Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations

Nationwide Suspicious Activity Reporting Initiative

Prepared by the
Program Manager, Information Sharing Environment

July 2010

For more information, go to:

www.ise.gov

PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES ANALYSIS AND RECOMMENDATIONS

NATIONWIDE SUSPICIOUS ACTIVITY REPORTING INITIATIVE

Prepared by the
Program Manager, Information Sharing Environment

July 2010

Table of Contents

I. Introduction

This *Nationwide Suspicious Activity Reporting Initiative (NSI) Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations* ("*Analysis*") provides an update to the *Initial Privacy and Civil Liberties Analysis*[1] of the now concluded Information Sharing Environment Suspicious Activity Reporting (ISE-SAR) Evaluation Environment (EE) and Functional Standard.[2] The *Initial Privacy and Civil Liberties Analysis* reflects the commitment to ensuring that privacy, civil rights, and civil liberties protections were built into the policies and processes of the sites[3] participating in the ISE-SAR EE and resulted in: (1) the revision and adoption of the ISE-SAR Functional Standard ("revised Functional Standard"), currently Version 1.5[4]; and (2) the development of a robust and comprehensive privacy, civil rights, and civil liberties protection framework for the NSI, known as the NSI Privacy Framework.[5]

The EE served as the demonstration phase or pilot phase of the NSI. The initial sites that participated in the EE implemented the recommendations from the *Initial Privacy and Civil Liberties Analysis* and currently participate in the NSI. Additional sites will be added now that the Initiative has moved from the demonstration phase of the EE to the nationwide implementation of the NSI.

The EE validated the recommendations of the *Initial Privacy and Civil Liberties Analysis*, thus enabling Federal partners to draw upon the experiences of the EE participating sites in fortifying and refining the NSI Privacy, Civil Rights, and Civil Liberties Framework.[6] The enhanced framework is comprised of the recommendations from the *Initial Privacy and Civil*

---

[1] *Information Sharing Environment – Suspicious Activity Reporting Functional Standard and Evaluation Environment: Initial Privacy and Civil Liberties Analysis* (September 2008).

[2] Further information regarding the development and implementation of the EE can be found in the accompanying reports: (1) *Final Report: Information Sharing Environment Suspicious Activity Reporting Evaluation Environment* (January 2010) (*Final Report: ISE-SAR EE*) from the Department of Justice Bureau of Justice Assistance; and (2) *The Nationwide Suspicious Activity Reporting Initiative Status Report* (February 2010), from the Office of the Program Manager for the Information Sharing Environment.

[3] The EE ultimately encompassed twelve NSI Environment sites and three Federal agencies. The EE participating sites included: Boston Police Department (PD), Chicago PD, Florida Department of Law Enforcement (FDLE), Houston PD, Las Vegas Metropolitan PD, Los Angeles PD (LAPD), Metropolitan (Washington) DC PD, Miami-Dade Fusion Center, New York State Intelligence Center, Arizona Counter Terrorism Information Center, Seattle Police Department and the Virginia Fusion Center. As for the Federal agencies involved in the EE, the Federal Bureau of Investigations (FBI) participated through its eGuardian system; the Department of Homeland Security (DHS) shared Federal Air Marshal Service (FAMS) data; and the Department of Defense (DoD) — also using eGuardian—gathered and shared SARs in support of its Force Protection mission. Not all sites and agencies are sharing data at this time due to the requirement that each site fully implement the NSI Privacy Framework.

[4] All references to the "revised ISE-SAR Functional Standard" refer to Version 1.5

[5] See Section IV of this *Analysis* for a comprehensive discussion of the NSI Privacy Framework.

[6] Throughout the remainder of this document, the term "NSI Privacy, Civil Rights, and Civil Liberties Framework" is normally abbreviated to "NSI Privacy Framework."

Liberties Analysis, the revised Functional Standard, and the experiences of the EE participating sites reflected in this Analysis. The implementation of the NSI Privacy Framework will ensure that privacy, civil rights, and civil liberties will continue to be appropriately protected as the Initiative moves beyond the EE to the nationwide implementation of the NSI in 2010. This Analysis was prepared in consultation with the Co-Chairs[7] of the ISE Privacy Guidelines Committee (PGC) and uses the experiences of the EE participating sites to further build upon the commitment made in the *Initial Privacy and Civil Liberties Analysis* by:

- Reviewing the development and implementation of EE participating sites' privacy, civil rights, and civil liberties protections;
- Outlining the observations of EE participating site experiences;
- Updating the initial privacy and civil liberties issues identified by and resolved between Federal sponsoring agencies, participating State and local partners, and privacy, civil rights, and civil liberties advocates during the EE; and
- Making recommendations to be followed during the nationwide implementation of the NSI.

In sum, the NSI Privacy Framework enabled the EE participating sites to fulfill the dual mandates of maximizing information sharing while protecting privacy, civil rights, and civil liberties. The effectiveness of this framework is underscored by the fact that the EE participating sites did not report any breaches of personal information with regard to SAR or ISE-SAR information. Nor did they receive any complaints for redress during the EE.

Going forward, NSI participants must continue to work together to ensure that robust privacy policies and procedures are adopted, properly implemented, and continuously assessed. Participants must also actively seek out opportunities to further enhance privacy, civil rights, and civil liberties protections.

[7] The Co-Chairs of the ISE Privacy Guidelines Committee are the Chief Privacy and Civil Liberties Officer, Department of Justice; the Civil Liberties Protection Officer, Office of the Director of National Intelligence; the Chief Privacy Officer, Department of Homeland Security; and the Officer for Civil Rights and Civil Liberties, Department of Homeland Security. In addition, the Chair of the PGC Legal Issues Working Group contributed to the development of this Analysis as well as the questionnaire found in Appendix A.

II. The Critical Role of Privacy, Civil Rights, and Civil Liberties Protections in the ISE-SAR EE

The key objective of the ISE-SAR EE was to establish, at each of the EE participating sites, policies and business processes that support the gathering, documenting, processing, analyzing, and sharing of SARs while also ensuring that privacy, civil rights, and civil liberties were protected in accordance with Federal, state, and local constitutions, laws, and regulations. As a condition of participation, the EE participating sites were required to implement a privacy, civil rights, and civil liberties protection framework. This framework included the adoption of appropriate policies, the institution of specialized business processes, and the training of all involved personnel before they were permitted to post or access ISE-SARs.

The EE enabled participants to assess the value of the ISE-SAR process and the ISE-SAR Functional Standard[8] and to provide a limited evaluation of the value of the Detailed versus Summary ISE-SAR formats[9] in advancing counterterrorism goals. Following the end of the EE pilot phase, all participants provided feedback to Federal privacy officials regarding the administrative and procedural aspects of the Initiative, including the process for designating reports as ISE-SARs, the management of postings in the ISE Shared Space, the processes for correcting inaccurate information, and other relevant program implementation issues. The ISE-SAR EE proved to be a valuable tool for refining the recommendations made in the *Initial Privacy and Civil Liberties Analysis*, and confirming that these recommendations must be addressed in the nationwide implementation of the NSI. [10]

III. Recommendations for the Nationwide Implementation of the NSI in 2010

The ISE-SAR EE resulted in significant implementation progress, while revealing areas that will require enhanced focus during the broader NSI implementation in 2010. Although the sites'

[8] The ISE-SAR Top-Level Business Process is set forth in Section II(D) of the ISE-SAR Functional Standard, Version 1.5 (May 2009).

