INFORMATION SHARING ENVIRONMENT – SUSPICIOUS ACTIVITY REPORTING FUNCTIONAL STANDARD AND EVALUATION ENVIRONMENT

Initial Privacy and Civil Liberties Analysis

September 2008—Version 1

Purpose

This analysis has been prepared for the purpose of conducting an initial examination of the privacy and civil liberties ramifications of the Information Sharing Environment – Suspicious Activity Reporting (ISE-SAR) Functional Standard and included Information Exchange Package Documentation (IEPD) component[1] and of the vision for deploying these in operating environments (ISE-SAR Evaluation Environment initiative), making recommendations to address issues identified as a result of the examination, and identifying policies and safeguards that should be implemented at the preliminary stages of this process. The overarching purpose of this analysis—as with all activities conducted in protecting the Nation from terrorism—is to help ensure those carrying out the activities contemplated by these plans do so in a manner that fully protects the legal rights of all United States persons, including information privacy, civil rights, and civil liberties guaranteed by the Constitution and laws of the United States.

Background

The Office of the Program Manager for the Information Sharing Environment (PM-ISE)—in consultation with the Civil Liberties and Privacy Office of the Office of the Director of National Intelligence (ODNI), the Office of Privacy and Civil Liberties of the Department of Justice (DOJ), and the Legal Issues Working Group of the ISE Privacy Guidelines Committee (PGC)—has prepared this Initial Privacy and Civil Liberties Analysis of the ISE-SAR Functional Standard and included IEPD component (ISE-FS-200).

This analysis consists of (i) an explanation of the ISE-SAR Functional Standard and associated IEPD components and plans to test the ISE-SAR Functional Standard at various sites, (ii) questions and answers exploring the privacy and civil liberties ramifications of the ISE-SAR data exchange model and of implementing the ISE-SAR initiative in the field, and (iii) conclusions and recommendations identifying key information privacy and civil liberties concerns that entities participating in the ISE-SAR Evaluation Environment initiative should address as they implement ISE-SAR sharing activities. This is an interim privacy and civil liberties analysis that will be updated as more information is obtained during the ISE-SAR Evaluation Environment initiative, including lessons learned from participants and feedback received from privacy and civil liberties advocates and other interested parties. Because the authors have conducted this analysis in order to help guide participants as they prepare key program documentation, the analysis and recommendations are necessarily general in nature.

The ISE-SAR Functional Standard and the IEPD are designed to enable a federated search of terrorism-related SARs originating at all levels of government. The search will occur within an unclassified information or controlled unclassified information (CUI) sharing environment. As the ISE-SAR Functional Standard deploys to the field, using the ISE Shared Space model

[1] The ISE-SAR Functional Standard was developed and released by the Office of the Program Manager for the Information Sharing Environment (PM-ISE) on January 25, 2008. The ISE-SAR Functional Standard constitutes the first of the Common Terrorism Information Sharing Standards (CTISS). More information on the CTISS Program can be found at http://www.ise.gov/pages/ctiss.html.

(explained below) at various proposed ISE-SAR Evaluation Environment sites, the authors of this report will work with the ISE-SAR Evaluation Environment sites to review and advise regarding the impact of ISE-SAR information sharing on the information privacy, civil rights, and civil liberties of Americans. Based on the experiences documented by the ISE-SAR Evaluation Environment sites, the PM-ISE, in consultation with the ODNI's Civil Liberties and Privacy Office, DOJ's Office of Privacy and Civil Liberties, and the ISE PGC's Legal Issues Working Group, will generate a Final ISE-SAR Privacy and Civil Liberties Analysis identifying how the various ISE-SAR Evaluation Environment sites, in implementing the ISE-SAR Functional Standard, addressed the "key issue" recommendations outlined below were addressed. This compilation of practices and experience from the ISE-SAR Evaluation Environments will inform future revisions to the ISE-SAR Functional Standard.

Introduction

On October 31, 2007, President George W. Bush issued the initial National Strategy for Information Sharing (NSIS) to prioritize and unify the Nation's efforts to advance the sharing of terrorism-related information among Federal, State, local, and tribal Governments, private sector entities, and foreign partners. The NSIS calls, in part, for the Federal Government to support a nationwide capability for the gathering, analysis, and sharing of information, including suspicious activity and incident reporting related to terrorism, with State, local, and tribal Governments and across the Federal Government. Consistent with the NSIS, and as a priority for the establishment of the Information Sharing Environment (ISE), the PM-ISE has helped coordinate a comprehensive effort to develop a nationwide network of state, regional, and major urban area fusion centers that will facilitate the sharing of terrorism-related information across the local, state, tribal, and federal communities. The ISE-SAR Functional Standard was developed and released by the PM-ISE on January 25, 2008, to specifically address the sharing of terrorism-related suspicious activity reports (hereinafter ISE-SAR information or ISE-SARs), with the overarching goal of enabling analysts and officers with counterterrorism responsibilities at all levels of government to discover and identify terrorist activities and trends.

The ISE-SAR Functional Standard (at "Definitions," Section 5 (g) of PM-ISE Memorandum, January 25, 2008) defines the term "suspicious activity report" (SAR) as "any official documentation of observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention."[2] The documenting of suspicious activity is well institutionalized in the law enforcement community, where federal and state, local, and tribal (SLT) agencies collect and document suspicious activities in support of their responsibilities to investigate and prevent potential crimes, protect citizens, and apprehend and prosecute criminals. Such reporting occurs with varying degrees of

[2] *Ballantine's Law Dictionary*, 1969, defines "illicit" as "unlawful, illegal, prohibited or forbidden by law." Because terrorism is defined as a criminal act, the suspicious behavior underlying an ISE-SAR must demonstrate a nexus to criminal activity or intent, as opposed to non-criminal, but illicit, activity or intent. This is further discussed in the Privacy and Civil Liberties Analysis Section, Q&A 1.

standardization and formality in other communities as well (intelligence, defense, homeland security), where entities document observed or reported suspicious activity as part of their mission or for the purpose of protecting personnel and facilities. In all of these arenas, some of the documented activities may bear a potential nexus to terrorism. In accordance with the NSIS, which identifies suspicious activity reports as one of the key information exchanges to be effected between the Federal and SLT Governments, the PM-ISE developed a standardized process (and associated data model) for identifying, documenting, and sharing ISE-SAR information to the maximum extent possible consistent with the protection of privacy and civil liberties.

The ISE-SAR Functional Standard envisions that agencies will share potential ISE-SAR information with a state or major urban area fusion center and, when appropriate and consistent with existing practice, the local FBI Joint Terrorism Task Force (JTTF). At the fusion center, analysts or law enforcement officers will evaluate the SAR against the ISE-SAR Functional Standard. If the SAR meets criteria as defined in the ISE-SAR Functional Standard, the fusion center will designate the SAR as an "ISE-SAR" and make it available to other ISE participants through the fusion center's Shared Space. Documenting, analyzing, and sharing of ISE-SAR information between and among SLT entities, state or major urban area fusion centers, JTTFs, and federal field components is designed to enable the identification of behaviors and indicators of criminal activity associated with terrorism.

Summary of the SAR Functional Standard for the ISE

The ISE-SAR Functional Standard

The ISE-SAR Functional Standard provides an important mechanism for representing details about terrorism-related suspicious activity in a consistent manner to help facilitate the identification of useful investigatory or trending information. The ISE-SAR Functional Standard is not intended to prescribe all processes, systems requirements, or other business rules governing the collection, processing, or sharing of SARs by law enforcement entities. The diverse entities that generate and use SARs have well-established processes and business rules for suspicious activity reporting.

The ISE-SAR Functional Standard sets forth a two-part "integration/consolidation" process for identifying, out of the thousands of suspicious activities documented through "organizational processing" activities conducted by source agencies each day, those that have a potential nexus to terrorism. The first step in the process of identifying an ISE-SAR is for a trained analyst or law enforcement officer at a fusion center, or JTTF, to determine whether suspicious activity falls within any of the criteria set forth in Part B – ISE-SAR Criteria Guidance of the ISE-SAR Functional Standard. These criteria describe behaviors and incidents identified by law enforcement officials and counterterrorism experts from across the country as being indicative of criminal activity associated with terrorism. The second step in the process is for a trained expert to determine, based on a combination of knowledge, experience, available information, and, importantly, personal judgment, whether the information has a potential nexus to terrorism. When suspicious activity is determined to have a potential nexus to terrorism, fusion center personnel will document it in the data format and schema (information exchange package documentation) prescribed by the standard and make it available to all appropriate ISE participants in the Shared Space.

Thus, the implementation of the ISE-SAR Functional Standard is designed as a tool to enable fusion centers and federal agencies to build upon and optimize reporting activities already taking place at the SLT and federal levels. The ISE-SAR Functional Standard will be implemented for evaluation purposes at diverse ISE-SAR Evaluation Environment sites, including major city and other police departments and state and major urban area fusion centers. However, numerous privacy and civil liberty concerns arise when information regarding suspicious activities associated with terrorism is shared between federal and SLT authorities. The ISE-SAR Evaluation Environment initiative will address these concerns through the development and application of appropriate privacy, civil rights, and civil liberties protection policies and procedures.

