Privacy Impact Assessment
for the

Department of Homeland Security Information Sharing Environment Suspicious Activity Reporting Initiative

November 17, 2010

Contact Point
Ronald Athmann
Office of Intelligence and Analysis
202-447-4232

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Department of Homeland Security (DHS or Department) Office and Intelligence and Analysis, primarily through the State and Local Program Office in coordination with the Office of Operations Coordination Planning, is leading the DHS effort to implement the Nationwide Suspicious Activity Reporting Initiative (NSI). The NSI is a key aspect of the federal Information Sharing Environment (ISE) that Congress created in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRPTA). The NSI is overseen by the Department of Justice (DOJ) and is designed to support the sharing of information through the ISE about suspicious activities which are defined as "official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity [related to terrorism]." The Office of Intelligence and Analysis and the Office of Operations and Coordination Planning have been jointly coordinating activities throughout DHS to develop a department-level interface with the NSI that will enable DHS to share Suspicious Activity Reporting (SAR) that meet the ISE-SAR Functional Standard Version 1.5 (hereinafter referred to as ISE-SAR)[1]. The ISE-SAR Functional Standard Version 1.5 defines an ISE-SAR as official documentation of observed behavior reasonably indicative of: pre-operational planning related to terrorism or other criminal activity associated with terrorism. DHS conducted this privacy impact assessment (PIA) because ISE-SAR may contain personally identifiable information (PII). This PIA describes the coordinated activities of the DHS ISE-SAR Initiative, including the process for DHS component level review, identification, and submission of ISE-SAR to the NSI Shared Space as well as the technology that DHS developed to support DHS' participation in the NSI.

Overview

Information Sharing Environment and the Nationwide Suspicious Activity Reporting Initiative

The federal ISE is designed to facilitate the sharing of terrorism information among all relevant entities through the combination of information sharing policies, procedures, and technologies.[2] A key aspect of implementing the ISE is the establishment and implementation of the NSI. The NSI is an outgrowth of a number of separate but related activities over the last several years that respond directly to the requirement to establish a "unified process for reporting, tracking, and accessing [SAR]," in a manner that rigorously protects the privacy, civil rights, and civil liberties of Americans, as called for in the National Strategy for Information Sharing. The long-term goal is that most federal, state, local, and tribal law enforcement organizations will participate in a standardized, integrated approach to gathering, documenting, processing, analyzing, and sharing information about suspicious activity that is potentially

[1] Throughout this PIA, the term "SAR" refers to suspicious activity reporting, which may include activities that do not have a nexus to terrorism, and the term "ISE-SAR" refers to a subset of SAR that meet the ISE-SAR Functional Standard.

[2] Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-485, 118 Stat. 3638, 3664 (2004), as amended, directs the ISE to improve the sharing of terrorism and homeland security information. The IRTPA definition of terrorism information encompasses all terrorism-related information "whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities," and was explicitly amended in 2007 to include weapons of mass destruction information. For brevity, these types of information are collectively referred to as "terrorism-related" information.

terrorism-related. In addition to government agencies, private sector organizations responsible for Critical Infrastructure/Key Resources and foreign partners are also potential sources for ISE-SAR.

The NSI is one of a number of government-wide efforts designed to implement guidelines first issued by the President on December 16, 2005, for establishing the ISE pursuant to section 1016 of IRTPA, as amended. The NSI establishes a nationwide capability to gather, document, process, analyze and share information about suspicious activities (hereinafter referred to as suspicious activity or activities) to enable rapid identification and mitigation of potential terrorist threats.