[9] See *Final Report: ISE-SAR EE*, at pages 11 and 43, for a discussion of the EE participating sites' use of the Summary and Detailed formats. The participating sites' evaluation was limited because the Evaluation Environment operated for a relatively short period of time. More data will be necessary to provide a full assessment of the implementation of the NSI Privacy Framework. It is, therefore, recommended that the NSI continue to evaluate the benefits of the Detailed and Summary ISE-SAR formats.

[10] The Program Manager for the Information Sharing Environment (PM-ISE) and the Department of Justice Bureau of Justice Assistance (DOJ BJA) conducted follow-up assessments of EE implementation using a questionnaire. *See* Appendix A for the ISE-SAR EE *Privacy and Civil Liberties Assessment Questionnaire*, and Appendix B for the *Observations of EE Participating Sites During the ISE-SAR EE*.

experiences varied,[11] all sites recognized the importance of maintaining strong privacy, civil rights, and civil liberties protections in every facet of the SAR process, including implementation of both privacy policies and the requirements of the Functional Standard. The experiences of the EE participating sites helped to shape the following recommendations which must be integrated into the nationwide implementation of the NSI.

RECOMMENDATION 1: The NSI Privacy Protection Framework must be adopted and implemented as a condition of participation in the NSI, with careful consideration of the resources necessary for full implementation.

The ISE-SAR EE required each EE participating site to develop and adopt a written policy that satisfies applicable ISE Privacy Guideline requirements as a precondition to sharing or receiving any personal information contained in the Privacy Fields that are part of the Detailed ISE-SAR format.[12] The Federal partners' insistence on compliance with this requirement ensured that robust privacy policies were in place to protect the information before information sharing activities began; it also meant that the EE participating sites were delayed in sharing or receiving Privacy Field information, due to the fact that the EE participating sites typically spent an average length of six months developing and implementing their respective privacy policies.

To assist the EE participating sites and to promote a standardized approach for developing site ISE-SAR specific privacy policies, the Joint DHS/DOJ Privacy Technical Assistance Program developed privacy policy templates, offered technical assistance, and reviewed each EE participating site's privacy policy. Additionally, the EE participating sites availed themselves of legal and compliance experts at both the state and local levels to ensure that site ISE-SAR policies complied with state open records laws and other requirements.[13]

Going forward, NSI sites should anticipate that they will need to dedicate sufficient resources and attention to facilitate the full and uniform implementation of the NSI Privacy Framework. In addition to addressing all aspects of the framework in their policies and processes, NSI sites should also implement the following:

---

[11] ISE-SAR EE participating site experiences based upon such factors as the successful development of a privacy policy, the alignment of business processes, and the availability of training resources. For further information regarding the experiences of the EE participating sites, *see* Appendix B, Section C.

[12] EE participating sites were given three options for developing privacy policies that would qualify them to share and receive personal information contained in privacy fields. The options are set forth in Section IV (D) of this Analysis. Each EE participating site developed and provided a draft privacy policy to the Privacy Policy Review Team for assessment and feedback. Once the site's policies satisfied the privacy requirements of the review team, the completed policy was recommended for approval to the Privacy Guidelines Committee Co-Chairs (privacy officials from the Office of the Director of National Intelligence, the Department of Justice, and the Department of Homeland Security) and the PM-ISE. Upon approval, DOJ/BJA was formally notified that the EE participant was authorized to "go live" in sharing and receiving privacy field information in Shared Spaces under the EE.

[13] See Appendix B, Section C (1) for further discussion.

a. At the beginning of the privacy development process, training on the NSI Privacy Framework and technical assistance must be provided to the designated privacy officer and the legal advisors at each NSI site;
b. Each NSI participating site must conduct the NSI process pursuant to its statutory authorities and its privacy, civil rights, and civil liberties policies and procedures that are "at least as comprehensive" as the ISE Privacy Guidelines and the *Baseline Capabilities for State and Major Urban Area Fusion Centers* (Baseline Capabilities);
c. Each NSI site must adopt and incorporate into existing business processes a formal and multi-layered vetting process in which each SAR is reviewed by a front-line supervisor and by an experienced investigator or analyst specifically trained in counterterrorism issues before it can be designated as an ISE-SAR;
d. Standardized training for front-line officers, investigators, analytic, and supervisory personnel must be provided and required in order to educate personnel on the purpose and use of the multi-layered vetting process required in the Functional Standard; line officers, in particular, should receive specialized training to strengthen their ability to recognize the types of behavior that may be indicative of criminal activity associated with terrorism; and
e. Local privacy, civil rights, and civil liberties advocates must be engaged at an early stage in the process to build trusted relationships between partners, the local community, and the public.

RECOMMENDATION 2: Going forward, it is imperative that each NSI site engage in outreach to members of the public, private sector partners, and privacy, civil rights, and civil liberties advocacy groups during its privacy policy development and updating process.

The ISE-SAR EE emphasized the importance of a transparent process and collaboration with the public and with privacy, civil rights, and civil liberties advocacy groups. During the EE, sites worked to provide transparency and to collaborate with the public in various ways, including:

a. EE participating sites with formalized community outreach programs successfully leveraged this resource for communicating the SAR process to the public;
b. Several sites noted plans to implement a community outreach model similar to Los Angeles Police Department's (LAPD) iWatch program;
c. Three sites took advantage of the Building Communities of Trust initiative pilot which provided sites with opportunities to engage with community advocacy groups through planning meetings and roundtable events;[14]

[14] The Building Communities of Trust initiative aims to build bridges and mutual understanding among the community groups, local law enforcement agencies, and state and major urban area fusion centers as a way of better protecting our local communities. The intent is that law enforcement officers, public safety personnel, community leaders, and citizens will be better

d. Other sites hosted community open house days and/or provided tours of facilities upon request from the public or the media; and
e. Several have reported plans to make the privacy policy available on a public website, either a fusion center-specific or Departmental website.

Going forward, the following controls should be implemented in order to further promote transparency and collaboration. First, the sites must ensure the broadest possible review of privacy policies and procedures, with due consideration given to stakeholder recommendations. Second, the sites must consistently provide thorough explanations in response to public inquiries about sites' privacy policies, information availability, and redress procedures. Third, the methods used by the sites to promote outreach and collaboration must be continually assessed for the purpose of identifying and sharing best practices. Transparency and collaboration will foster public trust and enable sites to better respond to the concerns of citizens and advocacy groups.

RECOMMENDATION 3: To mitigate the risk of profiling based on race, ethnicity, national origin, or religion, and to improve mission effectiveness, NSI participating sites must adhere to the standardized vetting process and consistently use the ISE-SAR Functional Standard criteria in the identification, documentation, and sharing of ISE-SAR information.

Federal, State, and local NSI partners recognize that mitigation of the risks associated with profiling is critical to the success of the Initiative. NSI partners must, therefore, remain vigilant in implementing the enhanced privacy, civil rights, and civil liberties protections for SARs and ISE-SARs, in order to avoid the dangers of profiling.

The privacy, civil rights, and civil liberties protections are multi-faceted and robust. First, NSI partners must implement the standardized vetting process for SARs. Second, NSI partners must ensure the consistent and objective application of the revised ISE-SAR Functional Standard criteria. The implementation of the revised ISE-SAR Functional Standard constitutes an essential safeguard supporting the NSI Privacy Framework and enhancing mission effectiveness. The revised Functional Standard expressly states that factors such as race, ethnicity, national origin, or religious affiliation or activity should not be considered as the sole factors that create suspicion (except if used as part of a specific suspect description). The revised Functional Standard serves as the basis for information to be collected for a SAR or ISE-SAR and shared by law enforcement, homeland security, and counterterrorism agencies; therefore the ISE-SAR Functional Standard must be fully and consistently implemented in each NSI site's policies and business processes. Third, NSI partners must provide specialized

able to distinguish between innocent cultural behaviors and behavior indicative of criminal activity; and local communities will play a more supportive role in combating terrorism-related crime.

training and guidance to NSI personnel in order to strengthen the ability of personnel to recognize suspicious behaviors in a uniform and objective manner. Finally, as the NSI effort grows, Federal, State, and local NSI partners must regularly assess the sites' vetting process, including determinations of "reasonably indicative", and efforts to prevent profiling.