The Information Exchange Package Documentation

The ISE-SAR Functional Standard is intended to support broad dissemination of ISE-SARs and sharing of the maximum relevant information. To facilitate this dissemination and sharing, two different data formats (information exchange packages) have been developed for packaging ISE-SAR information. The **Detailed format** includes information contained in all data elements set forth in Section IV of the ISE-SAR Functional Standard ("ISE-SAR Exchange Data Model"), including fields denoted as privacy fields. "Privacy fields" contain personal information that can be used to identify individual subjects, either alone or in combination with other information. The **Summary format** excludes fields or data elements identified as privacy fields in Part A – Section IV.[3] The ISE-SAR Functional Standard identifies the minimum privacy fields that must be excluded from a Summary ISE-SAR. Each ISE participant may exclude additional privacy fields from its Summary ISE-SARs, in accordance with its own statutory or policy requirements. The goal is for ISE-SARs to be shared, to the maximum extent possible, among SLT and federal law enforcement, homeland security, and other appropriate organizations participating in the ISE while protecting information associated with the designated privacy fields.

ISE-SAR Evaluation Environment

ISE-SAR Functional Standard/IEPD Evaluation Environment Goals

To test the assumption that the ISE-SAR Functional Standard will facilitate the sharing of terrorism-related SAR information across multiple domains and levels of government, the PM-ISE, in concert with its federal partners and national associations of law enforcement

[3] Because both Detailed and Summary formats contain contact information for the source organization, recipients of the Summary format could contact the source organization for additional information, as appropriate.

officials, is sponsoring a project embracing a variety of ISE-SAR Evaluation Environment sites. The umbrella project currently envisions twelve ISE-SAR Evaluation Environment sites to be implemented and activated incrementally as each site is provided the necessary technology package, including hardware, software, and technical assistance.[4] These ISE-SAR Evaluation Environment sites will be state and major urban area fusion centers and their source agency law enforcement partners. The ISE-SAR Evaluation Environment sites will assess the value of the ISE-SAR process and of the ISE-SAR Functional Standard and the Detailed and Summary ISE-SAR fields in advancing counterterrorism goals, i.e., (1) the usefulness of the ISE-SAR Criteria Guidance (Part B of the ISE-SAR Functional Standard) in identifying pre-operational planning related to terrorism, and (2) the extent to which the sharing of ISE-SARs, both Detailed and Summary, across the levels of government enables discovery and analysis of terrorism trends and supports counter-terrorism efforts. In addition to evaluating the ISE SAR Functional Standard, the ISE-SAR Evaluation Environment will also provide access to a library of free-text SAR summaries containing no privacy field information. Additionally, the participants will provide feedback regarding the administrative and procedural aspects of the ISE-SAR initiative, i.e., the process of designating information as an ISE-SAR, the management of postings in ISE Shared Space, the interagency processes for correcting inaccurate information, and other relevant program implementation issues.

The first three ISE-SAR Evaluation Environment sites, state fusion centers in Florida, New York, and Virginia, are scheduled to begin posting Summary ISE-SARs to their respective ISE Shared Spaces in Q4 FY2008.

Systems for Sharing ISE-SAR Information in the Evaluation Environment Initiative

Section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, as amended, directs that to the greatest extent possible, the ISE should be a decentralized, distributed, and coordinated environment that connects existing systems to share terrorism information. Accordingly, the ISE-SAR Evaluation Environment initiative has been designed to leverage architecture attributes of a distributed model. Participating fusion center entities will designate and format ISE-SARs using the ISE-SAR Functional Standard and post them to their individual Shared Space, controlled by the participating fusion center.[5] The ISE Enterprise Architecture Framework (EAF) envisions a federated system for managing access authorizations and a common architectural structure for ISE business processes, information

[4] These twelve ISE-SAR Evaluation Environment sites will be announced in the near future.

[5] The ISE Shared Spaces concept is a key element of the ISE EAF and addresses the stewardship problems identified by the 9/11 Commission by assigning exclusive control of an ISE-SAR to the submitting entity. ISE Shared Spaces are networked data and information repositories used by ISE participants to make their standardized terrorism-related information, applications, and services accessible to other ISE participants. ISE Shared Spaces also provide an infrastructure solution for those ISE participants with national security system (NSS) network assets, historically sequestered with only other NSS systems, to interface with ISE participants having only civil network assets. Additionally, ISE Shared Spaces also provide the means for foreign partners to interface and share terrorism information with their U.S. counterparts. For more information about the ISE Shared Spaces concept, reference the *ISE Enterprise Architecture Framework* and the *ISE Profile Architecture and Implementation Strategy* at www.ise.gov.

flows and relationships, services, and other functions.[6] However, in accordance with the mandate of the IRTPA, no single system for accessing or storing ISE-SARs is envisioned.

Sharing of law enforcement information between fusion centers and the federal law enforcement community currently occurs via the Regional Information Sharing Systems Network (RISSNET), Law Enforcement Online (LEO), and Homeland Security Information Network (HSIN). With regards to the DHS HSIN, ISE-SAR Evaluation Environment data will be limited to vetted members of the Homeland Security State and Local Intelligence Community of Interest (HS SLIC) who are able to access the data via the HSIN-Intelligence platform. All of these systems will support initial access to ISE-SARs data for the Evaluation Environment sites.

NOTE: This document is drafted with the assumption that the ISE Shared Spaces concept will be operational and that each ISE-SAR Evaluation Environment initiative participating agency will maintain and control information in the Shared Space.

Privacy, Civil Rights, and Civil Liberties Protections in the Evaluation Environment Initiative

As noted, the ISE-SAR Functional Standard does not prescribe a complete set of business rules for source agencies to use in collecting, processing, and sharing SAR data (as distinct from designating and formatting ISE-SARs using the ISE-SAR criteria and IEPD). As stated in the Memorandum of Understanding Between the DOJ's Bureau of Justice Assistance (BJA) and the PM-ISE,[7] the ISE-SAR Evaluation Environment effort will result in the development and publication of a guide or template for federal, state, local, and tribal entities to use in establishing policies, common business processes, and technical capabilities for the gathering, documenting, processing, analysis, and sharing of terrorism-related suspicious activities. The guide or template will be based on "best practices" identified at the ISE-SAR Evaluation Environment sites.

Currently, the ISE-SAR initiative contemplates implementation of the ISE-SAR Functional Standard in the context of the current business processes at the diverse Evaluation Environment sites. Consistent with this report's recommendations, the ISE-SAR Evaluation Environment sites will save Detailed ISE-SARs to the Shared Space, but until they develop or adopt policies and procedures to ensure that appropriate privacy and civil liberties protections are in place,

[6] The EAF envisions an ISE-wide system of attribute-based controls that would manage access authorization based on the mission and function of the ISE participant requesting access. Under such a system it would be possible, for example, to grant full access to one set of users and partial access to another set of users. As more ISE Shared Spaces become operational and the PM-ISE issues technical standards governing access rules and requirements for these ISE Shared Spaces, information sharing through the ISE will become more efficient. For example, once access, system certification, and accreditation rules are standardized and applied to ISE Shared Spaces that support connectivity among ISE participants, users will have direct access to ISE information within those ISE Shared Spaces, including ISE-SARs, rather than having to negotiate multiple systems with multiple access rules.

[7] The Memorandum of Understanding describes the scope of the ISE-SAR Evaluation Environment activities and the roles and responsibilities of the parties to the agreement.

the results to an ISE-SAR search will be viewable only without the privacy fields (Summary ISE-SAR format) (see Recommendation C(2)). Once the ISE-SAR Evaluation Environment sites have demonstrated that the necessary privacy policy framework is in place, they may share ISE-SAR information with privacy fields (Detailed ISE-SAR format). Subsequently, based on experience using the Detailed ISE-SAR format, the ISE-SAR Evaluation Environment sites will assess the additional value of sharing privacy field data, including a determination of when and under what circumstances it is necessary and appropriate to reveal these data.

In addition, the Concept of Operations (CONOPS)[8] under development for the ISE-SAR Evaluation Environment initiative will require that participating fusion centers adopt an umbrella ISE-SARs Evaluation Environment Privacy and Civil Liberties Protection Policy or evaluate and, if necessary, update their existing privacy and civil liberties policy to ensure the gathering, documenting, processing, and sharing of ISE-SARs is consistent with the umbrella policy (see Recommendation C(1)). In either instance, the policy for ISE-SARs must be consistent with applicable state constitutions, statutes, and local ordinances. Each participating fusion center is encouraged to use the *Guide to Conducting Privacy Impact Assessments for State and Local Information Sharing Initiatives* (DRAFT), produced by DOJ's Global Justice Information Sharing Initiative (Global), to determine whether additional protections are warranted (see Recommendation B(2)(b)).[9]

As part of the ISE-SAR Evaluation Environment initiative, the CONOPS will require each participating site to document the manner in which the ISE-SAR information is being posted and shared via the Shared Space and how the site is complying with its ISE-SAR privacy and civil liberties protection policy (see Recommendation C(1)).

With the goal of assisting fusion centers to establish guidelines (business rules) for law enforcement entities to follow in collecting, processing, and sharing suspicious activity and incident information, the practices of several major city police departments with established SAR processes and privacy protections were reviewed as a part of a BJA funded project, in coordination with the Major Cities Chiefs Association, Global and Global's Criminal Intelligence Coordinating Committee (CICC). The project's findings noted that the evaluated police departments did not have complete SAR processes and that improvements in privacy protections were needed. These departments' practices were evaluated and fashioned into recommendations provided to other cities to facilitate the establishment of a SAR process in additional urban areas. (See *Findings and Recommendations of the SAR Support and Implementation Project.*[10]) Specific attention was paid to ensure that procedures respect the information privacy

[8] The CONOPS describes the requirements and capabilities of a PM-ISE sponsored Evaluation Environment established to test and evaluate the ISE-SAR process in an operational setting at state and major urban area fusion centers.

