic inquiry log and dissemination records (audit trail) maintained that indicate who requested information and to whom the information is disseminated, the reason for release of the information, and the date of dissemination?

Yes ____ No ____

Comments: _____

_____

e) Are the intelligence enterprise's products labeled to indicate levels of sensitivity (e.g., information classification markings such as Law Enforcement Sensitive [LES], For Official Use Only [FOUO], and Controlled Unclassified Information [CUI]), levels of confidence, and the identity of the submitting person/agencies?

Yes ____ No ____

Comments: _____

_____

f) Is the submitting agency contacted prior to release of information to a third party?

Yes ____ No ____

Comments: _____

_____

6. Training

An intelligence enterprise should conduct continual training in order to address all policies. The questions in this section address the training programs instituted by the intelligence enterprise to provide the necessary training for agency personnel in privacy-related areas, including 28 CFR Part 23 and other essential areas. The intelligence enterprise must ensure that necessary training applicable to its mission is ongoing and current.

a) Does the intelligence enterprise have a formal training program for all employees on protection of privacy, civil rights, and civil liberties?

Yes ____ No ____

Comments: _____

_____

b) Does the intelligence enterprise provide ongoing training regarding changes in the law, policies, or practices associated with the protection of privacy, civil rights, and civil liberties?

Yes ____ No ____

Comments: _____

_____

c) Does the privacy training include an overview of the policies and procedures and how to report violations and sanctions for failure to comply?

Yes ____ No ____

Comments: _____

_____

d) Does the intelligence enterprise provide 28 CFR Part 23 training to those users who have access to its criminal intelligence system?

Yes ____ No ____

Comments: _____

_____

e) Does the intelligence enterprise keep records of those individuals who have received training?

Yes ____ No ____

Comments: _____

_____

7. Security

Security is a series of procedures and measures that, when taken together, protect people from harm, information from improper disclosure or alteration, and assets from theft or damage.

a) Is the intelligence enterprise located inside of a secure law enforcement agency?

Yes ____ No ____

Comments: _____

_____

b) Does the intelligence enterprise have designated security policies and/or a designated security officer?

Yes ____ No ____

Comments: _____

_____

i) If yes, is the designated security officer responsible for and/or does the policy address:

1) Physical security of the intelligence enterprise? Yes ____ No ____ N/A ____

Comments: _____

_____

2) Systems security? Yes ____ No ____ N/A ____

Comments: _____

_____

3) Information security? Yes ____ No ____ N/A ____

Comments: _____

_____

c) If there is a designated security officer, has the officer taken necessary steps to ensure that security measures provide the proper protection to information in compliance with all applicable laws and the intelligence enterprise's privacy policy?

Yes ____ No ____ N/A ____

Comments: _____

_____

d) If there is a designated security officer, does the intelligence enterprise provide training or authorize appropriate training for the officer?

Yes ____ No ____ N/A ____

Comments: _____

_____

e) Does the intelligence enterprise's privacy, civil rights, and civil liberties policy articulate a process for responding to and addressing security breaches, to include sanctions for noncompliance with the privacy policy?

Yes ____ No ____

Comments: _____

_____

i) If yes, is this process implemented in coordination with the intelligence enterprise's designated security officer?

Yes ____ No ____ N/A _____

Comments: _____

_____

f) Have the intelligence enterprise's security policies been reviewed to ensure that they are sufficient for providing appropriate physical, technical, and administrative measures to safeguard protected information?

Yes ____ No ____

Comments: _____

_____

g) Does the intelligence enterprise store information in the system in such a manner that it cannot be modified, destroyed, accessed, or purged without authorization?

Yes ____ No ____

Comments: _____

_____

h) If applicable, does the intelligence enterprise credential and allow access to intelligence/fusion/terrorism liaison officers?

Yes ____ No ____ N/A ____

Comments: _____

_____

8. Information Technology

The technical questions listed below are designed to be answered by the appropriate information technology personnel who are responsible for producing, manipulating, storing, communicating, and/or disseminating information within the intelligence enterprise.

a) Does each user who is authorized to store, process, and/or transmit information on a computer system that accesses intelligence information have a unique username?

Yes ____ No ____

Comments: _____

_____

b) Does the intelligence enterprise or network document the user's identity, agency associations, the authorization of the user, the purpose of use, and the frequency of use?

Yes ____ No ____

Comments: _____

_____

c) Is criminal intelligence information disseminated over the Internet protected by a minimum of 128-bit encryption?