RECOMMENDATION 4: The sites must designate a trained privacy, civil rights, and civil liberties officer who, in addition to carrying out delegated responsibilities, has access to the services of legal counsel with sufficient expertise to provide ongoing legal advice and assistance regarding privacy, civil rights, and civil liberties.

The EE demonstrated that each site should designate a privacy, civil rights, and civil liberties officer and, as needed, ensure that such officer is properly trained. The designated officer, if not an attorney, should have access to legal expertise in developing and implementing privacy, civil rights, and civil liberties policies and procedures and resolving legal issues. Few EE participating sites were able to designate or hire personnel with subject matter expertise to manage privacy, civil rights, and civil liberties issues on a full-time basis. In most cases, the sites relied upon legal staff from parent agencies or state attorney general offices to identify the relevant State and local legal and regulatory requirements for incorporation in their respective ISE-SAR or comprehensive privacy, civil rights, and civil liberties policies. Sites also used records managers and compliance officers to ensure ISE-SAR policy compliance with state open records laws and other state and local requirements.

Access to the services of a subject matter expert in the areas of privacy, civil rights, and civil liberties would have expedited privacy policy development and implementation during the EE and would have enabled the sites to access or share personal information contained in Privacy Fields earlier. Privacy officers and legal counsel are therefore necessary to ensure compliance with NSI Privacy Framework and to identify opportunities to further enhance privacy, civil rights, and civil liberties protections.

RECOMMENDATION 5: An ongoing, formalized review process must be established to ensure that business processes are aligned with privacy policies and procedures, and to assess the need for additional privacy, civil rights, and civil liberties protections.

All ISE-SAR EE participating sites recognized the importance of intermittently conducting reviews of their privacy policies and business processes. Many sites also indicated that they would conduct interim policy reviews as needed.

In order to ensure a standardized approach, a formalized review process must be established. At least annually, an onsite review team should assess adherence to and implementation of the NSI Privacy Framework. The review should include: (1) an assessment of accountability

actions, including documented changes in business processes that reflect the enhanced privacy protections; (2) documentation of any breaches involving personal information; (3) an assessment of the handling of information requests, error notifications, and complaints for redress; and (4) documentation of the delivery of required training activities.

RECOMMENDATION 6: Each participating site must exercise due diligence in implementing appropriate physical, technical, and administrative measures to safeguard information under its control from unauthorized access, disclosure, modification, use, or destruction.

The EE served to highlight security controls which are critical for ensuring appropriate safeguarding of personal information. Going forward, all NSI sites must exercise due diligence by:

a. Limiting access to ISE-SARs to agencies and individuals with proper credentials and roles;
b. Requiring a reason for all searches;
c. Implementing an appropriate electronic warning banner for users accessing the ISE Shared Space;
d. Mandating the maintenance of inquiry/access logs and audit trails; and
e. Requiring that all records provide notice about the nature and quality of the information, including confidence and dissemination codes.

RECOMMENDATION 7: Each participating site must emphasize and establish procedures to ensure personal responsibility and accountability for protecting privacy, civil rights, and civil liberties.

Although none of the EE participating sites reported a breach of personal information with regard to SAR or ISE-SAR information, personnel must remain vigilant in adhering to the site's privacy protection framework. Each site should ensure that all assigned personnel with access to SAR and ISE-SAR information review and acknowledge, on an annual basis, that they have read and understand the site's privacy policies and procedures and that they will execute their responsibilities in accordance with the site's policies and procedures.[15]

Sites should provide and require privacy training regarding their privacy policies, procedures, business processes, and updates thereto. NSI sites should also provide ongoing training which focuses on safeguarding personal information. Such training would strengthen the ability of personnel to prevent breaches involving personal information and should underscore the obligations of personnel to report privacy policy violations and breaches involving personal

[15] This requirement should apply to all personnel, including employees, contractors, and other support personnel. Some EE participating sites also provided training to personnel from other state and local partner agencies.

information. Training should be structured to ensure that personnel are informed of their individual, job-related responsibilities for protecting privacy, civil rights, and civil liberties and the consequences for violation of those responsibilities. Finally, to address some confusion regarding documentation of SARs (and subsequently ISE-SARs), personnel at source agencies and NSI sites should receive training in making "reasonably indicative" determinations.

RECOMMENDATION 8: Federal sponsoring agencies should work to ensure that technical assistance, guidance, and support focusing on privacy policy adoption, implementation, and training remain available and are expanded as needed to serve all NSI sites.

The sites confirmed that the technical assistance provided during the ISE-SAR EE facilitated each site's development and implementation of the privacy protection framework. Federal partners should ensure that technical assistance and training teams are available to NSI sites to ensure that adequate resources and policy guidance are available to resolve NSI issues.

RECOMMENDATION 9: When ISE Shared Spaces become better populated with new ISE-SARs, Federal partners should devise and conduct a more robust test of the value of the Summary Format.

During the EE, two data formats were developed for packaging ISE-SARs, namely, the Summary format and the Detailed format. The Summary format excludes Privacy Field information containing personally identifiable information (PII), whereas the Detailed format includes such information.[16] The Federal partners and the EE participating sites were not able to fully assess the utility of the Summary format due to a lack of sufficient data. There may, however, be value in making data in the Summary Format available to non-law enforcement public safety agencies, entities involved in critical infrastructure protection, terrorism researchers, subject matter experts, and first responders for use in identifying patterns and trends, on condition that appropriate privacy, civil rights, and civil liberties safeguards are in place.

RECOMMENDATION 10: Federal, State, local, and Tribal agencies should ensure that the experiences gained during the ISE-SAR EE and the fuller NSI implementation are considered as other ISE capabilities are developed.

Although the privacy, civil rights, and civil liberties concerns addressed in this Analysis are discussed in the context of the NSI, these concerns are not unique to SAR and ISE-SAR information. SARs are but one source of terrorism-related information, and the policies, procedures, and processes developed to handle SARs may also directly apply to other types of

[16] For further information regarding the EE participating sites' use of these formats, *see Final Report: ISE-SAR EE*, at pages 11 and 43.

ISE information. This would enable the government to achieve efficiencies and to better integrate operations that use all sources of information to carry out agency missions.

IV. Policies and Processes Supporting the NSI Privacy Framework

A. Recommendations of the *Initial Privacy and Civil Liberties Analysis*

The *Initial Privacy and Civil Liberties Analysis* included a number of recommendations to ISE-SAR EE participating sites designed to ensure the protection of privacy, civil rights, and civil liberties in the SAR EE. The recommendations urged the ISE-SAR EE participants to:

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.

These recommendations were integrated into the EE participating sites' privacy policies, procedures, and business processes as the ISE-SAR EE evolved and now serve as the foundation for the NSI Privacy Framework.

B. Strengthening the NSI Privacy Framework through Collaboration with Privacy, Civil Rights, and Civil Liberties Advocacy Groups

The Program Manager for the Information Sharing Environment (PM-ISE) and its Federal partners ensured transparency of and strengthened privacy, civil rights, and civil liberties protective measures for the NSI through consultation and collaboration with privacy, civil

rights, and civil liberties advocacy groups.[17] Advocacy groups served an essential role in shaping the privacy protection framework for ISE-SAR information sharing activities by assisting with the development and review of products (e.g., templates and training), and by participating in several meetings with the ISE-SAR EE implementation team to address EE implementation efforts.