[9] DOJ, DHS and Global have identified privacy and civil liberties as a priority. For example, the developed (and soon to be released) Fusion Center Baseline Capabilities document includes privacy and civil liberties requirements. Both the Fusion Center Baseline Capabilities and Fusion Center Guidelines address training, security, data accuracy, governance structures, etc., which all support the implementation and monitoring of privacy and civil liberties efforts.

[10] In June 2008, the *Findings and Recommendations of the SAR Support and Implementation Project* were developed to provide recommendations to the Criminal Intelligence Coordinating Council (CICC) from the Major Cities Chiefs Association. Findings

and other legal rights of Americans.[11] The *Findings and Recommendations* comport with the requirements of the ISE Privacy Guidelines.[12] As detailed in the Recommendations section of this analysis, entities seeking to develop a robust SAR business process are advised to adopt the "best practices" set out in the *Findings and Recommendations of the SAR Support and Implementation Project* and to implement the requirements of the ISE Privacy Guidelines for all SAR information. In addition, ISE-SAR business rules should address, among other considerations, the vetting of ISE-SARs for criminal predicate and terrorism nexus, constraints on secondary disclosure, logging and auditing of access to ISE-SARs, and procedures for notifying source organizations of inaccuracies in ISE-SAR data.

Privacy and Civil Liberties Analysis

1. What is an ISE-SAR? Must it relate to criminal activity?

The ISE-SAR Functional Standard defines a suspicious activity report (SAR) as "official documentation of observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention." As stated in the Introduction, the documenting of suspicious activity is well institutionalized in the law enforcement community, where federal and state, local, and tribal (SLT) agencies collect and document suspicious activities in support of their responsibilities to investigate and prevent potential crimes, protect citizens, and apprehend and prosecute criminals.

The term "illicit intention" is not defined by the ISE-SAR Functional Standard. *Ballantine's Law Dictionary*, 1969, defines "illicit" as "unlawful, illegal, prohibited or forbidden by law." Because terrorism is a criminal act under applicable laws, the authors of this report recommend that applicable documentation make clear that the suspicious behavior underlying an ISE-SAR must demonstrate a nexus to criminal activity or intent, as opposed to non-criminal, but arguably "illicit," activity or intent (see Recommendation B(3)(c)).[13]

The ISE-SAR Functional Standard further defines an ISE-SAR as a SAR that has been determined, pursuant to a two-part process (described in Q&A #4), to meet ISE-SAR criteria and have a potential terrorism nexus. Once this determination is made, the information becomes an ISE-SAR and is formatted in accordance with the ISE-SAR Functional Standard. The ISE-SAR

and recommendations are based on the practices of the Los Angeles, Boston, Chicago, and Miami-Dade police departments. At the time of this writing, a final draft of this report is under review at the CICC. At the time of this writing, the final draft is available at http://online.wsj.com/public/resources/documents/mccarecommendation-06132008.pdf.

[11] The development of SAR processes at the local law enforcement level has been spearheaded by the Los Angeles Police Department (LAPD). For example, LAPD's policies and procedures provide standardized codes that facilitate reporting and review of terrorism-related suspicious incidents. Reports that meet a criminal predicate are shared with experienced and trained investigators in the Major Crimes Division, who forward to the Joint Regional Intelligence Center analysts (JRIC) those SARs judged to be terrorism-related. Analysts at the JRIC combine the information with information from other jurisdictions to identify patterns and trends within the greater Los Angeles region. The LAPD SAR business process includes multiple levels of vetting to ensure information is legally obtained and that it indicates a potential terrorism nexus.

[12] More information on the ISE Privacy Guidelines can be found at http://www.ise.gov/pages/privacy-implementing.html.

[13] The observed behavior need not be in and of itself a crime, of course.

Functional Standard lists 189 data elements that experience with prior terrorism incidents has demonstrated are helpful in understanding potential incidents of terrorism planning or implementation and are therefore potentially contained in SAR reporting. These data elements can be found on pages 12 through 21 of the ISE-SAR Functional Standard.

2. Why is suspicious activity information collected and documented in the first place?

Suspicious activity information is collected and documented by a variety of organizations for a range of purposes. In many organizations within Federal and SLT Governments, as well as certain private sector entities, suspicious activity information is collected and documented to support core mission responsibilities. For example, local law enforcement organizations collect suspicious activity information as a key part of their mission to prevent, investigate, and prosecute criminal activity. In other organizations, suspicious activity information may be collected and documented solely for the purpose of protecting facilities or personnel.

Not all collection of information by government and the private sector that may be considered "suspicious" in a general sense will be considered eligible for a SAR or for an ISE-SAR under the ISE-SAR Functional Standard. Suspicious activity must be "indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention" for a report documenting such activity to be considered a SAR under this standard (see ISE-SAR Functional Standard, PM-ISE Memorandum, "Definitions," Section 5(g)).

3. What entity designates a SAR as an ISE-SAR?

The ISE-SAR Functional Standard (Part C – ISE-SAR Information Flow Description, Step 4) states that a SAR is designated as an ISE-SAR at one of two types of government entities:

- A state or major urban area fusion center (for SLT ISE-SAR information), or
- A federal agency[14]

In some cases, a federal agency field component (e.g., an FBI Joint Terrorism Task Force (JTTF) or Field Intelligence Group (FIG)) and the state or major urban area fusion center may be co-located. In other cases, the JTTF or FIG may be located separately but will collaborate with state or major urban area fusion centers to provide an integrated view of the terrorist threat. In yet other cases, SLT law enforcement entities may share SAR information directly with a federal agency outside of the fusion center or JTTF/FIG structure.[15] In practice, major city police agencies, such as the Los Angeles Police Department, may play a significant role in the

[14] For the purposes of the ISE-SAR Evaluation Environment, a federal agency could mean a headquarters or field component of a Federal Government agency with a counterterrorism (CT) mission (for federal department or agency ISE-SAR information). At least one federal entity (the Department of Defense) has indicated an intent to use the FBI's e-Guardian system as its Shared Space for posting ISE-SARs. Accordingly, e-Guardian may be one of several Federal Shared Spaces.

[15] The ISE-SAR Functional Standard does not affect currently supported and/or mandated direct interactions between SLT law enforcement and investigatory personnel and JTTFs or FIGs.

identification and designation of ISE-SARs. As appropriate, the next version of the ISE-SAR Functional Standard will be modified to reflect any changes in process and data format that are identified as necessary in the course of testing the ISE-SAR Functional Standard at the various Evaluation Environment sites.

4. How is the designation of an ISE-SAR made and by whom?

The ISE-SAR Functional Standard indicates the designation of an ISE-SAR as a two-part process (see Part C – ISE-SAR Information Flow Description, Step 4). First, at the state or major urban area fusion center or federal agency, a trained analyst or law enforcement officer reviews the newly reported information against ISE-SAR criteria (Part B of the ISE-SAR Functional Standard). Federal agency personnel with law enforcement or intelligence responsibilities, to include officials from DHS' Office of Intelligence and Analysis and the FBI, may be collocated or deployed to fusion centers and may participate in the review and designation of ISE-SARs at the fusion center level. Second, based on available information, knowledge and experience, the analyst or law enforcement officer determines whether the information may have a nexus to terrorism (i.e., the SAR information has been identified as potentially terrorism-related). (see ISE-SAR Functional Standard at C3.) The process requires human interaction and judgment and is not performed automatically by computer software. An ISE-SAR is created and shared with appropriate ISE participating organizations only when a trained expert has determined that the information meeting the criteria has a potential nexus to terrorism.[16]

The ISE-SAR Functional Standard does not prescribe processes at the source agency level to ensure that SAR information received is legally obtained and that suspicious incidents and activities are properly identified as having a potential terrorism nexus. Nor does the ISE-SAR Functional Standard provide more detailed guidance on how to apply the criteria in Part B. Those criteria are intended to be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention. Focusing attention on observable behaviors is important for intelligence purposes, as well as to avoid inappropriate reporting. The criteria, however, are general in nature, and while they may indeed be indicative of such intelligence gathering or pre-operational planning, they may also apply to innocent behavior. The purpose of requiring a separate determination, based on available information, knowledge and experience, that the SAR information is potentially terrorism-related, is to avoid a mechanical or automatic application of the Part B criteria to otherwise innocent behavior. However, more guidance on how to apply the Part B criteria to avoid over-inclusiveness, and to guard against inappropriate reporting, is important.

The authors of this report recommend that training programs and guidance documentation be developed on how to apply the Part B criteria to minimize the risks of over-inclusiveness and

[16] In addition to evaluating the ISE-SAR Functional Standard, the Evaluation Environment project will also evaluate the utility of creating and making accessible a library of Summary SARs that may have a nexus to terrorism. The Summary SARs Library will contain a mix of SARs (both terrorism-related and non-terrorism related) in free text format. These Summary SARs are completely anonymous (i.e., all privacy information is removed).

inappropriate reporting, and that the program documentation supporting the ISE-SAR Evaluation Environment (CONOPS, participation agreements, etc.) require ISE-SAR Evaluation Environment sites to obtain assurances from source agencies that all personnel involved in the gathering, processing, reporting, analyzing, and sharing of suspicious activity information have been trained on the ISE-SAR Functional Standard criteria and information collection limitations (see Recommendation B(3)(a)). Such training will help ensure that SAR reporting and designation of ISE-SARs are based on observable behaviors and incidents indicative of criminal activity related to terrorism and not on subjects' protected characteristics or lawful activities.

5. What level of review will source agency information be subject to prior to being posted in the Shared Space?

To be effective, information used to support law enforcement investigations and other counter-terrorism activities must be lawfully obtained and have a terrorism nexus.