Yes ____ No ____

Comments: _____

_____

d) Is the intelligence enterprise's criminal intelligence system protected by a firewall?

Yes ____ No ____

Comments: _____

_____

9. Miscellaneous

a) Does the intelligence enterprise conduct and document on-site inspections and audits of member agency files and records regarding submissions to the system to ensure compliance with intelligence enterprise policies and procedures?

Yes ____ No ____

Comments: _____

_____

b) Have internal procedures for redress—particularly to address complaints from protected persons regarding personally identifiable information about them to which they do not have a right of access under applicable law—been developed?

Yes ____ No ____

Comments: _____

_____

c) Were any stakeholder groups consulted in the development or revision of the privacy policy to ensure a transparent and collaborative process?

Yes ____ No ____

Comments: _____

_____

d) Does the privacy policy articulate an individual or group responsible for enforcing the provisions of the privacy policy?

Yes ____ No ____

Comments: _____

_____

e) Does the privacy policy state the contact information of those responsible for responding to questions and concerns about the intelligence enterprise and its policies?

Yes ____ No ____

Comments: _____

_____

Section II: Intelligence System Operations

This section addresses the protection of privacy, civil rights, and civil liberties in the intelligence enterprise's criminal intelligence system operation. The questions are founded on the requirements of 28 CFR Part 23, since the regulation has become the de facto standard for criminal intelligence systems, as recommended in the *National Criminal Intelligence Sharing Plan*.[8] Therefore, these questions may be applicable to all intelligence systems operated by an intelligence enterprise.[9]

Criminal intelligence system name: _____

Overview of the criminal intelligence system (attach if needed): _____

_____

_____

_____

_____

1. Governance

a) Is the system required to abide by the principles of 28 CFR Part 23?[10]

Yes ____ No ____

Comments: _____

_____

b) Does the criminal intelligence system operate in compliance with the principles set forth in 28 CFR Part 23?

Yes ____ No ____

Comments: _____

_____

c) Does the criminal intelligence system have operating procedures or bylaws that implement the operating principles set forth in 28 CFR Part 23?

Yes ____ No ____

Comments: _____

_____

8 The *National Criminal Intelligence Sharing Plan* is available at http://www.it.ojp.gov/documents/NCISP_Plan.pdf.

9 To ensure a comprehensive compliance verification process, some of the questions in this section are similar to questions in Section 1 due to commonalities in collection, validation, and dissemination procedures.

10 Additional information on 28 CFR Part 23 is available at http://www.iir.com/28cfr/.

d) Has the intelligence enterprise complied with all applicable grantor agency requirements; e.g., submitting policies and procedures when required for the system?

Yes ____ No ____

Comments: _____

_____

e) Is the required certification on file that states that the current agency head/designated official takes full responsibility and will be accountable for the information maintained by and disseminated from the intelligence system and that the system will be operated in compliance with the principles set forth in 28 CFR Part 23?

Yes ____ No ____

Comments: _____

_____

f) For interjurisdictional intelligence systems (or other intelligence systems, as appropriate), is there signed user documentation or participation agreements for each participating agency indicating that each agency accepts and agrees to the operating principles set forth in 28 CFR Part 23 which govern the submission, maintenance, and dissemination of information included as part of the system?

Yes ____ No ____

Comments: _____

_____

g) Is there documentation of the policies and procedures for the intelligence system providing that intelligence enterprise staff and any participating agencies will not violate the Electronic Communications Privacy Act of 1986; Public Law 99-508; 18 E.S.C. 2510–2520, 2701–2709, and 3121–3125; or any applicable state statute related to wiretapping and surveillance?

Yes ____ No ____

Comments: _____

_____

h) Is there documentation of policies and procedures for the intelligence system providing that intelligence enterprise staff and participating agencies will not harass or interfere with any lawful political activities as part of the intelligence operation?

Yes ____ No ____

Comments: _____

_____

2. Collection

a) Does the intelligence enterprise operate an interjurisdictional intelligence system?

Yes ____ No ____

Comments: _____

_____

b) Do the areas of criminal activity for which intelligence information is utilized:

i) Represent a significant and recognized threat to the population?

Yes ____ No ____

Comments: _____

_____

ii) Support the purpose of seeking illegal power or profits?

Yes ____ No ____

Comments: _____

_____

iii) Pose a significant and recognized threat to the population?

Yes ____ No ____

Comments: _____

_____

c) Is nonintelligence information stored along with criminal intelligence in the same system?