These meetings confirmed that the implementation of privacy protections would require a multi-faceted and iterative approach. The PM-ISE and its Federal partners looked to the experiences of the sites during the EE for validation of the recommendations from the *Initial Privacy and Civil Liberties Analysis* and verification that the recommendations had application to the broader National SAR Initiative. The experiences of the EE participating sites confirmed the value of the NSI Privacy Framework as an appropriate minimum standard for protection in view of the fact that hundreds of qualifying ISE-SARs were successfully posted to the Shared Space and that there were no incidents of inadvertent sharing of such data.

NSI partners agree that the following elements are the minimum essential measures for the NSI Privacy Framework and are the key to meaningful privacy and civil rights/civil liberties protections:

1. Each NSI participating agency must conduct the NSI process pursuant to its statutory authorities and its privacy, civil rights, and civil liberties policies and procedures that are consistent with the ISE Privacy Guidelines;
2. Each NSI participating agency must submit privacy, civil rights, and civil liberties policies and procedures for review to ensure consistency with the ISE Privacy Guidelines prior to posting or accessing personal information (i.e., Privacy Fields) in the ISE Shared Space;
3. Implementation must include training of front-line, investigative, analytic, and supervisory personnel regarding their respective site's privacy policy, as well as behaviors and indicators of terrorism-related criminal activity;
4. Each NSI participating agency must institute a formal and multi-layered vetting process in which each SAR is reviewed by a front-line supervisor and by an experienced investigator or analyst specifically trained in counterterrorism issues before it can be designated as an ISE-SAR; and
5. Sites should engage in outreach and collaboration at a local level with privacy, civil rights, and civil liberties advocacy groups.

Adherence to and implementation of all elements of the NSI Privacy Framework are essential preconditions to sharing personal information contained in Privacy Fields. Compliance with this approach will not only strengthen the protection of privacy, civil rights, and civil liberties

[17] See Appendix C for a listing of the advocacy groups which participated in the collaborative process.

throughout the NSI process, but also improve the quality of the information on which analytic and investigative judgments are based.

C. The Revised ISE-SAR Functional Standard

The *National Strategy for Information Sharing*[18] identified "suspicious activity reporting" as one of the key information exchanges to be effected between and among Federal and SLT governments. In furtherance of this strategy, the PM-ISE led the development of a standardized process known as the ISE-SAR Functional Standard[19] and an associated data model. This standard enables government analysts and officers with law enforcement, homeland security, and counterterrorism responsibilities to discover and identify potential terrorist activities and trends.

The ISE-SAR Functional Standard supports the identification, documentation, and sharing of ISE-SAR information to the maximum extent possible, and in a manner that is consistent with privacy, civil rights, and civil liberties protections. Following extensive collaboration with privacy, civil rights, and civil liberties advocates, the PM-ISE implemented key revisions to the ISE-SAR Functional Standard in May 2009. The revisions refined the SAR information collection and SAR/ISE-SAR determination process in order to ensure that ISE-SARs are "reasonably indicative of criminal activity associated with terrorism." Simply put, the "reasonably indicative" language applies to the identification of SAR information and, when coupled with the two-step review and vetting process at the fusion center, defines the permissible scope of what information may be included in the shared space environment.[20]

1. *The Process for Identifying, Documenting, and Sharing SAR Information and the Protection of Privacy, Civil Rights, and Civil Liberties of Americans*

The revisions to the Functional Standard enable NSI sites to better detect and prevent terrorism-related crime with increased safeguards for protecting privacy, civil rights, and civil liberties. The revised Functional Standard delineates the process for identifying, documenting, and sharing ISE-SAR information by identifying the types of behavior that may be terrorism-related and the circumstances under which such information may be retained and shared.[21]

---

[18] *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing* (October 2007).

[19] See Version 1.5 of the ISE-SAR Functional Standard.

[20] It does not set a standard for permissible police investigations -- investigations and detentions continue to be governed by applicable law and source agency policy.

[21] The EE partners worked closely with privacy and civil liberties advocates to address and mitigate privacy and civil liberties concerns raised by the original Functional Standard (Version 1.0). One area of concern focused on the requirement that SARs and

The revision of the Functional Standard establishes that "reasonably indicative" determinations apply to both the collection of SAR information and the identification of an ISE-SAR to be shared with law enforcement, homeland security, and counterterrorism agencies. To be considered an ISE-SAR, the terrorism-related activity must conform to one or more of the criteria identified in Part B of the ISE-SAR Functional Standard.[22]

The use of the "reasonably indicative" determination process allows supervisors at source agencies and trained analysts and investigators at fusion centers and other agencies to have a uniform process that will result in better quality SARs and the posting of more reliable ISE-SARs to the ISE Shared Spaces, while at the same time enhancing privacy, civil rights, and civil liberties protections. Furthermore, this revision improves mission effectiveness and enables NSI participating agency personnel to identify and address, in a more efficient manner, potential criminal and terrorism threats by using more narrowly targeted language. Finally, better quality SARS should result in a sufficiently high quality of information enabling agencies and analysts to "connect the dots" while not producing so much information as to overwhelm agency analytical capacity.

In addition, the "reasonably indicative" determination is an essential privacy, civil rights, and civil liberties protection because it emphasizes a behavior-focused approach to identifying

---

ISE-SARs be based on "[o]fficial documentation of observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention." SARs and ISE-SARs are distinguishable in that ISE-SARs would also be coupled with a determination that the SAR has a "potential terrorism nexus." The advocates' concern was that language in Version 1.0 ("may be indicative") was too loose, allowing "mere suspicion" to be the basis for a SAR or an ISE-SAR to be collected and shared by a law enforcement or counter-terrorism agency. One response to this concern was to revise the language; under Version 1.5, the language "reasonably indicative of pre-operational planning related to terrorism or other criminal activity" applies to the collection of SAR information and the identification of an ISE-SAR based on the two-step review process to determine if it has a potential terrorism nexus.

Other changes reflected in Version 1.5 of the Functional Standard include: (1) Clarifying that the same constitutional standards that apply when conducting ordinary criminal investigations also apply to law enforcement and homeland security officers conducting SAR inquiries; (2) Refining the ISE-SAR Criteria Guidance to distinguish between those activities that are "Defined Criminal Activity" and those that are "Potentially Criminal or Non-Criminal Activity," requiring additional fact information during investigation; and (3) Clarifying those activities which are generally protected by the First Amendment that should not be reported in a SAR or ISE-SAR, absent facts and circumstances that can be clearly articulated and that support the source agency's suspicion that the behavior observed is reasonably indicative of criminal activity associated with terrorism.