As described in the ISE-SAR Functional Standard (Part C – ISE-SAR Information Flow Description), the review and vetting process begins when a front-line law enforcement officer responds to a call for service, self-initiates law enforcement action based on a reported incident or observation, or observes suspicious behavior. To preclude reporting on individuals involved in innocent activities, front line personnel must be able to recognize indicators (incidents, behaviors, and modus operandi of individuals and organizations) of criminal activity associated with domestic and international terrorism and must understand the scope of their legal authority to obtain information. The authors of this report recommend that the ISE-SAR Evaluation Environment CONOPS and other participation agreements require appropriate training of front line personnel and multiple levels of report review by senior officers, investigators and analysts similarly trained on the criteria of the ISE-SAR Functional Standard and legal collection thresholds. (See Recommendation B(3)(a).) To satisfy privacy and civil liberties concerns, each fusion center and local entity participating in the ISE-SAR Evaluation Environment initiative should develop, or follow established, business rules for multi-level review and vetting of suspicious activity reporting by personnel trained in the ISE-SAR process.

6. What is the source of the suspicious activity information (i.e., from where/whom is the information collected)? How is the information collected?

There are many sources of suspicious activity information. In some cases the information is reported to SLT or federal law enforcement or homeland security officials by a concerned individual. The reporting of a suspicious activity or incident can be accomplished by telephone, via Internet, in person, or in writing (e.g., 9-1-1 and dispatch centers). Information concerning suspicious activities may also be directly observed or obtained by an authorized government official or by a private sector security guard (the private sector security guard would pass the information to an authorized government official). Agency resources, policies, and procedures determine how the information is first obtained and processed.

At the federal and SLT levels a common method of receipt is through a "Tip" line. Individuals are encouraged to report observed crime and suspicious activities to the police in a given geographic area using a "Tip" line, which is simply a toll-free or local telephone number that individuals can use to report such information. Some agencies, such as the FBI, also use Internet reporting systems for individuals to submit tips.

JTTFs have established policies and procedures in place for reviewing and determining which tips will be further investigated. Even if a tip is not determined to have a terrorism nexus, the relevant federal or SLT authorities may choose to retain it for other reasons, such as inclusion in an "all-crimes" database. Retention of personal information raises privacy and civil liberties concerns and must be consistent with policies and practices that govern how it is used and maintained.

7. How is received suspicious activity information documented?

Practices vary from jurisdiction to jurisdiction. For purposes of the ISE-SAR Functional Standard, suspicious activity information, whether obtained through direct observation by a government official, reported by an individual on a "Tip" line, or acquired via any other mechanism, becomes a "SAR" when it has been reviewed and validated in accordance with that organization's policies and documented in a written report(s) by an authorized official. Depending upon the policies and procedures of the receiving organization, there may be one or more documents/forms used to describe the activity. This documentation might contain, for example, information reported by an individual through a "Tip" line and the information has been reviewed and validated in accordance with that organization's policies. Alternately, a SAR document could contain a lead developed from an investigation or through information obtained by querying incident- and fact- based systems used by law enforcement and public safety organizations, such as the National Crime Information Center (NCIC), Department of Motor Vehicles (DMV), and other systems. It is also possible that the first documentation of a suspicious activity will be in the ISE-SAR format.

8. Are actions taken to ensure data quality (e.g., that the information reported in an ISE-SAR is accurate, timely, and reliable)?

The ISE-SAR Functional Standard does not dictate a common process that applies to data quality. Data contained in reports designated as ISE-SARs derive from information gathered by source or reporting law enforcement organizations. Before the suspicious incident or behavior is documented in the first instance, entities may apply various means, tools, and techniques to verify the accuracy, timeliness, and reliability of details surrounding the observed or reported "suspicious" conduct or event. Most often, this verification entails interviews with individuals who supplied the information or investigations of the reportedly "suspicious" circumstances. Law enforcement officers also may query fact-based systems to validate information relating to the incident or conduct.

As part of the Evaluation Environment effort, consistent with the Data Quality provision of the ISE Privacy Guidelines, sites will be asked to develop specific data quality and redress processes for correcting or purging information discovered or reported to be inaccurate. The authors of this report recommend that sites implement business processes, including steps to vet or validate the accuracy of observations, tips, leads, or other incident reporting and to remove from, or update in, an ISE Shared Space any ISE-SAR determined to be deficient or unfounded (e.g., redress) (see Recommendation B(1)(b)).

The authors of this report recommend that the ISE-SAR Evaluation Environment sites, under the CONOPS, require source agencies documenting suspicious activity to assess their confidence in the information they report, including source reliability and content validity (see Recommendation B(1)(g)). The assessment may rely on factors such as demeanor (e.g., intoxication level, mental state), credibility (based on prior experience, interview), or other indicia of reliability and validity. The assessed level of confidence will enable the fusion center or other recipient organizations to better gauge the value of the information to be designated an ISE-SAR and to ensure against erroneous reports or reports potentially motivated by racial, religious, or other animus. While no policy can completely eliminate the risk of such bias, responsible processes to validate and review possible suspicious activities before such activities are formally documented may reduce such risks. Repeated examination improves the quality of the information and also protects the information privacy and other legal rights of Americans.

9. What legal authorities govern the original collection of the information by government entities? Is "reasonable suspicion" required?

In order for documentation of suspicious activity to be considered an ISE-SAR under this Functional Standard, it must relate to "terrorism, criminal, or other illicit [i.e., illegal][17] intention." Each government entity that collects and documents suspicious activities at the federal or SLT level must do so in accordance with applicable law and policy. Nothing in the ISE-SAR Functional Standard alters this fundamental requirement.

The determination to document a suspicious incident as an ISE-SAR cannot be based solely on a subject's race, ethnicity, national origin, religious preference or the exercise of First Amendment or other constitutional rights. In addition, for federal agencies, the Privacy Act of 1974 prohibits the collection and maintenance of information in these categories except to the extent that the information is pertinent to and within the scope of an authorized law enforcement activity (5 U.S.C. 552a(e)(7)). Only reports of conduct consistent with criminal activities associated with terrorism, and regarding subjects whose potential involvement in that criminal activity cannot be discounted, will be designated an ISE-SAR. Absent a determination that a potential nexus to terrorism exists, the information will not become the subject of an ISE-SAR. The authors of this report recommend that business processes be implemented to incorporate training and guidance to implement these safeguards into the SAR process. (See Recommendations B(1)(b)

[17] See Recommendation B(3)(c).

and B(3)(a)). These safeguards are intended to ensure that information, consideration of which could violate an individual's privacy, civil rights, and civil liberties by unjustifiably associating him/her with terrorism, will not be intentionally or inadvertently gathered, documented, or processed as an ISE-SAR and shared though the ISE.

"Reasonable suspicion" is not a separate requirement of the ISE-Functional Standard. The ISE-Functional Standard is based on the premise that agencies will generate SARs based on applicable laws and policies in their jurisdictions, and that the ISE-Functional Standard will then standardize the process for determining when a SAR has a potential terrorism nexus, and will provide the relevant data format and elements. It was not originally intended to address the legal standard to be used by each federal, state, local, and tribal entity for determining what level of evidence or certainty is necessary or sufficient for submitting a SAR. The authors of this report acknowledge that questions arise as to whether a SAR should meet the "reasonable suspicion" standard established for Criminal Intelligence Systems under 28 C.F.R. Part 23, and support the privacy and civil liberties finding and recommendation in *Findings and Recommendations of the SAR Support and Implementation Project,* that agencies should clearly articulate when 28 C.F.R Part 23 should be applied. The business processes, training, and documentation identified in this analysis provide additional safeguards for ISE-SARs. For example, the CONOPS will require the ISE-SAR Evaluation Environment sites to recognize only those inquiries that provide a case, incident, or other justification (see Recommendation B(1)(l)) – the justification for disclosing certain information could be a particularized showing, subject to audit, designed to avoid privacy and civil liberties harm to the individual. The authors of this report will continue to evaluate how to address privacy and civil liberties concerns of this type throughout the course of the Evaluation Environment.

10. Is the information subject to retention limits?

Each government entity that obtains and documents information concerning suspicious activities at the federal or SLT levels may retain such information only in accordance with applicable law and policy. Retention limits, if any, can vary significantly across ISE participant organizations and may depend upon the type of information contained in the ISE-SAR. For SLT law enforcement, ISE-SAR information is considered fact-based information rather than criminal intelligence and may be subject to the requirements of 28 CFR Part 23. If an ISE-SAR also meets 28 CFR Part 23 criteria, it may be submitted to a criminal intelligence information database, and the information in the criminal intelligence system would be subject to the five-year review and validation/purge requirement under 28 CFR Part 23.[18] (Note that a state law, municipal code, or department policy may impose a more restrictive retention requirement on criminal intelligence information.) However, as a SAR, its retention would continue to be governed by state law, municipal ordinance, or agency policy.

[18] At the time of this writing, 28 CFR Part 23 is currently under revision and the noted five-year review timeframe may change.

