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

Intelligence Enterprise:	Oregon TITAN Fusion Center
Date of Review:	October 1, 2013
Names, Titles, and Contact Numbers of Reviewers:	Chuck Cogburn, Director, 503-934-2021
Names, Titles, and Contact Numbers of Employees Interviewed:	
Overview of the Intelligence Enterprise (attach additional pages if needed):[1]	

[1] 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:	
x	Other	Explain:	
Comments:	Letter from Governor		

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

Yes	x	No	
Comments:			

b) Oversight mechanisms (functions)

i) Does the intelligence enterprise have an oversight mechanism?

Internal:	Yes	x	No	
External:	Yes	x	No	
Comments:	Governance Board with multiple participants			

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

Yes	x	No	
Comments:			

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

Yes		No		N/A	x
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	x	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	x	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	x	No	
Comments:			

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

Yes	x	No	
Comments:			

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

x	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	x	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	x	No		N/A	
Date of DHS notification to the fusion center:					2009
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	x	No	
Comments:			

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

Yes	x	No	
Comments:			

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

Yes	x	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	x	No	
Comments:			

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

Yes	x	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	x	No	
Comments:			

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

Yes	xx	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.[2]

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

Yes	x	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	x	No		N/A	
Comments:	Needs to be updated this fall/winter				

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	x
Comments:	Given during Privacy Policy training and initial brief to the enterprise		

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

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

Yes	x	No	
Comments:	Cj Policy manual and Privacy Policy		

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

Yes	x	No	
Comments:	As applicable		

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	x	No	
Comments:	CJ Policy Manual		

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	x	No	
Comments:	Done during initial review of information after that it follows privacy policy and cj policy manual guidelines		

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	x	No	
Comments:	We have not crossed this bridge yet		

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

Yes		No	x
Comments:	We receive all information, then determine if illegal or not appropriate		

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	x	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	x	No	
Comments:	Privacy Officer		

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

Yes	X	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	X	No	
Comments:	CJ Policy manual and privacy policy, constantly updated		

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	x	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	x	No	
Comments:	Privacy Policy		

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

Yes	x	No	
Comments:	We have not had this issue yet		

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

Yes	x	No	
Comments:			

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

Yes	x	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	x	No	
Comments:			

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

Yes	x	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	x	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	x
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	x	No	
Comments:			

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

Yes	x	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	x	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	x	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	x	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	x	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	x	No	
Comments:			

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

Yes	x	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	x	No		N/A	
Comments:					

(2) Systems security?

Yes	x	No		N/A	
Comments:					

(3) Information security?

Yes	x	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	x	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	x	No		N/A	
Comments:	Participates in Webinar and Internet based training				

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	x	No	
Comments:			

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

Yes	x	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	x	No	
Comments:	CJ Policy manual		

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	x	No	
Comments:			

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

Yes		No		N/A	x
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	x	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	x	No	
Comments:			

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

Yes	xx	No	
Comments:			

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

Yes	x	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	x	No	
Comments:	Through Ken Rueben SAC CJ		

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	x
Comments:			

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

Yes	x	No	
Comments:	Initially reviewed by ACLU and DHS Privacy Officials		

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

Yes	x	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	x	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*.[3] Therefore, these questions may be applicable to all intelligence systems operated by an intelligence enterprise.[4]

Criminal intelligence system name:	Oregon State Intelligence Network
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?[5]

Yes	x	No	
Comments:			

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

Yes	x	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	x	No	
Comments:			

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

[4] 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.

[5] 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	x	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	x	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:	Unknown		

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	x	No	
Comments:			

2) Collection

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

Yes	x	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	x
Comments:			

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

Yes		No	x
Comments:			

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

Yes		No	x
Comments:			

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

Yes	x	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	x	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	x	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	x	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	x	No	
Comments:			

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

Yes	x	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	x	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	x	No		Automatic Purge	
Comments:					

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

Yes	x	No	
Comments:			

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

Yes	x	No	
Comments:	During submission in OSIN		

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

Yes	x	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	x	No		N/A	
Comments:					

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

Yes	x	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	x	No	
Comments:			

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

Yes	xx	No	
Comments:			

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

Yes	x	No	
Comments:			

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

Yes	x	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	x	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	x	No	
Comments:			

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

i) Directly by telephone?

Yes	x	No	
Comments:			

ii) Telephone callback basis only?

Yes		No	
Comments:			

iii) Mail or e-mail?

Yes	x	No	
Comments:			

iv) Teletype?

Yes	x	No	
Comments:	If needed		

v) Direct electronic connection?