[22] Before an agency can move SARs from the agency systems to the ISE, two forms of vetting must occur. Supervisors who initially receive a SAR from law enforcement officers, public safety agencies, private sector partners, or citizens must initially review the SAR to determine whether it has a nexus to terrorism and whether it includes the behaviors identified in the ISE-SAR Functional Standard. Trained analysts must then analyze the SAR against the behaviors identified in Part B of the ISE-SAR Functional Standard. Throughout the vetting process, privacy, civil rights, and civil liberties are vigilantly and actively protected through the training that analysts receive and through the system attributes that are a part of the NSI.

suspicious activity and mitigates the risk of profiling based upon race, ethnicity, national origin, or religious affiliation or activity.[23]

2. *The Standardized, Multi-Level Vetting Process*

The implementation of the revised ISE-SAR Functional Standard (Version 1.5) constitutes an essential safeguard supporting the NSI Privacy Framework. This standard requires the use of a multi-level business process to identify information with a potential nexus to terrorism out of the thousands of suspicious activities documented by source agencies each day. Following information gathering by law enforcement officers who have been trained to recognize terrorism-related behaviors and a preliminary review by a local agency, a trained analyst or law enforcement officer at a fusion center or Federal agency would determine whether the suspicious activity is indicative of criminal behavior or activity associated with terrorism.[24] The analyst or officer would then determine whether the facts and circumstances, taken as a whole, support a determination that "… the information has a potential nexus to terrorism."[25] If this determination is made, the SAR will be documented and made available as an ISE-SAR to all appropriate ISE participants in the agency's Shared Space.[26]

The enhancements to the ISE-SAR Functional Standard (Version 1.5) protect privacy, civil rights, and civil liberties by ensuring that information is submitted by trained staff; is gathered for a valid law enforcement or counterterrorism purpose; is subject to front-line supervisory review; and undergoes a formal two-step vetting process by an experienced investigator or analyst specifically trained in counterterrorism issues before being designated as an ISE-SAR.

---

[23] The revised Functional Standard expressly states that factors such as race, ethnicity, national origin, or religious affiliation or activity should not be considered as factors that create suspicion (except if used as part of a specific suspect description).

[24] The criteria for making this determination are set forth in Part B of the revised ISE-SAR Functional Standard (Version 1.5).

[25] An additional safeguard in the revised Functional Standard is the separation of potential terrorism-related behaviors into two categories: (1) those observed behaviors that are inherently criminal; and (2) those that involve the exercise of a constitutionally protected activity, but which may be criminal in nature. The revised Functional Standard provides that when the constitutionally protected behaviors are involved, there must be articulable facts and circumstances that support the officer or agency's suspicion that the behavior is not innocent, but rather reasonably indicative of criminal activity associated with terrorism.

[26] It is envisioned that agencies will share potential ISE-SAR information with State or major urban area fusion centers 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 it meets criteria as defined in Part B of the revised ISE-SAR Functional Standard (Version 1.5), the fusion center will designate the SAR as an "ISE-SAR" and make it available to other ISE participants through the fusion center's ISE Shared Space. Documenting, analyzing, and sharing of ISE-SAR information between and among State, local, and tribal organizations, State or major urban area fusion centers, JTTFs, and other Federal field components is designed to provide early indications to all NSI participating agencies of behaviors and indicators of criminal activity associated with terrorism.

D. Standardized Approach to Privacy, Civil Rights, and Civil Liberties Privacy Policies

A critical first step for each NSI site in implementing the NSI Privacy Framework is the development of a written privacy policy as a precondition to sharing or receiving any personal information contained in Privacy Fields. The site's privacy policy must be "at least as comprehensive" as the ISE Privacy Guidelines and the Baseline Capabilities in order to satisfy the requirements of: purpose specification; notice mechanisms; data quality; data security; accountability, enforcement, and audit; and redress.

EE participating sites were given three options for developing privacy policies that would qualify them to share and receive personal information contained in Privacy Fields. The options included the following:

1. Completing a comprehensive privacy policy based on DOJ Global Justice's *Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Template;*[27]
2. Formulating an ISE-SAR specific policy based upon the *ISE-SAR Evaluation Environment Privacy, Civil Rights, and Civil Liberties Protection Policy Template;*[28] or
3. Refining its existing privacy policy to ensure that it addressed all the ISE Privacy Guidelines requirements for enhanced protection of terrorism-related information.

Each participating site developed a draft privacy policy and provided it to the Privacy Policy Review Team for assessment and feedback. Once the Privacy Policy Review Team determined that the draft policy was "at least as comprehensive" as the ISE Privacy Guidelines, the team recommended the completed policy for approval to the PGC Co-Chairs and the PM-ISE. Upon approval, DOJ's Bureau of Justice Assistance (BJA) was formally notified that the EE participant was authorized to "go live" in sharing and accessing Privacy Field information in the ISE Shared Spaces.

E. Federal Privacy Technical Assistance and Training

Federal partners provided technical assistance, subject matter expertise, and training to ISE-SAR EE participants. Technical assistance included making privacy, civil rights, and civil liberties subject matter experts available to assist in developing and strengthening participant site privacy policies. The provision of technical assistance enabled Federal partners to ensure a standardized approach to privacy policy development at EE participating sites and to provide guidance regarding privacy and civil liberties issues with widespread impact beyond the state and local level.

[27] The Fusion Center Privacy Policy Template was updated in April 2010 to include language for SAR privacy provisions.

[28] This template was developed by Federal partners in collaboration with privacy and civil liberties advocacy groups. The PGC's Legal Issues Working Group finalized and approved the template for distribution to the EE participating sites in January 2009.

In addition to assisting with privacy policy development, DHS and DOJ/BJA, through their joint Privacy Technical Assistance Program, developed and provided training on privacy, civil rights, and civil liberties issues to personnel at ISE-SAR EE participant sites. Federal partners also provided role-based ISE-SAR training modules which included privacy, civil rights, and civil liberties components targeted to executives, senior leadership, front-line officers, and analysts.

EE participating sites indicated that privacy technical assistance and training were valuable in maximizing participation in the ISE-SAR EE. They also confirmed that without the provision of assistance, the ISE-SAR EE would not have resulted in meaningful implementation progress.

V. Success Stories and Best Practices from EE Sites

During the follow-up discussions with each EE participating site, several success stories and best practices emerged demonstrating the success of efforts to protect privacy, civil rights, and civil liberties.

A. Success Stories

- The commander of the Florida Fusion Center (FFC) received a telephone call from an individual concerning the FCC's ISE-SAR privacy, civil rights, and civil liberties policy. The FFC commander walked the individual through the privacy policy and protections and answered each of his questions. Upon completion, the caller identified himself as a Certification Assessor from the Commission on Accreditation for Law Enforcement Agencies and congratulated the FFC commander on the thoroughness of her response to his questions.

- Through its formal community outreach campaign, iWatch, the Los Angeles Police Department (LAPD) has informed, trained, and educated its community on SARs including privacy and civil liberties protections at outreach events throughout the Los Angeles metropolitan region. Community training on SAR privacy and civil liberties emphasizes suspicious behaviors over individual characteristics. LAPD considers its iWatch campaign to be the "community part of its SARs process."
- The Florida Department of Health, a state government agency participating in the FFC's terrorism liaison officer program, had previously limited its reporting of SAR information due to its privacy concerns with releasing personal health information. Through the SAR training, the Florida Department of Health understood that its submission to the FFC of SAR information based upon suspicious behaviors was permissible. One of those reports resulted in an open investigation on a person of interest related to terrorism.

B. Best Practices

- The Arizona Counter Terrorism Information Center (ACTIC) actively monitors privacy, civil rights, and civil liberties issues raised by other fusion centers around the country through fusion center regional conferences and other outreach events and uses lessons learned as a guide for adjusting its own policies and procedure.
- The FFC sought an extensive policy review from a variety of external stakeholders, including review by the Florida's state advisory board on privacy and civil liberties, citizen advisory groups, and the legal counsels of all of the site's partner agencies in the process of developing its privacy, civil rights, and civil liberties protection policy.

VI. Conclusion

Since the inception of the NSI, Federal and SLT partners have remained steadfast in their commitment to protecting privacy, civil rights, and civil liberties. In moving from the ISE-SAR EE demonstration phase to the national implementation of the NSI, the NSI Privacy Framework will remain a critical touchstone and be regularly reviewed and updated as necessary. Federal and SLT partners must continue to work together to ensure that robust privacy, civil rights, and civil liberties policies and procedures are adopted, properly implemented, and continuously assessed. The NSI sites must continue efforts to identify opportunities for strengthening and improving privacy, civil rights, and civil liberties protections. The NSI Program Manager's Office should lead efforts to ensure continued oversight of framework implementation, with guidance from the ISE PGC and the President's Privacy and Civil Liberties Oversight Board. Maintaining an unrelenting focus on the protection of privacy, civil rights, and civil liberties will assure the public that the legal rights of all Americans are fully protected and will continue to be a national priority.