Given the wide variability in retention standards, it is impossible to define a fixed retention limit for all ISE-SARs without simply adopting the shortest retention period applicable to any ISE participant organization. One of the lessons learned from the terrorist attack of September 11, 2001, is that individual "dots" of information may not paint a picture until a later-acquired piece of information ties them together; thus discarding ISE-SARs too quickly could negatively affect the government's counterterrorism activities. Conversely, retention periods are an important aspect of data quality and a valuable information privacy safeguard. Rather than impose a single retention standard for all ISE-SARs, the ISE-SAR Functional Standard allows submitting organizations to manage retention (control) of ISE-SARs within their own ISE Shared Space (see Q&A #15 for ISE Shared Spaces definition.) Accordingly, the following two elements included in the Functional Standard allow submitting organizations to "tag" the privacy fields with "purge" or "review" (and purge if not validated) dates:

- The *Report Purge Date:* the date by which the privacy information (information in privacy fields) will be automatically purged from the record system; general observation data is retained.
- The *Report Purge Review Date*: the date for conducting a review to determine the disposition of the privacy fields in a Detailed ISE-SAR record (i.e., the review date).

Unlike the *Report Purge Date,* which automatically removes the privacy fields, the *Report Purge Review Date* alerts a human to conduct a review to determine, based on a validation process, whether some or all of the privacy fields should be purged. The submitting organizations' business rules will determine whether or not privacy fields will be purged from the record. The analyst's determination to extend the report purge date must consider the continued value of the privacy fields in light of policies limiting retention of sensitive data by law enforcement entities. It should be noted, however, that the ability to control the purge or review dates for privacy-protected information extends only to ISE-SARs that reside in the submitting organization's Shared Space. In the event future functionality authorizes bulk information to be copied (downloaded) from the ISE Shared Space and incorporated into another information system, such information would not automatically be purged or reviewed unless required by the receiving entity's business rule.

11. Do individuals have any ability to control how SAR privacy information about them is collected, used, or shared by the original collector (source agency)?

Generally, no. However, each government entity that collects and documents suspicious activities at the federal, state, local, or tribal level must do so in accordance with applicable law and policy. Again, it is impermissible for entities to collect information based on factors the consideration of which would violate a subject's civil rights and civil liberties (e.g., race, ethnicity, national origin, religious preference, or freedoms protected by the Constitution (speech or political association) that have no reasonable relation to the criminal activity).

The Privacy Act of 1974 and Freedom of Information Act (FOIA) provide mechanisms by which individuals can determine what information about them is available in federal records. The

Privacy Act generally requires federal agencies to ensure that the information collected about individuals is complete, accurate, and timely. Similar laws have been enacted in many states. These federal laws, and the laws of many states, however, allow agencies to exempt law enforcement-related records from disclosure and data quality requirements under information access, privacy, and sunshine laws that would otherwise give individuals the ability to access or correct records about themselves.

Under the Privacy Act, federal agencies need not in all cases obtain an individual's consent in order to disclose information collected about the individual. The Privacy Act permits agencies to publish "routine uses," articulating the circumstances in which collected information may be disclosed routinely, provided the use is for an agency purpose compatible with the purpose for which the information was initially collected. Generally speaking, information collected for a law enforcement purpose may be shared outside the agency for law enforcement purposes, without consent of the individual to whom it pertains.

See also Q&A #13 below regarding redress under the ISE Privacy Guidelines.

12. Do individuals have any ability to request and obtain SAR information maintained about them from the original collector?

Theoretically, yes. In the federal system the procedure by which individuals may request and obtain information maintained about them is governed by the FOIA and the Privacy Act. In the state and local arena there exist similar laws and requirements, often referred to as "Sunshine Laws." However, as noted, access to SARs information may be extremely limited under disclosure exemptions available for law enforcement records.

13. Can individuals correct the SAR information if they believe it to be inaccurate? If so, what is that mechanism?

Neither the ISE-SAR Functional Standard nor other provision of law or regulation dictates a common process or standard that applies to the correction of information contained in ISE-SARs by subject individuals.

Because of the disclosure exemptions that typically apply to law enforcement records, ISE-SAR subjects generally will not have access to government files and therefore have no way to ascertain the accuracy of records about them. Privacy laws typically exempt law enforcement records from amendment (correction) requirements as well, so that even when access to records is obtained, e.g., through discovery in litigation, the exemption from amendment still applies. However, consistent with the ISE Privacy Guidelines, both federal agencies and SLT agencies such as fusion centers that anticipate participating in the ISE and receiving terrorism-related information directly from federal agencies will be required to have procedures in place for addressing complaints (redress) from individuals who believe the authorities possess inaccurate information about them and who request that erroneous information be corrected. Additionally, individuals may be able to seek assistance within the appropriate federal or state court system.

As part of the Evaluation Environment effort, consistent with the Data Quality provision of the ISE Privacy Guidelines, sites will be asked to develop a specific data quality and redress process for correcting or purging information discovered or reported to be inaccurate. The authors of this report recommend that sites implement business processes, including steps to vet or validate the accuracy of observations, tips, leads, or other incident reporting and to remove from, or update in, an ISE Shared Space any ISE-SAR determined to be deficient or unfounded (e.g., redress) (see Recommendation B(1)(b)).

14. Will personal information be shared by the SAR Evaluation Environment sites? Will there be variations in availability of Detailed ISE-SARs versus Summary ISE-SARs?

Yes, personal information in designated privacy fields will be shared by the SAR Evaluation Environment sites upon demonstration that adequate privacy protection policies are in place.

The ISE-SAR Functional Standard provides two ISE-SAR information exchange formats—”Detailed” and “Summary”—that are the principal mechanism for varying information content based on the operational situation. By flagging specified privacy fields, the ISE-SAR Functional Standard allows for either a Detailed Report (inclusive of privacy fields) or Summary Report (exclusive of privacy fields) to be made available as appropriate to the circumstances, e.g., whether a mission need is served by sharing personal information, limitations on receipt, or disclosure of privacy elements by particular ISE participants. The Detailed ISE-SAR information exchange includes all defined data elements (including privacy protected fields such as name, address, vehicle registration, etc.). The Summary ISE-SAR information exchange includes all data elements except those flagged as privacy fields. The data fields coded as privacy fields in the ISE-SAR Functional Standard are the minimum data that all jurisdictions would likely consider to be privacy protected. Each ISE participant can exclude additional privacy fields from the Summary ISE-SAR information exchange package in accordance with its own legal and policy requirements.

Using point of contact (POC) information established in the IEPD, entities accessing Summary ISE-SARs will be able to contact the source organization if further analysis or investigation demonstrates the need for additional (detailed) information concerning a particular report. Law enforcement personnel having a legitimate reason to obtain the identity of an individual, or individuals, referred to in a Summary SAR would do so through established investigative channels. In addition, the authors of this report recommend that the CONOPS prohibit users from “reverse engineering” Summary ISE-SAR information in an effort to determine the identity of protected persons (see Recommendation (B(1)(j)). The relative value of the Summary and Detailed ISE-SARs ultimately will be tested as part of the ISE-SAR Evaluation Environment initiative. However, in view of privacy and civil liberties concerns when sharing information about ostensibly “criminal” and “terrorism-related” activity, the authors of this report recommend that the first ISE-SAR Evaluation Environment sites to test the ISE-SAR Functional Standard make available only Summary ISE-SARs. The ISE-SAR Evaluation Environment sites will save Detailed ISE-SARs to the Shared Space, but until they develop or adopt policies and procedures to ensure that appropriate privacy and civil liberties protections are in place, the results to an ISE-SAR search will be viewable only without the privacy fields. Once the ISE-SAR Evaluation Environment sites have demonstrated that the necessary privacy and civil liberties policies are in place, they may share ISE-SAR information in the Detailed ISE-SAR format. (See Recommendation C(2).)

In addition, the ISE-SAR Functional Standard contains a "Dissemination Description Code" (generally established locally) that permits the submitting organization to specify "who gets what." This code enables the submitting organization to code the ISE-SAR to limit the authorized recipients of the ISE-SAR within the ISE Shared Spaces, possibly by using CUI designations. (See President's Memorandum for the Heads of Executive Departments and Agencies, "Designation and Sharing of Controlled Unclassified Information (CUI)," May 9, 2008.)

15. How will ISE-SARs be maintained and shared (e.g., what systems are used)?

Per the ISE-SAR Functional Standard, the following steps would apply:

- An ISE participant (the "submitting organization") designates and formats a Detailed ISE-SAR in accordance with ISE-SAR Functional Standard (see Q&A #3).
- The submitting organization stores the ISE-SAR in a dedicated SAR system (the ISE Shared Space). Such system should meet the standards of an ISE Shared Space, as described in Version 1 of the ISE Enterprise Architecture Framework (ISE EAF):

> "This infrastructure remains outside a participant's internal network, yet is still under the management and control [including infrastructure, policy and internal processes] of that ISE participant. The ISE Shared Space is designated to host ISE participant shared services and data. For example, in the case of an ISE-SAR, the Shared Space of a participant would be the access point, and optionally the repository, for SAR data. ISE participants will determine their services and data appropriate for sharing based upon applicable policy and internal processes. Those shared services and data will be placed in a separate area behind the organization's network firewall, but within the ISE Shared Space. The ISE Shared Space is the key to the ISE Core which is the information transport for the participants' capabilities." (Information Sharing Environment Enterprise Architecture Framework, August 2007, p. 32)

As reflected in the ISE-EAF, the agencies' ISE-SAR Shared Spaces will be capable of sharing data at the appropriate level (Detailed or Summary) based on identified criteria and policies. Each submitting organization must manage its Shared Space to give effect to applicable legal, privacy, and other policy requirements with respect to access to information contained in the privacy fields. SARs in the ISE Shared Space will remain under the exclusive control of the submitting organization, which may replace (update) or delete the record based on additional information or consistent with purging or retention requirements.

Given the breadth of the ISE and the fact that ISE Shared Spaces have not yet been created and enabled, it is not possible to list the specific systems that will be used to store and retrieve ISE-SAR information.