Yes	x	No	
Comments:			

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

Yes	x	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	x	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	x	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	x	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	x
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	x	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	x	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	x	No	
Comments:			

6) Technical

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

Yes	x	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	x	No	
Comments:			

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

Yes		No	x
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	x
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	x	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	x	No		N/A	
Comments:					

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

Yes	x	No		N/A	
Comments:					

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

Yes	x	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	x	No		N/A	Prior to their access

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

Yes	x	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	x	No		N/A	

Comments:	Reviewed before added to system

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

Yes	x	No	
Comments:			

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

Yes	x	No	
Comments:			

Suspicious Activity Report (SAR) Information

Suspicious activity is defined as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." This information, which in and of itself may seem insignificant, plays an important role in the prevention of terrorism and other crime. Many agencies are incorporating suspicious activity efforts into their crime prevention and crime-fighting efforts.

This appendix applies to agencies that are participants in the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) or have implemented a SAR process. While the *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise* addresses the collection, storage, and dissemination of information in general, this appendix applies specifically to suspicious activity reports (SARs).

In addition to the questions in this appendix, participants in the verification process (internal staff, peer assessors, etc.) may also request to review a sample of SARs to compare to applicable policies and procedures.

Does your intelligence enterprise collect terrorism-related suspicious activity reports (SARs)?

Yes __ X No_____

If yes, are these reports collected based on the ISE-SAR Functional Standard, version 1.5?

Yes ___ X No ____

If no, the following questions do not apply.

b) Is your agency a participant in the NSI? (See http://nsi.ncirc.gov/documents/NSI_Overview.pdf for additional information on the NSI.)

Yes ____ No_____

If yes, are there any gaps currently in your privacy policy that need to be mitigated as a result of joining the NSI?

Yes ____ No ____

Additional information on NSI and privacy policy requirements is available in the *Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template* (http://it.ojp.gov/docdownloader.aspx?ddid=1269).

If yes, do you have a formal vetting process for all SARs as called for in the ISE-SAR Functional Standard 1.5, to include a review for compliance with your agency's privacy policy?

Yes ____ No ____

If no, do you comply with the foundational tenets of the NSI?

Yes ____ No ____

- Additional information on the tenets is available in the *Suspicious Activity Reporting Process Implementation Checklist* (http://it.ojp.gov/docdownloader.aspx?ddid=1147) and *Findings and Recommendations of the Suspicious Activity Reporting (SAR) Support and Implementation Project* (http://nsi.ncirc.gov/documents/SAR_Report_January_2009.pdf).

c) Is SAR information stored in a case management system, an intelligence system, or some other repository?

____ Case management system _____

X ___ Intelligence system _____

____ Some other repository _____

If yes, is criminal intelligence information (as determined by 28 CFR Part 23) housed in this system?

Yes ____ No ___ X

If yes, is the SAR information subjected to the same policies and procedures as other information in the applicable system?

Yes____ No _____

If yes, is the SAR information separated from the criminal intelligence information and identifiable as noncriminal intelligence information?

Yes____ No _____

ii) If no, have policies and procedures been developed regarding the collection and storage of SAR information?

Yes ____ No ___ X

d) Does your intelligence enterprise/fusion center vet each SAR before entry into:

The agency/statewide intelligence system?

Yes ___ X No ____

The ISE Shared Space (if a participant in the NSI)?

Yes ___ X No ____

e) Are agencies that input SARs into the agency/statewide intelligence system required to abide by:

Your agency's privacy policy?

Yes ___ X No ____

A nondisclosure agreement (NDA)?

Yes ____ No ____

Other agreements (please list)?

Yes ____ No ____

Other agreements: _____

_____

f) If your enterprise or fusion center has a privacy officer, does he/she have a working knowledge of your SAR processes?

Yes __ X No_____

If no, has the enterprise or fusion center designated someone to be responsible for privacy-related questions?

Yes ____ No ____

g) **Does your agency's/enterprise's privacy policy comprehensively address the collection, retention, and dissemination of SAR information?**

Yes ___x No_____

If yes, has the policy been determined by the U.S. Department of Homeland Security's Privacy and Civil Liberties Office to be at least as comprehensive as the ISE Privacy Guidelines? (Note: this question is applicable to DHS-designated fusion centers.)

Yes ____x No ____

h) **Does your agency have a SAR Standard Operating Procedure/General Order/Concept of Operations?**

Yes ____ No____ x

If yes, does it reference your agency's privacy policy?

Yes ____ No ____

If no, has your agency documented the collection, retention, and use of SARs in an agencywide policy or procedure?

Yes ____x No ____

i) **How often are reviews conducted regarding fusion center personnel use of and/or access to systems that contain SAR data?**

X ___ Yearly

____ Biannually

____ Other (specify)_____

Describe briefly how these system-usage audits are conducted and by whom and how misuse is identified/determined.

_____

Currently the OTFC NSI system has been up and running since Jan 2012. During this time there have been many times where the system has not worked, this is currently the case. The OTFC has put approximately 50 intakes into the system. As the supervisor of the system I vet each intake before it goes into the shared space or eguardian which minimizes misuse.

We have not conducted an official audit as the system inputs are under the OTFC Directors control.

_____

_____

_____

_____

_____