Yes ____ No ____

Comments: _____

_____

d) If nonintelligence information is stored along with criminal intelligence in the same intelligence system, are there written standards or criteria for collecting such information?

Yes ____ No ____

Comments: _____

_____

e) Does the criminal intelligence system have a policy that criminal intelligence information may be collected or maintained on an individual or organization only if the individual or organization is reasonably suspected of involvement in criminal activity and the information is relevant to that criminal activity?

Yes ____ No ____

Comments: _____

_____

f) Does the criminal intelligence system receive sufficient supporting information with the submission to determine that reasonable suspicion and relevancy requirements are met?

Yes ____ No ____

Comments: _____

_____

i) If no, is this responsibility delegated to a properly trained participating agency?

Yes ____ No ____

Comments: _____

_____

g) Does criminal intelligence system policy prohibit collection and maintenance of records in the intelligence system on political, religious, and social views, associations, or activities of individuals, businesses, or groups unless such information directly relates to criminal activity and there is reasonable suspicion that the subject of the information is involved in criminal conduct or activity?

Yes ____ No ____

Comments: _____

_____

h) Does criminal intelligence system policy prohibit the collection and maintenance in the intelligence system of any information obtained in violation of any applicable local, state, or federal law or ordinance?

Yes ____ No ____

Comments: _____

_____

i) Is noncriminal identifying information entered and maintained in the criminal intelligence system?

Yes ____ No ____

Comments: _____

_____

i) If yes, is noncriminal identifying information attached only to a valid, existing record(s) in the system pertaining to individuals or organizations that are reasonably suspected of involvement in criminal activity?

Yes ____ No ____

Comments: _____

_____

3. Validation/Retention/Destruction/Purge

a) Does the criminal intelligence system use a review-and-validation process that provides advance notice to the submitter or an automatic purge to comply with the purge/retention requirement?

Yes ____ No ____ Automatic Purge ____

Comments: _____

_____

i) If yes, is this process established in the criminal intelligence system's operating policies and procedures?

Yes__ __ No

Comments: _____

_____

b) Are there procedures in place to ensure that all information retained in the criminal intelligence system is relevant?

Yes ____ No ____

Comments: _____

_____

c) Is information in the criminal intelligence system periodically reviewed and validated for continuing compliance with system submission criteria?

Yes ____ No ____

Comments: _____

_____

d) If applicable, does the validation process occur before the expiration of the retention period for the information (which can be no longer than five years)?

Yes ____ No ____ N/A ____

Comments: _____

_____

e) Is misleading, obsolete, or otherwise unreliable information removed from the criminal intelligence system and destroyed?

Yes ____ No ____

Comments: _____

_____

f) Is a record maintained that documents the review, validation, and retention of information which defines the name of the reviewer, review date, and explanation of reason to retain?

Yes ____ No ____

Comments: _____

_____

g) Are records (including backups of records) destroyed/purged in a timely manner?

Yes ____ No ____

Comments: _____

_____

h) Is the entering agency, if applicable, contacted prior to destroying/purging information?

Yes ____ No ____

Comments: _____

_____

i) Is there an internal audit of review practices to ensure compliance?

Yes ____ No ____

Comments: _____

_____

4. Sharing/Dissemination

a) Is dissemination from the criminal intelligence system restricted only to those law enforcement authorities who agree to follow procedures regarding information receipt, maintenance, security, and dissemination that are consistent with the 28 CFR Part 23 operating principles (except that an assessment of criminal information may be disseminated when necessary to avoid imminent danger to life or property)?

Yes ____ No ____

Comments: _____

_____

b) Has a written policy for the criminal intelligence system been adopted to authorize and govern the dissemination of an assessment of criminal intelligence information to government officials or other individuals when necessary to avoid imminent danger to life or property?

Yes ____ No ____

Comments: _____

_____

c) Can a participating agency obtain criminal intelligence information from the system:

i) Directly by telephone? Yes____ No____

Comments: _____

_____

ii) Telephone callback basis only? Yes____ No____

Comments: _____

_____

iii) Mail or e-mail? Yes____ No____

Comments: _____

_____

iv) Teletype? Yes____ No____

Comments: _____

_____

v) Direct electronic connection? Yes____ No____

Comments: _____

_____

d) If remote terminal access is allowed for participating agencies to access the criminal intelligence system, are appropriate security procedures implemented?

Yes ____ No ____

Comments: _____

_____

e) Are participating agency representatives (individual users) identified who are authorized to request and receive criminal intelligence information from the criminal intelligence system?