There is a long history of documenting suspicious activity, particularly in the law enforcement community; these reports are sometimes referred to as suspicious activity reports, tips and leads, or other similar terms. Federal, state, local and tribal agencies and the private sector currently collect and document suspicious activities in support of their responsibilities which may include investigating and preventing potential crimes, protecting citizens, apprehending and prosecuting criminals, and/or protecting critical infrastructure. Since some of these documented activities may bear a nexus to terrorism, the Program Manager for the Information Sharing Environment (PM-ISE)[3] has developed a standardized process for identifying, documenting, and sharing ISE-SAR, which meet the definition and criteria set forth in the ISE Functional Standard Version 1.5 (May 2009), to the maximum extent possible consistent with the protection of individual privacy, civil rights, and civil liberties.[4] The ISE-SAR Functional Standard Version 1.5 defines ISE-SAR as official documentation of observed behavior reasonably indicative of: pre-operational planning related to terrorism, or other criminal activity associated with terrorism. Appendix B contains the text of the ISE-SAR Functional Standard, which includes both the definition of an ISE-SAR that NSI participants must use when including an ISE-SAR in the NSI Shared Space and a full listing of the data elements including those containing PII, which are identified as "Privacy Fields." ISE-SAR data varies and may or may not contain PII. For example, the ISE-SAR Summary Format, used by DHS to enter ISE-SAR obtained from an external agency, does not contain PII.

NSI Shared Space and the DHS ISE-SAR Server

Section 1016 of IRTPA, as well as the NSI, direct that, to the greatest extent possible, the ISE should be a decentralized, distributed, and coordinated environment that connects existing systems to share terrorism information. Each of the NSI participants will own or administer proprietary servers that maintain their validated ISE-SAR and against which other NSI participants will be able to conduct federated searches. This set of servers, although maintained by different participants, is referred to as the NSI Shared Space. Accordingly, DHS, like each NSI participant, has developed its own server to maintain its ISE-SAR (hereinafter referred to as the DHS ISE-SAR Server), which will enable authorized

[3] IRTPA established the position of Program Manager to "plan for and oversee the implementation of, and manage the ISE," and to be "responsible for information sharing across the Federal Government." Consistent with the direction and policies issued by the President, the Director of National Intelligence, and the Director of the Office of Management and Budget, the PM-ISE issues government-wide procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and proper operation of the ISE. To better assist in ISE implementation activities, the Office of the PM-ISE has staff with experience in counterterrorism, homeland security, information sharing, technology, and policy at all levels of government. See http://ise.gov/Pages/ProgramManager.aspx.

[4] http://nsi.ncirc.gov/documents/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf

DHS components and other NSI participants to search DHS ISE-SAR. In addition, authorized DHS components will have access to a federated search capability, available through the NSI, for searching all ISE-SAR available in the NSI Shared Space.

A prerequisite for participation in the NSI is that each NSI participating agency must adopt a written privacy, civil rights, and civil liberties policy that is at least as comprehensive as the protection standards promulgated by the PM-ISE in the Privacy Guidelines.[5] Draft policies are submitted to the PM-ISE for review and approval before participants are permitted to post or access PII (i.e., Privacy Fields) in the NSI Shared Space. DHS met this requirement with PM-ISE's review and approval of its Federal Information Sharing Environment Privacy and Civil Liberties Privacy Protection Policy, which was published in June 2009.[6]

Suspicious Activity Reporting Activities at DHS

Several operational components within DHS regularly observe or otherwise encounter suspicious activities while executing their authorized missions and performing operational duties. Components document those observations or encounters as a SAR. Across the Department, the operational setting or context for activities reported in SAR are as varied as the Department's mission responsibilities. Engagement with the NSI will alter neither those underlying mission functions nor upset the current methodologies employed by DHS components collecting and documenting information on suspicious activities. Rather, the NSI will facilitate the more effective sharing and discovery of ISE-SAR – both internally and among DHS and external NSI participants – by incorporating a standardized technological and functional approach for recording and storing ISE-SAR throughout DHS.

DHS is taking a phased approach to connecting authorized components to the DHS ISE-SAR Server. The publication of this PIA marks the availability of the DHS ISE-SAR Server for inclusion into the NSI Shared Space; however, not all eligible DHS components will be connected to the DHS ISE-SAR Server initially. Before components connect to the DHS ISE-SAR Server and access the NSI Shared Space, components must:

- identify IT systems that currently store SAR data as well as applicable privacy documentation;
- determine the method for entering ISE-SAR into the DHS ISE-SAR Server (e.g., direct connection or manual entry); and
- ensure that personnel have been trained on applying the ISE-SAR Functional Standard Version 1.5 prior to submitting ISE-SAR data or querying the NSI Shared Space. Components will make a list of the dates and names of personnel who have received training available to DHS Privacy Office.