The ISE-SAR Functional Standard and ISE Shared Spaces concept are being implemented and tested as part of the ISE-SAR Evaluation Environment. Each fusion center participating in the ISE-SAR Evaluation Environment will copy the SARs it has designated as ISE-SARs onto its own separate server ("Shared Space") in accordance with applicable laws, regulations, and policies for protecting privacy information, including purging and retention requirements. The Fusion Center ISE Shared Spaces server is connected to one of several existing unclassified, protected networks (e.g., Regional Information Sharing Systems Network (RISSNET), Law Enforcement Online (LEO), Homeland Security Information Network (HSIN), or (potentially) Director of National Intelligence (DNI) Unclassified (DNI-U)). These systems connect the fusion center ISE Shared Space server to a federated environment architected and enabled to provide an aggregate query function (from a central, DOJ-hosted Web page) for linking the distributed ISE-SAR data.

As the operational aspects of the ISE-SAR initiative evolve, the potential functionality of the agency "SAR" server or an ISE Shared Space may develop further. The authors of this report recommend that the CONOPS under development for the ISE-SAR Evaluation Environment limit functionality in the ISE Shared Spaces to "read only" access and not enable annotation of postings by users of the federated search system (see Recommendation B(1)(l)). Thus a participating entity that queries the federated system and identifies a connection between two or more records in various Shared Spaces would need to take affirmative steps to alert the respective source organizations to update their records. Future functionality may permit users to access and incorporate ISE-SARs posted by submitting organizations into their own information systems or to participate in a community of users, e.g., Wikipedia style, where they can add to the submission. Should these capabilities be realized, the privacy and civil liberties ramifications will be assessed for each possible "use" scenario.

16. With whom (agencies, organizational elements, and personnel) is a Detailed ISE-SAR shared?

In the initial ISE-SAR Evaluation Environment sites, and until adequate privacy protections have been determined to be in place, Detailed ISE-SARs will be placed in the Shared Space but will not be shared. Eventually (most likely after the Evaluation Environment is completed), Detailed ISE-SARs should be available to all credentialed participants possessing access to the RISSNET, LEO, and designated HSIN networks. These unclassified, secure systems are virtual, secure connections between different servers that ride the Internet. They vet members prior to granting access to information databases on the "network." In the case of RISSNET, for example, access is limited to agencies with law enforcement responsibilities or functions, and users may have access only to specific databases on the network. Depending upon the access rules governing the system or network, submitting organizations may need to exclude from

Detailed ISE-SARs privacy field information that cannot be provided to other users or classes of users. The submitting organization will ensure that its own ISE Shared Space system accommodates applicable privacy and other legal requirements.

As it relates to the ISE-SAR Evaluation Environment initiative, the sharing of ISE-SARs will take place between law enforcement, homeland security, public safety, and other credentialed personnel. The expectation is to share non-privacy related ISE-SAR information to the maximum extent through the Summary ISE-SAR format, while making available the Detailed ISE-SAR where appropriate and necessary, and subject to applicable legal and policy limits. The ISE Privacy Guidelines and any further guidance issued by the PM-ISE or the ISE Privacy Guidelines Committee also potentially govern the sharing of ISE-SARs.

Longstanding policies and rules governing how law enforcement information is shared with the Intelligence Community will be applied when determining how ISE-SARs will be made available to members of the Intelligence Community.

17. With whom (agencies, organizational elements, and personnel) is a Summary ISE-SAR shared?

The expectation is that Summary ISE-SARs shall be available via the agency SAR system or Shared Space to authorized personnel at all ISE participating organizations.

18. How will access to ISE-SARs be authorized and by whom?

See Q&A #14. The ISE-SAR Functional Standard contains a "Dissemination Description Code" (generally established locally) that permits the submitting organization to specify "who gets what." This code enables the submitting organization to limit the recipients of the ISE-SAR, based on applicable governing authorities. In the long term, the intent is to establish an ISE-wide system of attribute-based access controls that would manage access authorization based on the class or operational role of the ISE participant requesting access. Under such a system, it would be possible, for example, to grant full access (including privacy fields) to one set of users, where such users have a need for such fields, partial access (entire ISE-SAR minus privacy fields), or, in some cases, no access to ISE-SARs. Realization of this goal will require the development and issuance of common access standards and requirements across the ISE.

19. Are there use restrictions on ISE-SARs? Describe all uses of the data.

The ISE-SAR Functional Standard was not intended to cover restrictions on how ISE-SARs will be used once the information was inputted and formatted in accordance with the standard.

The ISE-SAR Evaluation Environment will contain use restrictions. As provided in the ISE-SAR Evaluation Environment CONOPS under development, ISE-SARs will be used only to support U.S. law enforcement (LE) and counterterrorism (CT) activities.

Authorized LE and CT uses include:

- ***Investigation.*** ISE-SARs can be used to support criminal investigations of possible terrorist activities by federal, state, and local law enforcement officers.
- ***Analysis.*** ISE-SARs are one source of information that analysts use to develop and issue terrorist threat reports for LE and CT activities. Analysts may use information from a number of sources in producing alerts, warnings, and notifications; situational awareness reporting; or strategic threat or risk assessments.
- ***Information Needs.*** ISE-SARs may be used to help develop priority information needs.

At SLT levels, the use and sharing of information for each of these purposes is governed by agency policy, municipal codes, state and tribal laws and constitutions, and the U.S. Constitution.

In its final draft report, the *SAR Support and Implementation Project*[19] finds and recommends that participating agencies and entities should evaluate and update their privacy and civil liberties policies and related training to ensure that the information privacy, civil liberties, and other legal rights of Americans are protected in the use of SAR data. (See Recommendation B(2)(b))

To the extent that information contained in ISE-SARs, or that is derived from ISE-SARs, is made available to agencies within the Intelligence Community (IC), such information could be used, to the extent it contains U.S. person information, only in a manner consistent with the relevant agency's Attorney General-approved guidelines pursuant to Executive Order 12333. IC agencies should note that even Summary ISE-SARs may contain information identifying a U.S. organization or corporation. In addition, while ISE-SARs have been determined to have a nexus to terrorism, no determination has been made that such SARs are related to international terrorism (because homeland security information and law enforcement information related to terrorism, unlike "terrorism information" as defined for the ISE, need not be related to international terrorism). Thus ISE-SARs do not necessarily constitute foreign intelligence or counterintelligence information, the necessary threshold criterion for collection by an IC element.

Moreover, separate criteria exist for nominating individuals to the U.S. Government's Consolidated Terrorist Watch List. That watch list is administered by the Terrorist Screening Center of the FBI. An ISE-SAR is not a basis for placing an individual on the watch list.

The authors of this report recommend that business processes be developed to implement user restrictions for ISE-SARs. In particular, program documentation and business processes must make clear that documentation of information in an ISE-SAR cannot be used as the sole basis for action to be taken against an individual. ISE-SARs are for lead purposes only, and remain subject to all applicable laws and policies. Users of ISE-SARs should be trained on the inherent limitations of such information, and appropriate notices should be put in place advising users

[19] The final draft can be found at http://online.wsj.com/public/resources/documents/mccarecommendation-06132008.pdf.

of such limitations (e.g., appropriate use-limitation markings could be placed on ISE-SAR documents; use-limitation notice screens could be used on ISE-SAR shared spaces) (see Recommendation B(1)(k)).

20. Does maintaining ISE-SARs in an ISE Shared Space create a Privacy Act system of records? If so, is there a routine use that covers sharing with relevant ISE participants?

Depending upon how the SAR systems or ISE Shared Spaces are implemented by the ISE participants, maintenance of ISE-SARs on such ISE Shared Spaces by federal entities may create a system of records under the Privacy Act, the existence and character of which must be published in the Federal Register. A Privacy Act "system of records" is a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, etc. Each federal ISE participant organization that administers a Detailed ISE-SAR Privacy Act system of records in its SAR system or ISE Shared Space must develop and publish a "routine use," which authorizes it to disclose ISE-SAR information outside the agency. A routine use is a published statement by an agency that articulates, with respect to one or more system of records, to whom and for what purpose information from individuals' Privacy Act records may be disclosed outside the agency.

21. Will there be a mechanism or requirement to notify the submitting organization of information believed to be inaccurate or information improperly designated as an ISE-SAR so that corrective action can be taken?

Currently, the process envisioned for notifying either the source organization or the submitting organization of information that may be inaccurate or improperly designated as having a terrorism nexus is set forth in Section 5b of the ISE Privacy Guidelines:

> ***Notice of Errors.*** Each agency, consistent with its legal authorities and mission requirements, shall ensure that when it determines that protected information originating from another agency may be erroneous, includes incorrectly merged information, or lacks adequate context such that the rights of the individual may be affected, the potential error or deficiency will be communicated in writing to the other agency's ISE privacy official…

Each entity participating in the ISE-SAR Evaluation Environment will be required to adopt an appropriate policy for error notification (as well as policies ensuring other privacy protections, as set forth in the ISE Privacy Guidelines). Feedback mechanisms may be kept simple, employing either telephone or e-mail.

The PM-ISE will require participants in the ISE-SAR Evaluation Environment to provide feedback regarding notice of errors in three areas in order to maximize the effectiveness of ISE-SAR sharing and protect the privacy and civil liberties of record subjects. These three areas are:

- Feedback to originators when fact information is incorrectly designated as ISE-SAR
- Feedback to all participants if further evidence determines that an ISE-SAR was designated incorrectly
- Recommended changes to the ISE-SAR Criteria Guidance (Part B of the ISE-SAR Functional Standard)

22. What security measures or safeguards will be implemented to protect the information in ISE Shared Spaces and in the federated system (e.g., encryption, classification, other)?