Yes ____ No ____

Comments: _____

_____

f) Are appropriate measures implemented to verify or authenticate that the requester is authorized to access the system and receive criminal intelligence information?

Yes ____ No ____

Comments: _____

_____

5. Security

a) Has the criminal intelligence system adopted administrative, technical, and physical safeguards (including audit trails) to ensure against unauthorized access and intentional or unintentional damage to criminal intelligence information in the system?

Yes ____ No ____

Comments: _____

_____

b) Does the criminal intelligence system restrict access to its facility's operating environment and documentation to authorized organizations and personnel?

Yes ____ No ____

Comments: _____

_____

i) If yes and the system employs outside IT contractors, have they been fully apprised of the nature of their security responsibilities and the consequences of any violation of these responsibilities and any related contractual requirements?

Yes ____ No ____ N/A _____

Comments: _____

_____

c) Has the criminal intelligence system instituted procedures to protect criminal intelligence information from unauthorized access, theft, sabotage, fire, flood, or other natural or man-made disaster?

Yes ____ No ____

Comments: _____

_____

d) If the criminal intelligence system authorizes and utilizes remote (off-premises) system databases, do such databases comply with the above security requirements?

Yes ____ No ____

Comments: _____

_____

e) Have sanctions been adopted to control unauthorized access, utilization, or disclosure of information contained in the criminal intelligence system, and do these sanctions include the immediate removal of users who have abused the system?

Yes ____ No ____

Comments: _____

_____

6. Technical

a) Does the criminal intelligence system design and configuration allow direct remote terminal access to data by system users?

Yes ____ No ____

Comments: _____

_____

b) Is the criminal intelligence system remotely accessed by:

i) Individual users (e.g., established Internet or dial-up connections to individual personal computers or small office networks)?

Yes ____ No ____

Comments: _____

_____

ii) Another intelligence system or large-scale network (node)?

Yes ____ No ____

Comments: _____

_____

c) If accessed by another intelligence system or large-scale network, have policies and procedures been established and approved by the Office of Justice Programs (OJP) to ensure that the system is accessible only to authorized system users?

Yes ____ No ____ N/A ____

Comments: _____

_____

7. Miscellaneous

a) By agreement or operating procedures, are participating agency files addressed in the intelligence system maintained in a reasonably secure manner to preclude unauthorized access or disclosure?

Yes ____ No ____ N/A ____

i) Has the criminal intelligence system delegated to participating agencies and implemented policies regarding:

1) Determining reasonable suspicion of criminal activity for individuals submitted to the system?

Yes ____ No ____ N/A _____

Comments: _____

_____

2) Determining that there have been no violations of applicable laws in collecting the information submitted?

Yes ____ No ____ N/A _____

Comments: _____

_____

3) Determining need to know/right to know for dissemination of information?

Yes ____ No ____ N/A _____

Comments: _____

_____

b) If the criminal intelligence system delegates responsibility for the previous question to participating agencies, does the project provide the following to its participating agencies:

i) Training on the requirements of 28 CFR Part 23?

Yes ____ No ____ N/A _____

ii) Routine review and inspection of the participating agencies for compliance and supporting documentation for submissions?

Yes ____ No ____ N/A _____

iii) Standardized submission form or format with assurance statement that reasonable suspicion and no violation of law requirements have been met?

Yes ____ No ____ N/A _____

Comments: _____

_____

c) Are the operating principles set forth in 28 CFR Part 23 made part of the bylaws or operating procedures for the system?

Yes ____ No ____

Comments: _____

_____

d) Do all participating agencies accept in writing the operating principles of 28 CFR Part 23?

Yes ____ No ____

Comments: _____

_____

Appendix A: Recommended Verification Process

The purpose of the compliance verification document is to enable agencies to internally assess their intelligence enterprise to ensure that comprehensive privacy, civil rights, and civil liberties protections have been developed and implemented into the enterprise. Though the document can be used as a self-assessment, a peer-to-peer review process is recommended to exchange best practices and lessons learned and to obtain input from colleagues outside of the agency.

Compliance Planning Session

As agencies begin their internal compliance verification, it is recommended that at least one compliance planning session be held with internal agency personnel. The meeting(s) should be one to two weeks prior to the peer-to-peer assessment (if applicable) and should address:

- Reviewing the compliance verification template questions and discussing the process to complete the compliance verification.
- Identifying supporting documentation, which may include:
  - Intelligence enterprise/agency privacy policies and procedures.
  - Intelligence enterprise operating guidelines.
  - Intelligence enterprise security policies and procedures.
  - Criminal intelligence system operating guidelines.