Once these requirements have been met, the component will be authorized to connect to the DHS ISE-SAR Server and contribute ISE-SAR if appropriate, and/or query the NSI Shared Space. In some cases a component may only make use of the NSI Shared Space query capabilities. Components are responsible for ensuring that ISE-SAR submitted to the DHS ISE-SAR Server meet the ISE-SAR

[5] http://www.ise.gov/docs/PrivacyGuidelines20061204.pdf
[6] http://www.dhs.gov/xlibrary/assets/privacy/privacy_crcl_guidance_ise_2009-01.pdf.

Functional Standard. Appendix A lists the DHS components and their respective programs currently authorized to participate in the NSI as a contributor of ISE-SAR and/or user of NSI Shared Space query capabilities along with the following information:

- program name and description;
- description of planned use of NSI Shared Space query capabilities;
- applicable IT system(s) and associated privacy documentation;
- date(s) of analyst training; and
- method of connection to the DHS-ISE SAR Server.

As more DHS components and programs meet the conditions described above, they will be added to Appendix A. In addition, the DHS Privacy Office will conduct a privacy compliance review of the program's NSI participation within nine months of the program's inclusion as an authorized NSI recipient.[7]

Privacy Risks Presented by Participation in NSI

The major privacy risk identified through this assessment is that action will be taken by DHS or an NSI participant based on ISE-SAR containing erroneous, inaccurate, untimely, or incomplete information available in the NSI Shared Space. Given the nature of SAR, it is not always possible to obtain accurate, relevant, timely and complete information. Recognizing this, DHS issued a notice of proposed rulemaking to propose exemptions from the Privacy Act's accuracy, relevancy, timeliness and completeness requirements. To mitigate this risk, DHS users are trained how to properly input and interpret ISE-SAR using contextual data concerning the source of the information to help assess the quality and reliability of each ISE-SAR. DHS users of ISE-SAR are trained on the nature of SAR and as a requirement for participation in the NSI, must take NSI training on applying the ISE-SAR Functional Standard. The ISE-SAR Functional Standard Version 1.5 provides for DHS and other NSI contributors to identify a source reliability code, defined as the reliability of the source in the assessment of the reporting organization (i.e., "reliable," "unreliable," or "unknown"); a content validity code, defined as the validity of the content, in the assessment of the reporting organization (i.e., "confirmed," "doubtful," or "cannot be judged"); nature of source code, defined as the nature of the source (i.e., "anonymous tip," "confidential source," "trained interviewer," "written statement – victim, witness, other, private sector," or "other source," as well as a free form text field to describe the nature of the source if "other source" is selected). Mandatory NSI training means that DHS users understand how to interpret ISE-SAR appropriately and contribute ISE-SAR to the NSI that contain appropriate context. Furthermore, DHS users are obligated to delete or edit previously submitted ISE-SAR if they subsequently determine that the

[7] The DHS Privacy Office exercises its authority under Section 222 of the Homeland Security Act to assure that technologies sustain and do not erode privacy protections through the conduct of Privacy Compliance Reviews. Consistent with the Privacy Office's unique position as both and advisor and oversight body for the Department's privacy sensitive programs and systems, the privacy compliance review is designed as a constructive mechanism to improve a program's ability to comply with assurances made in existing privacy compliance documentation including Privacy Impact Assessments, System of Records Notices and/or formal agreements such as Memoranda of Understanding or Memoranda of Agreements.

data is now erroneous or newly discovered information related to the SAR has been discovered and appropriate editing is required. DHS' planned uses of the information in the NSI Shared Space are to draw linkages among ISE-SAR made available by NSI participants for the purposes of preventing, disrupting, or halting terrorism-related incidents and for analytical purposes that are consistent with the ISE-SAR Functional Standard Version 1.5 to identify possible trends and provide general analytical products that inform other components as well as state and local users. Consistent with the NSI Concept of Operations, as with any analytic tool, DHS and authorized recipients of DHS ISE-SAR will conduct proper due diligence to verify any leads before incorporating such information into analytical products or taking any adverse action against an individual.[8]