Appendix A – ISE-SAR EE Privacy and Civil Liberties Assessment Questionnaire

[AGENCY NAME]
ISE-SAR Evaluation Environment
Final Project Privacy & Civil Liberties Protections Assessment

The purpose of the ISE-SAR Evaluation Environment (EE) was to develop a learning environment in which to determine whether a national standard (the SAR Functional Standard) for reporting and evaluating suspicious activity could facilitate the identification of patterns of criminal activity with a nexus to terrorism. To enable implementation of the ISE-SAR EE, it was essential that policies be implemented for ensuring that privacy, civil rights, and civil liberties are protected in the ISE-SAR identification process and in the sharing of ISE-SAR information. These privacy policies also support transparency to the public regarding the sharing of information about terrorism-related suspicious activity between fusion centers and with other law enforcement and homeland security agencies. This assessment seeks to capture the experience of agencies participating in the ISE-SAR EE regarding development and implementation of privacy and civil liberties protections for identifying and sharing ISE SAR information and the integration of these protections into agency business processes and activities. This Privacy Assessment is a requirement of the *Initial Privacy and Civil Liberties Analysis* of the Suspicious Activity Reporting Functional Standard and Evaluation Environment (September 2008 - Version 1).

Site Visit information

Date:	[Date and Time of Call, Eastern Standard Time]
Method of Visit:	Conference Call
Personnel:	[Names and Titles of Site Personnel]

DEVELOPING AND IMPLEMENTING AGENCY PRIVACY POLICIES

1) During the ISE-SAR EE, did your agency develop and implement either a comprehensive information and intelligence privacy policy using the Fusion Center Privacy Policy Development Template or an ISE-SAR specific Privacy Policy?
    a) If so, has the Privacy Policy been promulgated agency wide?
2) Has your agency communicated its Privacy Policy to the public, community organizations, and other groups as appropriate?
3) Have you conducted a Privacy Impact Assessment for your ISE-SAR activity?
4) Did your agency utilize legal/privacy advisors when developing the agency's privacy policy?
5) Does the jurisdiction where your agency is located (regional, state, urban) have specific privacy laws or regulations that you incorporated into your privacy policy?
    a) If yes, please describe these laws or regulations.
    b) Did any of these laws or regulations impact the development of your agency's privacy and civil liberties policies?
6) Does your agency have a plan for regular review of your privacy policy, i.e. biannual review?

IMPLEMENTING AGENCY PRIVACY POLICIES INTO ISE-SAR BUSINESS PROCESSES

1) In what ways, if at all, did privacy and civil liberties considerations affect your agency's ability to integrate ISE-SAR activities pre-existing business processes? Describe.
2) How does your agency ensure that an ISE-SAR meets the criteria established by the ISE-SAR Functional Standard?
3) Does your agency have a mechanism for timely informing the original submitter of SAR information that the SAR has been determined to be an ISE-SAR?
4) If an ISE-SAR is determined to be erroneous in content or designation after being posted to the ISE Shared Space, what processes have you implemented to remedy the situation (correction, notice, etc.)?
5) What is your procedure for handling SARs that do not meet the criteria of an ISE-SAR? Do you retain and use those SARS and, if so, how do you ensure the privacy and civil liberties protection of those SARs?
6) How does your agency ensure that appropriate quality controls are in place for SARs and ISE-SARs (example of controls may include use of labels and markings to indicate questionable accuracy of SAR or ISE-SAR)?
7) Are periodic audits of SAR and ISE-SAR data conducted by command-level staff or agency designees?
    a) If yes, describe your audit process.

ISE-SAR Privacy and Civil Liberties Protections

1) What procedures, both internally and with SAR source agencies, has your agency established to ensure against "profiling" on the basis of race, ethnicity, national origin, religion, or other suspect classifications?
2) What procedures, both internally and with SAR source agencies, has your agency established to ensure that individuals' other Constitutional rights are not violated in the gathering of SAR information?
3) Have you received any privacy or civil liberties complaints arising from your SAR or ISE-SAR activities?
    a) How does your agency handle privacy or civil liberties complaints?
    b) Do you track complaints? Do you track resolution of complaints?
    c) Are complaints shared with any external organizations (for example, Attorney General's office, Inspector General, Internal Affairs, etc.)?
4) Has your agency experienced any inadvertent sharing of ISE-SARs (such as a technical or personnel glitch that inadvertently caused a release)?
    a) Did the inadvertent sharing come to light as sources?
    b) What procedures does your agency follow to correct an incident where an ISE-SAR is inadvertently shared? Internal fixes? External notification? Other?
    c) Are cases of inadvertent sharing reported external to your agency? If so, to whom (for example, Attorney General's office, Inspector General, Internal Affairs, etc.)?

Training Agency Personnel on Privacy and Civil Liberties Protections as part of the SAR Process

1) Have you trained personnel with ISE-SAR responsibilities on privacy and civil liberties protections applicable to the gathering, processing, analyzing, and sharing of SARs and ISE-SARs?
    a) Provide examples of training provided to your staff to support the ISE-SAR EE.
2) Has your agency identified privacy and civil liberties issues for which additional training is needed?
    a) If so, what types of additional training would your agency need?

CHALLENGES AND LESSONS LEARNED DURING ISE-SAR EE

1) What is the most significant change you have made to business processes as a result of the privacy and civil liberties considerations implicated by the ISE-SAR EE?
   a) Describe other privacy and civil liberties considerations and resulting process changes.
2) Were privacy and civil liberties issues identified in any "lessons learned?"
   a) If yes, please describe the lessons learned and the relationship to privacy and civil liberties concerns or protections.
   b) Have you modified your privacy policy or business processes as a result of the lessons learned?

Appendix B – Observations of EE Participating Sites During the ISE-SAR EE

A. Overview of Results

All EE participating sites adopted the recommendations in the *Initial Privacy and Civil Liberties Analysis* and implemented the NSI Privacy Framework. This Appendix will address the methodology used during the EE to evaluate implementation policies and procedures and will highlight common themes that emerged during the assessment. This Appendix will also show that each EE participating site had unique experiences in implementing this framework.

B. Methodology

The PM-ISE and DOJ/BJA conducted follow-up assessments of EE implementation through conference calls with each EE participating site in the Fall of 2009. For the purpose of assessing privacy, civil rights, and civil liberties protections, a survey questionnaire[29] was developed by the PM-ISE, with input from the PGC Legal Issues Working Group. During conference calls with the EE participating sites, PM-ISE staff used the questionnaire to frame the discussion and then documented the responses from each site in a draft privacy, civil rights, and civil liberties assessment. The draft assessments were electronically submitted to each participating site for formal review and vetting.

Each site was requested to formally review and vet the draft response and to return it to the PGC Executive Director. Four of the twelve sites returned their assessment questionnaires using this process. Given the limited number of corrections to the draft responses made by these four sites, the PM-ISE determined that the draft privacy and civil liberties assessments would suffice for the purposes of analyzing the protection of privacy, civil rights, and civil liberties during the EE.