Agency representatives to invite to the planning session include agency/enterprise privacy officials (fusion center privacy official, General Counsel), the Inspector General, the intelligence enterprise director, the intelligence enterprise operations supervisor, the intelligence enterprise lead analyst, and the intelligence enterprise/agency security official.

The *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise* can be used as a self-assessment, but a peer-to-peer review process is recommended to exchange best practices and lessons learned and to obtain input from colleagues outside of the agency.

Compliance Verification Resources and Documentation

After the initial discussion of the compliance verification document and the self-assessment commences, it is recommended that the following documents and resources be created and included in the self-assessment:

- Intelligence enterprise overview document:
  - The overview should include a summary of the sections of the compliance verification, including:
    - Structure of the center (governance/authorities).
    - Organizational hierarchy.
    - Operational processes.
    - Description of the process for collection and dissemination.
- A comprehensive binder/folder that includes the supporting policies, procedures, and guidelines, such as:
  - Intelligence enterprise overview.
  - Intelligence enterprise/agency privacy policy and procedures.
  - Intelligence enterprise operating guidelines.
  - Intelligence enterprise security policies and procedures.
  - Criminal intelligence system operating guidelines.

As part of the peer-to-peer assessment, the agency should provide:

- Copies of the completed internal compliance verification.
- Copies of the supporting documentation.

Peer-to-Peer Exchanges

Beneficial to the compliance verification process is the peer-to-peer exchange. Valuable best practices, lessons learned, and potential solutions can be exchanged between intelligence enterprise personnel through this exchange. It is recommended, as a part of the full compliance verification process, that at the completion of the enterprise's self assessment, leadership from a similar agency's enterprise (such as fusion center to fusion center) be invited to the intelligence enterprise to go through the compliance verification. The purpose of this exchange is to obtain different perspectives on the enterprise's privacy policy, operating guidelines, and intelligence system guidelines to ensure comprehensive implementation of privacy, civil rights, and civil liberties protections.

Corrective Action Plan

As a result of completing the compliance verification process, agencies should identify any areas that may need additional policies, procedures, or operating guidelines to ensure that privacy, civil rights, and civil liberties protections are institutionalized within the intelligence enterprise. Key to this recognition is the identification and specification of corrective action that will be undertaken by the enterprise to mitigate any deficiencies and/or problems noted during the verification process. Additionally, agencies may implement annual privacy reports to demonstrate the corrective action steps that have been developed and implemented during the year as a result of undergoing the compliance verification.

Additional Resources, Sample Documentation, and Verification Documents

To assist intelligence enterprise personnel as the compliance verification is conducted, sample resources will be available on the secure side of the National Criminal Intelligence Resource Center (NCIRC).[11] These resources will include:

- Sample completed assessments
- Fusion center overviews
- Best practices
- Privacy policies
- Sample documents

11 Access to the secure side of NCIRC is available via RISS, LEO, and HSIN.

Appendix B: Definitions

Information—Pieces of raw, unanalyzed data that identify persons, evidence, or events or illustrate processes that possibly indicate the incidence of a criminal event or witnesses or evidence of a criminal event.

Intelligence (Criminal)—The result of the process of systematic gathering, evaluation, and synthesis of raw data on individuals or activities suspected of being or known to be criminal in nature. Intelligence is information that has been analyzed to determine its meaning and relevance. Information is compiled, analyzed, and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity. The product of the analysis of raw information related to crimes or crime patterns with respect to an identifiable person or group of persons in an effort to anticipate, prevent, or monitor possible criminal activity.

Intelligence Enterprise—A unit, organization, task force, center, or initiative created for collecting, analyzing, sharing, or producing intelligence.

Intelligence Process—An organized process by which information is gathered, assessed, and distributed in order to fulfill the goals of the intelligence function. It is a method of performing analytic activities and placing the analysis in a useable form.

Intelligence Products—Reports or documents that contain assessments, forecasts, associations, links, and other outcomes of the analytic process that may be disseminated for use by law enforcement agencies for the prevention of crimes, target hardening, apprehension of offenders, and prosecution.

Intelligence Records (Files)—Stored information on the activities and associations of individuals, organizations, businesses, and groups who are suspected (reasonable suspicion) of being involved in the actual or attempted planning, organizing, financing, or commissioning of criminal acts or are suspected of being or having been involved in criminal activities with known or suspected crime figures.