Related to the potential for adverse action against an individual based upon erroneous or inaccurate information in the NSI Shared Space is concern about the NSI's "reasonably indicative" criteria. Because this criteria is broader than other criteria typically associated with law enforcement authorities like probable cause or reasonable suspicion, there is a risk that more information about individuals who have no relationship to terrorism may be recorded in the NSI Shared Space. DHS mitigates this risk in a number of substantial ways. First, initial vetting requires NSI participants to manually review each proposed ISE-SAR against the ISE-SAR Functional Standard Version 1.5. Generally this will narrow the scope of the reports in the NSI Shared Space to those bearing a nexus to terrorism. Second, DHS has limited its retention of ISE-SAR data available in the DHS-ISE SAR Server to five years unless a component proactively validates that the information continues to meet the ISE-SAR Functional Standard Version 1.5. Third, the Department's data quality practices will require it to delete or edit, as appropriate, ISE-SAR records, once entered, that are later found to be erroneous or bear no nexus to terrorism. Finally, and most importantly, DHS and authorized recipients of DHS ISE-SAR will conduct proper due diligence to verify any leads before incorporating such information into analytical products or taking any adverse action against an individual.

Mission creep is also another major privacy risk presented by participation in the NSI; specifically the risk that DHS SAR that are not terrorism-related are submitted to the NSI Shared Space. DHS has mitigated this risk by establishing a review process that is documented in the DHS ISE-SAR Initiative Concept of Operations to ensure that components review their SAR data (the contents of which may contain information outside the scope if the ISE-SAR Functional Standard), for adherence to the ISE-SAR Functional Standard Version 1.5 before submitting those ISE-SAR to the DHS ISE-SAR Server. In addition the DHS Privacy Office will conduct a privacy compliance review of the program's NSI participation within nine months of a program's inclusion as an authorized NSI participant. This will include an assessment of whether ISE-SAR contributed by DHS components to the DHS ISE-SAR Server adhere to the ISE-SAR Functional Standard. Component participation in the NSI is contingent upon completion of mandatory NSI training. While the NSI actively contemplates eventual expansion of nationwide SAR efforts beyond the current terrorism-related scope and corresponding ISE-SAR Functional Standard, such expansion is currently outside the scope of DHS' near-term efforts upon which

[8] NSI Concept of Operations, Version 1 (December 2008) at 22: "As in any analytic process, all information is subject to further review and validation, and analysts must coordinate with the submitting organization to ensure that the information is still valid an obtain any available relevant supplementary material before incorporating it into an analytic product."

this PIA is based. Any expansion in scope would require additional consideration of the privacy impact including a revision of this document as appropriate.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

Several operational components within DHS regularly observe or otherwise encounter suspicious activities while executing their authorized missions and performing operational duties. Components document those observations or encounters in SAR. Across the Department the operational setting or context for activities reported in SAR, including reports from the public and private sectors, are as varied as the Department's mission responsibilities. Engagement with the NSI will alter neither those underlying mission functions nor upset the current methodologies employed by DHS components collecting information on suspicious activities and documenting SAR. Rather, the NSI will facilitate the more effective sharing and discovery of ISE-SAR – both internally and among DHS and external NSI participants – by incorporating a standardized technological and functional approach for recording and storing ISE-SAR throughout DHS.

DHS' legal authorities to participate in the NSI can be found in:

- the Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002);
- the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266 (2007) (codified in various sections of the U.S.C.);
- the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004) (codified in various sections of U.S.C.);
- the National Security Act of 1947, as amended;
- 5 U.S.C. Section 301; and
- Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans.*

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

DHS ISE-SAR submitted to the NSI Shared Space are covered by the "DHS/ALL-031 Information Sharing Environment Suspicious Activity Reporting Initiative System of Records," September 10, 2010, 75 FR 55335. Concurrent with the publication of DHS/ALL-031, DHS issued a Notice of Proposed Rulemaking to exempt this system from certain provisions of the Privacy Act September 10, 2010, 75 FR 55290.

Additionally as previously noted, several operational components within DHS regularly observe or otherwise encounter suspicious activities while executing their authorized missions and performing

operational duties. To the extent these activities trigger the requirements of the Privacy Act, they will be conducted in accordance with the applicable component-specific SORN (See Appendix A).