C. Results of Follow-up Assessments

The experiences of the EE participating sites in implementing the SAR process and the NSI Privacy Framework are summarized as follows:

1. Developing Privacy Policies Consistent with ISE Privacy Guidelines

With respect to policy alignment, a number of sites had privacy policies in place prior to participating in the ISE-SAR EE consistent with their State and local requirements. However, all of the EE participating sites noted that they devoted additional effort and resources to ensuring

[29] See *ISE-SAR EE Privacy and Civil Liberties Assessment Survey Questionnaire* contained in Appendix A of this Analysis.

that their existing privacy policies and procedures were fully compliant with the privacy, civil rights, and civil liberties requirements for ISE-SAR participation.

The development and implementation of the elements of the privacy policy framework generally took longer than anticipated at most EE participating sites. Most sites reported an average length of about six months to develop, review, approve, and implement the policy for the following reasons:

1) A number of sites experienced delays in coordinating the review of draft privacy policies with internal and external stakeholders; and
2) Coordinating the review and approval of policies between multiple State and local parties, including legal counsels, required several iterations of draft policy documents and extended the length of time before which the EE participating site was authorized to "go live" in sharing and receiving Privacy Field information.

These delays resulted in an inability to participate in information sharing activities for several sites. A few sites found that assigning a staff member as the single point of contact for development and coordination was a key factor in getting privacy policies completed faster.

The designation of privacy officials proved to be another area for improvement. There has been nominal progress in putting privacy officers in place at EE participating sites. Many sites noted that they were in the process of hiring a privacy officer or privacy and civil liberties subject matter expert.

To address this issue, most sites relied upon internal or departmental legal staff to determine the applicable SLT legal and regulatory requirements to be incorporated into ISE-SAR privacy policies. Some sites relied upon the expertise of records managers and compliance officers in the development and review of ISE-SAR policies. One site sought an extensive policy review from a variety of external stakeholders, including review by the state's advisory board on privacy and civil liberties, citizen advisory groups, and site partner agency legal counsels. Another site noted that while it did not involve the state's homeland security privacy officer in the development of its privacy policy, the site does coordinate with this privacy officer in planning other operational initiatives.

Some states have both a state fusion center and one or more Urban Area Security Initiative (UASI) fusion center sites in the state. None of the UASI sites coordinated with its designated state fusion center on the development of its privacy policy.

2. Privacy Policy Adoption and Community Outreach

Implementation strategies for adopting privacy, civil rights, and civil liberties policies and processes varied across the twelve EE participating sites. Every site with a privacy policy in place during the EE required personnel[30] involved in the SAR process to review and certify

[30] This included personnel assigned to the center from other organizations.

acceptance of the site's privacy, civil rights, and civil liberties policy. A number of sites plan to or are in the process of developing in-house training modules.

The majority of outreach efforts to the public and to privacy, civil rights, and civil liberties advocacy groups occurred after the site completed development of its privacy policy. Sites pursued varying approaches to informing the public. A number of sites posted privacy policies to a public websites, either a fusion center-specific or Departmental website. Other sites chose to include information on the ISE-SAR process in agency command and staff presentations. Finally, one site organized community training sessions on the SAR process, to include training on privacy, civil rights, and civil liberties, as part of its larger community outreach efforts.

A few sites focused on outreach to local advocacy groups as part of their commitment to transparency throughout the development and implementation of the SAR process. All of these sites confirmed the critical role of transparency in addressing concerns of citizens and watchdog groups. One site walked staff from the local ACLU through the site's Special Orders and Process steps; now, the ACLU is a partner that regularly compliments this site's efforts to protect privacy, civil rights, and civil liberties. A few sites also discussed holding open house events and providing facility tours. Another means of outreach involved the "Building Communities of Trust" initiative, where EE participating sites invited local privacy, civil rights, and civil liberties advocacy groups to participate in planning meetings and subsequent outreach events.

With respect to the use of Privacy Impact Assessments (PIAs) as a tool for ensuring transparency, very few sites were familiar with the concept of PIA. Only one of the EE participating sites has conducted a PIA. Two sites indicated that command staff was considering conducting a PIA sometime in the future. A brief description of a PIA was provided to the remaining sites, after which several sites noted that it sounded useful and recommended that guidance and templates for use of PIAs be made available to NSI sites.

3. Integrating Privacy, Civil Rights, and Civil Liberties Protections into Business Processes

The *Initial Privacy and Civil Liberties Analysis* recommended that sites "integrate the management of [SAR] processes with existing processes and systems . . . thereby leveraging existing policies and protocols that protect privacy, civil rights, and civil liberties." All EE participating sites confirmed their full compliance with the SAR Functional Standard. However, some sites found that they needed to update their existing business processes and procedures to comply with requirements of their privacy policies. For example, one site specifically described how it had changed existing business processes to comply with privacy policy requirements for redress, labeling, data quality, retention, and purging.

As for the sites' SAR submission status, most sites described business processes that included a requirement to provide feedback status to SAR originators. Those still engaged in developing an implementation strategy reported plans to include a process for providing feedback to source agencies (the agency documenting/submitting the SAR) that the SAR has been

designated as an ISE-SAR. Finally, in cases where EE participating sites referred ISE-SARs to the local FBI Joint Terrorism Task Force (JTTF), most of the sites have policies for notifying the source agency of the referral to the JTTF.

With respect to monitoring the status of ISE-SARs submitted to JTTFs, a number of sites reported terminating tracking/final outcomes upon submission of the ISE-SAR to the JTTF.

The sites were also assessed in terms of whether and to what extent they provided feedback on erroneous SAR information. Most sites indicating that feedback would be provided to the original submitter when SARs contained erroneous information. Several sites also indicated that SARs would be updated to correct the erroneous information. Few sites reported using labels to indicate when a SAR contained erroneous information. The majority of participants, however, confirmed that quality controls built into the SAR vetting process, especially multiple levels of analysis and review, would minimize the possibility of posting an ISE-SAR with erroneous information to the ISE Shared Space. Additionally, several sites emphasized the need to ensure that all NSI participating sites strictly adhere to the vetting and feedback processes to assure information quality and integrity.

With respect to inadvertent sharing, the *Initial Privacy and Civil Liberties Analysis* acknowledged the concerns of some advocates that the privacy, civil rights, and civil liberties of individuals could be placed at risk in the event that an ISE-SAR containing personal information was inadvertently shared. However, it is significant to note that none of the participants reported any instances where ISE-SARs were inadvertently shared. Moreover, all sites had established departmental policies and processes in place to address an inappropriate use of information or data breaches, should such a breach occur.

As for quality control and auditing, the majority of EE participating sites reported that they are subject to regular audits by Internal Affairs or Inspectors General offices. Quality control and audit functions were also performed through daily reviews of new SARs and ISE-SARs by senior level and/or experienced staff. This process served to address quality control and auditing needs.

4. Profiling Protections and Constitutional Rights

All EE participating sites reported strong emphasis within their departments and agencies on upholding constitutional rights of individuals and avoidance of any actions that could be interpreted as profiling. All sites cited training programs for site personnel and partners that focused on the importance of behavior-based SAR collection, i.e. gathering information associated with suspicious behavior rather than suspicious persons.

The supporting departments or agencies of a number of EE participating sites have previous experience with mitigating the risk of "profiling" based upon race, ethnicity, national origin, religion, etc. At least two sites noted that their departments were subject to tracking and auditing requirements for "profiling" activities at vehicle traffic stops as a result of earlier lawsuits or Federal consent decrees. Several sites reported rejecting or avoiding the use of any SAR that included information which could create the appearance of profiling or could impact

an individual's civil rights or civil liberties, even if that information came from a partner agency or the site's supporting department or agency. Moreover, in cases where a SAR meets the criteria of an ISE-SAR, any formats containing race or ethnicity information that are not deemed critical to the ISE-SAR are not uploaded to the ISE Shared Space.