Although ISE-SARs will not be classified, they will be considered law enforcement sensitive and thus warrant protection. The President's new directive concerning Controlled Unclassified Information (CUI) has not yet been fully implemented; however, it is anticipated that ISE-SARs will be handled with appropriate markings and safeguards to protect sensitive information. As with other such information, ISE-SARs shall be stored, processed, and disseminated in a protected information environment that provides adequate security controls. These safeguards may include:

- Controlled access to the information that will allow only authorized ISE users to access, retrieve, and display ISE-SAR information and restricts writing and updates to authorized members of the submitting organization
- Encrypted transmission of information shared between participating organizations

The distributed model itself affords protections and is superior to a centralized model in that it allows for control of data; the ISE-SAR is updated as necessary by authorized members of the source organization, rather than pushed to a repository beyond the submitting agency's control where it remains static and ages. In addition, the distributed model better protects the information, in that it allows for individualized data use agreements between participants. As further protection, the ISE-SAR Evaluation Environment sites will be strictly governed. Formal agreements for the sharing of data with other federal, state, local, or tribal law enforcement agencies will be established among participants, outlining the policies, procedures, and practices for the handling and use of information (including adherence to the requirements of the ISE Privacy Guidelines).

23. Can the data be modified? By whom? Is there a system for tracking modifications?

The CONOPS currently under development for the ISE-SAR Evaluation Environment initiative prescribes that ISE-SARs remain under exclusive control of the submitting organization, which may update the initial record based on additional information provided by the source agency. For purposes of the Evaluation Environment effort, the submitting organization is the only organization authorized to replace (update) or delete ISE-SARs. As previously noted, should the ISE-SAR be imported into another agency's system or subject to collaborative efforts on the part of authorized users, examination of applicable business rules and related privacy and civil liberties protections would be warranted.

24. Will the data be available for searching?

Yes. In the ISE-SAR Evaluation Environment, ISE-SARs will be available in ISE Shared Spaces for search and retrieval in accordance with the ISE EAF. The CONOPS under development for the ISE-SAR Evaluation Environment envisions that, ultimately, depending on roles, authorizations, and specified purpose, ISE participants may retrieve, as appropriate, either the Detailed or Summary ISE-SAR record. However, the authors of this report recommend that the CONOPS being developed will permit the first Evaluation Environment sites to share only Summary ISE-SARs from their ISE Shared Space, with detailed privacy fields disclosed only through individualized contact with the submitting agency. The CONOPS will stipulate that Detailed ISE-SARs may be accessed through the Shared Space only after the ISE-SAR Evaluation Environment sites have adopted appropriate policies for protecting privacy and civil liberties. The authors of this report recommend that the CONOPS prohibit users from "reverse engineering" Summary ISE-SAR information in an effort to determine the identity of protected persons (see Recommendation B(1)(j)). Thus, users with access only to Summary ISE-SAR information will not be able to access the privacy fields within the Detailed ISE-SARs.

In addition the authors of this report recommend that the CONOPS require the ISE-SAR Evaluation Environment sites to recognize only those inquiries that provide a case, incident, or other justification; will limit the number of records that can be accessed in response to the inquiry; and, will permit "read only" access (see Recommendation B(1)(l)). In the future, should users be enabled to more freely access and incorporate ISE-SARs from the submitting organization's SAR system or ISE Shared Space or modify a submission, a full examination of the applicable business rules and policies will need to be undertaken. Central to that examination, for example, would be whether the policies and practices of the submitting organization (e.g., purge dates, dissemination limitations) continue in effect for ISE-SARs accessed and incorporated into another agency's system.

25. How will the data be retrieved? Can it be retrieved by personal identifier?

The ISE-SAR Functional Standard assumes that ISE-SAR information may be retrieved using a variety of search keys, including personal identifiers in the event that a user has access, based on need, to Detailed ISE-SARs. Using such personal identifiers as the search key results in a more narrowly focused set of search results than would be available using broader categories such as geographic area. Federal entities administering their ISE-SARs by personal identifier must comply with the requirements of the Privacy Act to establish a Privacy Act System of Records Notice (see Q&A #20).

26. Can ISE-SAR data be merged with data from another system (e.g., reverse telephone directory)?

The ISE-SAR Functional Standard does not dictate how ISE-SAR data will be merged with data from other systems.

In the current ISE-SAR Evaluation Environment initiative, the answer is "no." For example, while a fusion center could make a reverse telephone directory available for analytic or investigative use, separate from the ISE-SAR Evaluation Environment, the directory capability would not be integrated into the ISE-SAR Evaluation Environment. In the future, any merging of ISE-SAR data with data from other systems will be fully assessed in terms of business rules and privacy and civil liberties protections, including the merger provision of Section 5c.(i) of the ISE Privacy Guidelines.

27. Will analysis be conducted as part of the ISE-SAR Evaluation Environment initiative?

One of the purposes of developing the ISE-SAR Functional Standard and an integrated ISE-SAR process is to allow authorized ISE participants to identify and analyze incidents and observations that, taken together, may provide indicators of terrorist plans or activities. This analysis would be done locally by analysts. To this end, the ISE-SAR Functional Standard standardizes the format and content of an ISE-SAR. However, development and use of specific tools and techniques to support pattern and trend analysis are not part of the ISE-SAR process. ISE participants may employ local tools or techniques as appropriate. The ISE-SAR Evaluation Environment initiative is designed to provide controlled access to ISE-SAR information hosted by a state or major urban area fusion center through a federated search capability. A federated search allows a user to search all available data repositories for which they are authorized for specific information via a single search interface. The single federated search interface should allow a user the ability to formulate a query based on a set of parameters and subsequently narrow the search through more specific parameter refinement. Pursuant to the ISE-SAR Functional Standard, search results will be structured in the IEPD format so that such results may also be processed in other applications used by the analyst. The functionality may include a link analysis tool. To conduct a link analysis, users must separately enter their ISE-SAR search results into whatever software they have that enables that type of analysis.

28. What type of training will be required for users of the data?

The authors of this report recommend that users of ISE-SARs receive training about the basic ISE-SAR business process; the ISE-SAR information flow description (Part C of ISE-FS-200); guidance on the criteria for designating an ISE-SAR (Part B of ISE-FS-200); application of the ISE

Privacy Guidelines to the ISE-SAR business process and, as appropriate, guidance on other privacy and civil liberties implications of the ISE-SAR process (e.g., racial, ethnicity, national origin, or religion-based profiling concerns and other constitutional rights issues). (See Recommendations B(1)(a) and B(3)(a).) ISE-SAR training will be developed through the ISE-SAR governance structure. The ISE-SAR governance structure will be detailed in the CONOPS.

29. What auditing and technical safeguards are in place to prevent misuse of the data?

The ISE-SAR Functional Standard standardizes the format and content of an ISE-SAR but does not address the auditing and technical safeguards applicable to agencies' SAR systems or ISE Shared Spaces. These safeguards and procedures, such as retention of inquiry and access log data and frequency of audits, vary from state-to-state, agency-to-agency, and department-to-department. Accordingly, consistent with paragraph 11 of the ISE Privacy Guidelines, the authors of this report recommend that the CONOPS for the ISE-SAR Evaluation Environment require the Evaluation Environment sites to establish and implement auditing and technical safeguard requirements that are as comprehensive as those required by the ISE Privacy Guidelines (see Recommendations A(5) and B(1)(i)).

30. Is there a requirement to notify the submitting agency prior to further disclosure of the ISE-SAR?

The ISE-SAR Functional Standard does not embrace operational, on-the-ground, sharing practices by participating agencies. Initially, for purposes of the ISE-SAR Evaluation Environment initiative, access to information in the participants' ISE Shared Spaces will be based on a case, incident, or other justification; limit the number of records that can be accessed in response to the inquiry; and, permit "read only" access. However, in the future, if ISE participating organizations are authorized to access and incorporate data from other entities into their own databases, or collaborate by providing input to submitting agency ISE-SARs, the development of business rules for such sharing or record modification will need to be addressed. The CUI framework may govern secondary disclosure in some circumstances.

Summary

To enhance the utility of terrorism-related suspicious activity and incident reporting, both practically and analytically, the ISE-SAR Functional Standard provides a framework for the standardized documenting of ISE-SARs that are intended to be disseminated to ISE participants. Broad adoption of the ISE-SAR Functional Standard will facilitate increased ISE-SAR sharing, making protection of privacy and civil liberties critical to the ISE-SAR Evaluation Environment initiative.

That the ISE-SAR Functional Standard establishes a convention for representing ISE-SAR information using common criteria and data elements is both its strength and weakness from a privacy and civil liberties protection perspective. The ISE-SAR Functional Standard does not prescribe the business rules (processes and procedures) that source organizations must follow for collecting, analyzing, maintaining, or sharing ISE-SAR data; these procedures and analytical processes remain organization-specific. Accordingly, the foregoing Q&A section identifies those areas where ISE-SAR entities must develop business rules and examine the attendant privacy and civil implications of proposed operational choices.