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. The Authority to Operate was issued on November 17, 2010 and will be valid for three years.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

DHS is working with NARA to develop a records retention schedule of no more than five years for DHS ISE-SAR data maintained on the DHS ISE-SAR Server. This retention schedule does not alter the retention schedules of the information identified in existing components' retention schedules for their underlying SAR data. DHS components maintain the authority to withdraw and/or edit any and all ISE-SAR data that they have entered into the DHS ISE-SAR Server in accordance with their respective policies

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

ISE-SAR data is not subject to the requirements of the Paperwork Reduction Act because a specific form completed by the public is not used to populate the information in DHS-ISE SAR Server.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

Categories of individuals whose information may be included in ISE-SAR include:

- Individuals whose behavior is reasonably indicative of pre-operational planning related to terrorism or other criminal activity associated with terrorism.
- Witnesses who have observed individuals whose behavior reasonably is indicative of pre-operational planning related to terrorism or other criminal activity associated with terrorism.
- Individuals who have a material relationship to the activity or behavior reported in an ISE-SAR (e.g., the owner of a particular vehicle that was observed in a ISE-SAR, where it is unclear whether the person was actually driving the vehicle).

- DHS employees and contractors who have submitted ISE-SAR data to the DHS ISE-SAR Server.
- DHS employees and contractors who use the NSI Shared Space for conducting research and analysis with a potential terrorism nexus.
- Federal, state, local, tribal, territorial and private sector officials whose agency or organization is part of the NSI and have submitted ISE-SAR that meets the ISE-SAR Functional Standard Version 1.5 and whose information DHS personnel have a need to know for the performance of their official duties.
- Federal, state, local, tribal, territorial, and private sector officials whose agency or organization is an NSI participant and who use the NSI Shared Space for conducting research and analysis with a potential terrorism nexus.

The content of an ISE-SAR varies and may or may not contain PII. For example, the ISE-SAR Summary Format, used by DHS for ISE-SAR obtained from an external agency, does not contain PII. SAR data that is entered into the NSI may include the following elements as made available by the reporting source: description of the suspicious activity (by code), a description of a possible threat (by code), date, time and location of incident, reliability rating of informational source, validity rating of content, cross-referenced record number (if applicable), critical infrastructure indicators, and names and contact information of reporting and/or responding agency personnel. An "additional comment" section provides a contextual narrative of the event and may include the following PII when available: name, alias, height, weight, sex, build, race, complexion, eye color, hair color, hair style/length, ethnicity, distinguishing features and personal identifiers (e.g., driver's license, passport, Social Security number, etc.) of the person(s) engaged and/or connected to the suspicious activity. Information that may be maintained in an ISE-SAR about an individual is described in the ISE-SAR Functional Standard Version 1.5 (see Appendix B for a full listing).

DHS will use the information in the NSI Shared Space to draw linkages among ISE-SAR made available by NSI participants for the purposes of preventing, disrupting, or halting terrorism-related incidents and for analytical purposes that are consistent with the ISE-SAR Functional Standard Version 1.5 to identify possible trends and provide general analytical products that inform other components as well as state and local users.

2.2 What are the sources of the information and how is the information collected for the project?

Each of the NSI participants own or administer proprietary servers that maintain their validated ISE-SAR and against which other NSI participants will be able to conduct federated searches. This set of servers, although maintained by different participants, is referred to as the NSI Shared Space. Like each NSI participant, DHS has developed its own server, known as the DHS ISE-SAR Server, which will enable authorized DHS components and other NSI participants to search all DHS ISE-SAR. Records available for querying in the NSI Shared Space are obtained from ISE-SAR submitted by federal, state, local, tribal, and territorial agencies and private sector organizations who are NSI participants.

The respective mission sets of DHS components are varied and entail coverage across multiple sectors. DHS components use a standardized technical approach across DHS to incorporate SAR data into the DHS ISE-SAR Server. Trained DHS personnel will review component SAR and submit to the DHS ISE-SAR Server only those SAR data that meet the ISE-SAR Functional Standard. DHS will use the SAR Vetting Tool, a solution developed by the NSI, to manage the creation, editing, and contribution of ISE-SAR to the DHS ISE-SAR Server.. A list of authorized DHS components participating in the NSI is included in Appendix A and will be updated as each component meets the DHS ISE-SAR Initiative requirements.