Intelligence Records Guidelines—Guidelines/standards for the development of records management policies and procedures used by law enforcement agencies.

Law Enforcement Intelligence—The end product (output) of an analytic process that collects and assesses information about crimes and/or criminal enterprises with the purpose of making judgments and inferences about community conditions, potential problems, and criminal activity with the intent to pursue criminal prosecution, project crime trends, or support informed decision making by management.

Need to Know—As a result of jurisdictional, organizational, or operational necessities, intelligence or information is disseminated to further an investigation.

Privacy (Information)—The assurance that legal and constitutional restrictions on the collection, maintenance, use, and disclosure of personally identifiable information will be adhered to by criminal justice agencies, with use of such information to be strictly limited to circumstances in which the legal process permits use of the personally identifiable information.

Privacy (Personal)—The assurance that legal and constitutional restrictions on the collection, maintenance, use, and disclosure of behaviors of an individual—including his/her communications, associations, and transactions—will be adhered to by criminal justice agencies, with the use of such information to be strictly limited to circumstances in which legal process authorizes surveillance and investigation.

Privacy Act—Federal legislation that allows an individual to review almost all federal files pertaining to him/her, places restrictions on the disclosure of personally identifiable information, specifies that there be no secret records systems on individuals, and compels the government to reveal its information sources.

Reliability—Asks the question, "Is the source of the information consistent and dependable?"

Right to Know—Based on having legal authority, one's official position, legal mandates, or official agreements, allowing the individual to receive intelligence reports.

Rules Assessment—Each agency shall implement an ongoing process for identifying and assessing the laws, executive orders, policies, and procedures that apply to the protected information that it will make available or access through the Information Sharing Environment (ISE). Each agency shall identify, document, and comply with any legal restrictions applicable to such information. Each agency shall adopt internal policies and procedures requiring it to:

i) Only seek or retain protected information that is legally permissible for the agency to seek or retain under the laws, regulations, policies, and executive orders applicable to the agency; and

ii) Ensure that the protected information that the agency makes available through the ISE has been lawfully obtained by the agency and may be lawfully made available through the ISE.[12]

12 http://www.ise.gov/docs/privacy/PrivacyGuidelines20061204.pdf.

Appendix C: Privacy-Related Resources

- Global's privacy-related documents[13]
  - *Privacy and Civil Liberties Policy Development Guide and Implementation Templates: Policy Development Checklist*
  - *10 Steps to a Privacy and Civil Liberties Policy*
  - *Privacy and Civil Liberties Policy Development Guide and Implementation Templates*
  - *Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Information Sharing Initiatives*
  - *Information Quality: The Foundation for Justice Decision Making*
  - *Implementing Privacy Policy in Justice Information Sharing: Executive Summary*
  - *Implementing Privacy Policy in Justice Information Sharing: A Technical Framework*
  - *Privacy Technology Focus Group: Executive Summary*
  - *Privacy Policy Development Guide Overview* CD
- LEIU *Audit Checklist for the Criminal Intelligence Function*[14]
- LEIU's *Criminal Intelligence File Guidelines*[15]
- *Baseline Capabilities for State and Major Urban Area Fusion Centers*[16]
- Information Sharing Environment (ISE) Privacy Guidelines[17]
- 28 CFR Part 23
- *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*[18]

13 Global privacy guidelines and templates are available at http://www.it.ojp.gov/default.aspx?area=globalJustice&page=1151.
14 The LEIU *Audit Checklist* is available at http://www.it.ojp.gov/documents/LEIU_audit_checklist.pdf.
15 LEIU's *Criminal Intelligence File Guidelines* are available at http://it.ojp.gov/documents/LEIU_Crim_Intell_File_Guidelines.pdf.
16 The *Baseline Capabilities for State and Major Urban Area Fusion Centers* is available at http://www.it.ojp.gov/documents/baselinecapabilitiesa.pdf.
17 To learn more about the ISE Privacy Guidelines, visit http://www.ise.gov/docs/privacy/PrivacyGuidelines20061204.pdf.
18 *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies* is available at http://www.cops.usdoj.gov/pdf/e09042536.pdf.

BJA
Bureau of Justice Assistance
U.S. Department of Justice

For More Information
Please call (850) 385-0600 or e-mail it@it.ojp.gov.
For more information about DOJ information sharing initiatives, go to

www.it.ojp.gov