Recommendations

A. General

The authors of this report support the privacy and civil liberties measures recommended in the *Findings and Recommendations of the SAR Support and Implementation Project.* Based on site visits to and evaluations of the model of the LAPD and police departments in Boston, Chicago, and Miami, the *Findings and Recommendations of the SAR Support and Implementation Project* urge entities engaged in SARs activities to consider the following measures:

1. Promote a policy of openness and transparency when communicating to the public regarding their SAR process;

2. Integrate the management of terrorism-related suspicious information with processes and systems used to manage other crime-related information and criminal intelligence, thereby leveraging existing policies and protocols that protect the information privacy, civil liberties, and other legal rights of Americans; clearly articulate when 28 CFR Part 23 should be applied;

3. Ensure privacy and civil liberties policies address core privacy principles, such as accuracy, redress, retention/disposition, and disclosure of personally identifying information, consistent with federal, state, and local statutory and regulatory requirements;

4. Evaluate and, as necessary, update privacy and civil liberties policies to ensure that they specifically address the gathering, documenting, processing, and sharing of terrorism-related information;

5. Audit SARs for quality and substance to ensure that the integrity of the SAR program is maintained; and,

6. Use legal and privacy advisors in the development of the SAR process.

B. ISE-SAR Evaluation Environment

The authors of this report recommend that the program documentation for the ISE-SAR Evaluation Environment initiative (i.e., CONOPS, program guidance, participation agreements) require, as appropriate to the purpose and audience for each document, the following specific measures addressing “key” privacy and civil liberties issues:

1. **Develop business processes:** Implement mechanisms to ensure suspicious activity reporting protects civil rights and civil liberties, including business processes that

   a. incorporate checks/procedures to ensure against "profiling" on race, ethnicity, national origin, or religious grounds or violating a person's constitutional rights (training and written guidance in these areas will assist law enforcement professionals to determine when these criteria have proper investigatory significance)[20] (see Q&A #28);

   b. include steps to vet or validate the accuracy of the observations, tips, leads, or other incident reporting and to remove from, or update in, an ISE Shared Space any ISE-SAR determined to be deficient or unfounded (e.g., redress) (see Q&A #8 and #13);

   c. require an ISE-SAR be based on the ISE-SAR criteria (Part B of the ISE-SAR Functional Standard) and establish a potential nexus to terrorism (see Q&A #4);

   d. provide multiple layers of review and vetting (see Q&A #5);

   e. require a demonstration of need for personal information elements (privacy fields) before sharing those elements from the Detailed ISE-SARs (see Q&A #14);

   f. provide notice to sources or users of errors in the content or designation of an ISE-SAR (see Q&A #21);

   g. provide notice of source reliability and content validity of an ISE-SAR (see Q&A #8);

   h. include maintenance of detailed information logs (queries, accesses) (see Q&A #29);,

   i. include an audit element and technical safeguard requirements (see Q&A #29);

   j. prohibit users from "reverse engineering" Summary ISE-SAR information in an effort to determine the identity of protected persons (see Q&A #14 and 24);

   k. implement user restrictions for SE-SARs, such as user training, and user notification mechanisms (see Q&A #19); and

   l. limit functionality in the ISE Shared Spaces so that access to will be based on a case, incident, or other justification; limit the number of records that can be accessed in response to the inquiry; and permit "read only" access (see Q&A #15, 24, and 30).

2. **Develop privacy, civil rights, and other civil liberties protections consistent with the ISE Privacy Guidelines:** Develop and implement privacy policies that afford protections that

[20] See, e.g., International Association of Chiefs of Police (2006) "Protecting Civil Rights: A Leadership Guide for State, Local, and Tribal Law Enforcement." available at: http://www.cops.usdoj.gov/files/ric/Publications/e06064100.pdf http://www.theiacp.org/documents/pdfs/RCD/PCR_LdrshpGde_Part3.pdf.

are at least as comprehensive as those required of federal agencies participating in the ISE under the ISE Privacy Guidelines.

a. As highlighted throughout this analysis, paragraph 11 of the ISE Privacy Guidelines reflects that non-federal entities, to participate in the ISE, must "develop and implement appropriate policies and procedures that provide protections that are at least as comprehensive as those contained in these [ISE Privacy] Guidelines." The ISE-SAR Evaluation Environment sites that anticipate receiving information from federal entities (e.g., fusion centers and some local agencies) should designate a "privacy official" to coordinate review of existing policies and adoption of ISE-SARs policy and to oversee ISE-SARs privacy policy implementation. (See Q&A #13.)

b. To evaluate whether their terrorism-related information sharing operations appropriately consider the information privacy and legal rights of Americans, ISE-SAR Evaluation Environment sites should review their privacy and civil liberties policies and related training. To this end, ISE-SAR Evaluation Environment sites should be encouraged to consult the Global's templates for privacy policy development and the *Guide to Conducting Privacy Impact Assessments for State and Local Information Sharing Initiatives (DRAFT)*[21]. (See Q&A #19.)

c. Federal entities documenting suspicious activities should be mindful that most Detailed ISE-SARs contain protected information subject to the requirements of the ISE Privacy Guidelines. Accordingly, federal entities that share Detailed ISE-SARs must ensure that protected information in ISE-SAR systems and ISE Shared Spaces is protected consistent with ISE Privacy Guidelines and with the requirements of federal privacy law. Likewise, federal entities documenting suspicious activities must do so consistent with civil rights and civil liberties requirements and should employ mechanisms affording the necessary protections. See, e.g., United States Department of Justice, Civil Rights Division (2003), "Guidance Regarding the Use of Race in Law Enforcement Agencies."[22] (See Q&A #28.)

3. **Develop and Provide Appropriate Training and Documentation:**

a. Recommend training and guidance documentation on how to apply the criteria in Part B of the ISE-SAR Functional Standard to minimize the risks of over-inclusiveness and inappropriate reporting (See Q&A #4);

b. Recommend program documentation supporting the ISE-SAR Evaluation Environment (CONOPS, participation agreements, etc.) require ISE-SAR Evaluation Environment sites to obtain assurances from source agencies that all personnel (e.g., front line

[21] The *Guide to Conducting Privacy Impact Assessments for State and Local Information Sharing Initiatives* was developed by Global's Privacy and Information Quality Working Group. At the time of this writing, the document is under final review and is on the agenda for the Global Justice Advisory Committee October 2008 meeting.

[22] United States Department of Justice, Civil Rights Division (2003), "Guidance Regarding the Use of Race in Law Enforcement Agencies" document is available at http://www.usdoj.gov/crt/split/documents/guidance_on_race.htm

personnel, senior and expert officers, investigators/analysts) involved in the gathering, processing, reporting, analyzing, and sharing of suspicious activity information have been trained on the ISE-SAR Functional Standard criteria (See Q&A #4); the ISE-SAR business process and information flow; and on the privacy and civil liberties implications of suspicious activity reporting (e.g., constitutional and other legal protections). (See application of the ISE Privacy Guidelines in the ISE-SAR context (see Q&A #28) and U.S. person-related collection limitations (see Q&A #19).)

c. The grantor agency should formally obtain participants' agreement to comply with the terms and requirements of the initiative as reflected in the CONOPS and other program implementation guidance. (Best practice.)

d. Applicable documentation should be revised to clarify meaning of "illicit activity," (see Q&A #1) and to otherwise be consistent with the recommendations in this Analysis).

e. Recommend that agencies participating in the ISE-SAR Evaluation Environment develop privacy and civil liberties protection policies and guidance documentation that is designed to accompany, complement, and/or be integrated with its SAR documentation and guidance.

C. Initiating the ISE-SAR Evaluation Environment Effort

As an initial matter, the authors of this report recommend the following steps:

1. ISE-SAR Evaluation Environment sites should develop or adopt and implement robust privacy, civil rights, and civil liberties protection policies for all its information collection, use, storage, and sharing activities (best practice).

   In particular, the CONOPs should require that participating fusion centers adopt an umbrella ISE-SARs Evaluation Environment Privacy and Civil Liberties Protection Policy or evaluate and, if necessary, update their existing privacy and civil liberties policy to ensure that the gathering, documenting, processing, and sharing of ISE-SARs is consistent with the umbrella policy. The CONOPS will also require each participating site to document the manner in which the ISE-SAR information is being posted and shared via the Shared Space and how the site is complying with its ISE-SAR privacy and civil liberties protection policy. (See general discussion preceding Privacy and Civil Liberties Analysis).

2. ISE-SAR Evaluation Environment sites will save Detailed ISE-SARs to the Shared Space, but until adequate privacy and civil liberties policies are in place, the results to an ISE-SAR search will be viewable only without the privacy fields (see Q&A #14).

3 ISE-SAR Evaluation Environment initiative sites should document steps taken to address the recommendations and key issues outlined in this analysis; this documentation will assist the authors of this report in evaluating whether the use of the

Detailed IEPD is appropriate and to develop a final ISE-SAR Privacy and Civil Liberties Analysis of the ISE-SAR Functional Standard, IEPD and ISE-SAR Evaluation Environment initiative (best practice).

D. PGC's Legal Issues Working Group Participation

As the ISE–SAR Functional Standard deploys to the field through the ISE-SAR Evaluation Environment initiative, the PM-ISE will enlist the assistance of the PGC's Legal Issues Working Group to ensure that participating entities receive ongoing advice and guidance with respect to protecting information privacy, civil rights, and other civil liberties. The PGC's Legal Issues Working Group will identify one or more subject matter experts to serve in an advisory capacity to the ISE-SAR Steering Committee, which in turn will deploy these experts to the ISE-SAR Evaluation Environments for field visits, consultations, and training.

Conclusion

The ISE-SAR Evaluation Environment contemplates an iterative process involving phased implementation of the ISE-SAR Functional Standard and IEPDs in diverse operating environments and continuous reexamination of the assumptions, processes, and standards for designating and sharing ISE-SARs. The authors of this report will advise the relevant ISE-SAR project committees on an ongoing basis and participate in the review and evaluation of site activities.