Process for determining a DHS ISE-SAR

The first step in the process of identifying an ISE-SAR is for a trained analyst in the component collecting the SAR 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 Version 1.5 (see Appendix B). 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 exercise personal judgment based upon a combination of knowledge, experience, and available information, to determine whether the information has a potential nexus to terrorism. In keeping with current NSI standards when suspicious activity is determined to have a potential nexus to terrorism, trained DHS personnel will enter the ISE-SAR data into the DHS ISE-SAR Server.

Process for determining an External DHS ISE–SAR

DHS will only submit information obtained from an external agency into the DHS ISE-SAR Server in the Summary ISE-SAR Information format. This format excludes privacy fields or data elements that contain PII as identified in Section IV of the ISE-SAR Functional Standard. It is believed the data contained within a Summary ISE-SAR Information format will support sufficient trending and pattern recognition to trigger further analysis and/or investigation where additional information can be requested from the submitting organization. Because of variances in the ISE-SAR DHS expects to share, only the minimum elements are considered mandatory. These minimum elements include date, time, location, and behavior.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

The DHS SAR initiative may use commercial or publicly available data to provide supplementary information related to the ISE-SAR. In cases where commercial or publicly available data is relevant and necessary to the ISE-SAR, the analyst will include it.

2.4 Discuss how accuracy of the data is ensured.

Given the nature of SAR, it is not always possible to obtain accurate, relevant, timely and complete information. Recognizing this, on September 10, 2010, DHS issued a notice of proposed rulemaking (75 FR 55290) to propose exemptions from the Privacy Act's accuracy, relevancy, timeliness, and completeness requirements. To mitigate this risk, DHS users are trained how to properly input and interpret ISE-SAR using contextual data concerning the source of the information to help assess the quality and reliability of each ISE-SAR. DHS users of ISE-SAR are trained on the nature of SAR and as a requirement for participation in the NSI, must take NSI training on applying the ISE-SAR Functional Standard. The ISE-SAR Functional Standard Version 1.5 provides for contributors to identify a source reliability code, defined as the reliability of the source in the assessment of the reporting organization (i.e., "reliable," "unreliable," or "unknown"); a content validity code, defined as the validity of the content, in the assessment of the reporting organization (i.e., "confirmed," "doubtful," or "cannot be judged"); nature of source code, defined as the nature of the source (i.e., "anonymous tip," "confidential source," "trained interviewer," "written statement – victim, witness, other, private sector," or "other source," as well as a free form text field to describe the nature of the source if "other source" is selected). Mandatory NSI training means that DHS users understand how to interpret an ISE-SAR appropriately and contribute ISE-SAR to the NSI that contain appropriate context. Furthermore, DHS users are obligated to delete or edit previously submitted SAR if they subsequently determine that that the data is now erroneous or newly discovered information related to the SAR has been discovered and appropriate editing is required.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

The major privacy risk associated with the collection is that an NSI participant may take action based on ISE-SAR data that is made available in the DHS ISE-SAR Server that may contain erroneous, inaccurate, untimely, or incomplete data. Given the nature of SAR, it is not always possible to obtain accurate, relevant, timely, and complete information. Recognizing this, DHS issued a notice of proposed rulemaking to propose exemptions from the Privacy Act's accuracy, relevancy, timeliness and completeness requirements. To mitigate this risk, DHS users are trained how to properly input and interpret ISE-SAR using contextual data concerning the source of the information to help assess the quality and reliability of each ISE-SAR. DHS users of ISE-SAR are trained on the nature of SAR and as a requirement for participation in the NSI, must take NSI training on applying the ISE-SAR Functional Standard Version 1.5. Accordingly DHS users understand how to interpret ISE-SAR appropriately and contribute ISE-SAR to the NSI that contain appropriate context. Furthermore, DHS users are obligated to delete or edit previously submitted SAR if they subsequently determine that the data is now erroneous or newly discovered information related to the SAR has been discovered and appropriate editing is required. Consistent with the NSI Concept of Operations, as with any analytic tool, DHS and authorized recipients of DHS ISE-SAR will conduct proper due diligence to verify any leads before incorporating such information into analytical products or taking any adverse action against an individual.