Many sites were subject to mandates for regular training of all personnel (e.g. sworn officers or State employees) on civil rights and civil liberties issues, including the First and Fourth Amendments. Additionally, many sites provide follow-up feedback and training to front-line officers or partner agencies if these sources submit SARs that contain information that indicates profiling based on factors such as race or ethnicity.

Finally, there were no reports or complaints of privacy, civil rights, or civil liberties violations at any participating sites. All sites reported the existence of a formal process within their supporting departments or agencies to review, investigate, and address such complaints.

5. Training and Documentation

Most sites indicated a reliance upon existing privacy, civil rights, and civil liberties training offerings from Federal partners. All sites reported that their site personnel have achieved Federal 28 CFR Part 23 training certification and participated in SAR training (chief executive, analyst, and front-line officer training). Some sites have sent personnel to attend training conducted by DOJ BJA and DHS at regional fusion center conferences and meetings. Some of the sites had sent personnel to attend civil rights and civil liberties training sessions conducted by the DHS Office of Civil Rights and Civil Liberties. A number of EE participating sites also reported supplementing this training through the use of local civil liberties training which also covered First and Fourth Amendment issues and state privacy, civil rights, and civil liberties laws.

As for the development of in-house and academy training, many sites reported ongoing efforts or plans to develop in-house training for site personnel and partners on privacy, civil rights, and civil liberties requirements for the ISE-SAR process and are working with police academies to develop a curriculum for new cadets and in-service [continuing officer] training. The majority of sites specified that training curricula would include a focus on training front-line officers to establish clear expectations of the information gathering requirements for SARs given that front line officers generate the largest number of incoming reports. A number of sites also reported that their police academies have already integrated information on the SAR process, including information on privacy policies, into current cadet training and in-service training offerings.

Several EE participating sites remarked upon the differences in perspective and understanding between law enforcement and non-law enforcement personnel with respect to the SAR process. All of these sites confirmed that training is critical to bridging these perspective differences and that training should be provided at regular opportunities.

Finally, the assessment covered the training of citizenry. Citizens are a source of reporting SAR information that is documented by law enforcement agencies and a few sites have devoted time and attention to the training of citizens as a way to improve the relevancy of incoming

information pertaining to suspicious behavior from the public. One site noted that information on the SAR process has been incorporated into the curriculum of the city's citizen academy. Another reported providing feedback directly to citizens who have called in to report tips, particularly when those reports don't contain information indicative of suspicious behavior. One site commander provided suspicious behavior training to an individual citizen who called to report that several men of Middle Eastern origin had moved into the house next to her property; the site noted that training of citizens to identify suspicious behaviors is part of the site's ongoing commitment to ensuring a focus on the recognition and reporting of suspicious behaviors and not on personal attributes, such as national origin, race, ethnicity, religion, or other personal attributions.

Appendix C – Organizations That Participated in Outreach Efforts

Privacy and Civil Liberties Advocates

American-Arab Anti-Discrimination Committee

American Civil Liberties Union of Southern California

American Civil Liberties Union - Washington Legislative Office

Bill of Rights Defense Committee

Center for Democracy and Technology

Electronic Information Privacy Center

Freedom and Justice Foundation

Islamic Shura Council of Southern California

Muslim Advocates

Muslim Public Affairs Council

Rights Working Group

State, Local, and Tribal Law Enforcement Agencies

Georgia Bureau of Investigation

Intelligence Fusion Center
Iowa Department of Public Safety

Los Angeles Police Department

Los Angeles City Attorney's Office
New Jersey State Police

Pennsylvania State Police

Washington State Fusion Center
Seattle Police Department

Law Enforcement Professional Organizations

American Probation and Parole Association

International Association of Chiefs of Police

National Fusion Center Association

Federal Agencies

Civil Liberties and Privacy Office
Office of the Director of National Intelligence

Privacy and Civil Liberties Office
Office of the Deputy Attorney General
U.S. Department of Justice

Office of the Chief Information Officer
U.S. Department of Justice

Bureau of Justice Assistance
Office of Justice Programs
U.S. Department of Justice

Privacy and Civil Liberties Unit
Office of the General Counsel
Federal Bureau of Investigation
U.S. Department of Justice

National Threat Center Section
Counterterrorism Division
Federal Bureau of Investigation
U.S. Department of Justice

Community Oriented Policing Services Office
U.S. Department of Justice

Chief Privacy Office
U.S. Department of Homeland Security

Office for Civil Rights and Civil Liberties
U.S. Department of Homeland Security

Information Sharing and Collaboration
U.S. Department of Homeland Security

State and Local Program Office
U.S. Department of Homeland Security

Office of Counterterrorism and Security Preparedness
Protection and National Preparedness Division
Federal Emergency Management Agency
U.S. Department of Homeland Security

Office of the Program Manager, Information Sharing Environment

Appendix D – Acronyms and Abbreviations

ACLU	American Civil Liberties Union
BJA	Bureau of Justice Assistance
CR/CL	Civil Rights/Civil Liberties
DHS	Department of Homeland Security
DoD	Department of Defense
DOJ	Department of Justice
EE	Evaluation Environment
FBI	Federal Bureau of Investigation
ISE	Information Sharing Environment
JTTF	Joint Terrorism Task Force
NSI	Nationwide Suspicious Activity Reporting Initiative
ODNI	Office of the Director of National Intelligence
PIA	Privacy Impact Assessment
PGC	Privacy Guidelines Committee
PM-ISE	Program Manager, Information Sharing Environment
SAR	Suspicious Activity Reporting
SLT	State, local, and tribal
UASI	Urban Area Security Initiative

Appendix E – Referenced Documents and Resources

This appendix provides a comprehensive listing of the documents referenced in this Analysis.

The Nationwide Suspicious Activity Reporting Initiative Program Management Office, http://nsi.ncirc.gov/

Baseline Capabilities for State and Major Urban Area Fusion Centers: A Supplement to the Fusion Center Guidelines (September 2008)
http://it.ojp.gov/documents/baselinecapabilitiesa.pdf

The Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment ("ISE Privacy Guidelines") (December 2006),
http://www.ise.gov/docs/privacy/PrivacyGuidelines20061204.pdf

Fusion Center Privacy Policy Development – Privacy, Civil Rights, and Civil Liberties Policy Template (April 2010),
http://it.ojp.gov/docdownloader.aspx?ddid=1269

The ISE-SAR Functional Standard, Version 1.5 (May 2009),
http://www.ise.gov/docs/ctiss/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf

National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing (October 2007),
http://www.ise.gov/docs/nsis/nsis_book.pdf

The Initial Privacy and Civil Liberties Analysis of the Information Sharing Environment - Suspicious Activity Reporting (ISE-SAR) Functional Standard and Evaluation Environment (September 2008),
http://www.ise.gov/docs/sar/ISE_SAR_Initial_Privacy_and_Civil_Liberties_Analysis.pdf

Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project, (October 2008), http://www.it.ojp.gov/documents/SAR_Report_October_2008.pdf

Final Report: Information Sharing Environment Suspicious Activity Reporting Evaluation Environment (January 2010), Department of Justice Bureau of Justice Assistance, http://nsi.ncirc.gov/documents/NSI_EE.pdf

The Nationwide Suspicious Activity Reporting Initiative Status Report (February 2010), Office of the Program Manager for the Information Sharing Environment, http://www.ise.gov/docs/sar/NSI_Status_Report_FINAL_2010-02-03.pdf

Office of the Director of National Intelligence
Attention: Program Manager, Information Sharing Environment
Washington, DC 20511

(202) 331-2490

For more information, go to:

http://www.ise.gov