Related to the potential for an adverse action against an individual based upon erroneous or inaccurate information in the NSI Shared Space is concern about the NSI's "reasonably indicative" criteria. Because this criteria is broader than other criteria typically associated with law enforcement authorities like probable cause or reasonable suspicion, there is a risk that more information about individuals who have no relationship to terrorism may be recorded in the NSI Shared Space. DHS mitigates this risk in a number of substantial ways. First, initial vetting requires NSI participants to manually review each proposed ISE-SAR against the ISE-SAR Functional Standard Version 1.5. Generally, this will narrow the scope of the ISE-SAR available in the NSI Shared Space to those bearing a nexus to terrorism. Second, DHS has limited its retention of ISE-SAR data available in the DHS-ISE SAR Server to five years unless a component proactively validates that the information continues to meet the ISE-SAR Functional Standard. Third, the Department's data quality practices will require it to delete SAR records, once entered, that are later found to be erroneous or bear no nexus to terrorism. Finally, and most importantly, DHS and authorized recipients of DHS ISE-SAR will conduct proper due diligence to verify any leads before incorporating such information into analytical products or taking any adverse action against an individual.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

Once ISE-SAR are accessible, they can be used to support a range of counterterrorism analytic and operational activities. This step involves the actions necessary to integrate ISE-SAR information into existing counterterrorism analytic and operational processes, including efforts to "connect the dots," identify information gaps, and develop formal analytic products. It is also important to note that ISE Shared Spaces implementation concept is focused exclusively on terrorism-related information.[9] The ISE-SAR Functional Standard Version 1.5 is designed to support the sharing, specifically through the NSI, of information about suspicious activities that have a potential terrorism nexus. The NSI participants include: DHS; DOJ; other federal agencies carrying out counterterrorism mission functions; state, local, and tribal entities, including law enforcement agencies represented at state, regional and major urban area fusion centers; and the private sector to the extent authorized by applicable law. Components will make use of the NSI query capabilities in a manner consistent with the ISE-SAR Functional Standard Version 1.5 and their component-specific authorities. In addition to providing specific indicators of possible terrorism-related crimes, pattern and trend analysis can be performed by querying the NSI Shared Space making more information available than would typically be available within a single jurisdiction, state, or territory. Standardized and consistent sharing of suspicious activity information regarding potential terrorist threats and possible criminal activity associated with terrorism among state and major urban area fusion centers and federal agencies is vital to assessing, deterring, preventing, or prosecuting those involved in criminal activities associated with terrorism.

[9] ISE-SAR Functional Standard Version 1.5 (May 2009) pp. 10-11.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

Yes. The NSI provides a query capability to authorized NSI participants who have taken the necessary training that enable each participant to conduct a federated search of the NSI Shared Space. The NSI Shared Space employs a distributed model, where data is stored locally by the originating or contributing agency, and is "exposed" to other users in a common environment. Searches of data occur within the common environment through a single, common interface utilizing universally defined data fields, also common to the data, against which the actual queries are conducted. ISE-SAR data remains at all times under the exclusive control of the originating or submitting agency. When another NSI participant's query results in a match to a detailed SAR, that participant will be able to view the content of the associated ISE-SAR, including its PII content and contextual narrative. If, after viewing the content of a particular ISE-SAR, that participant then determines it is relevant to its mission as a result of the established nexus to terrorism, it will contact the originating or submitting participant, as appropriate, and request permission to incorporate the ISE-SAR into their data. NSI participants may also enter data into the NSI Shared Space utilizing the Summary ISE-SAR Information format, which excludes privacy fields or data elements that contain PII as identified in Section IV of the ISE-SAR Functional Standard. An authorized NSI participant may request additional information about a Summary ISE-SAR from the submitting organization.

In addition to providing specific indicators of possible terrorism-related crimes, ISE-SAR can be used to look for patterns and trends by analyzing information at a broader level through querying the NSI Shared Space than would typically be recognized within a single jurisdiction, state, or territory.

3.3 Are there other components with assigned roles and responsibilities within the system?

DHS Components identified in Appendix A are authorized to contribute ISE-SAR to the DHS ISE-SAR Server and also have querying privileges in the NSI Shared Space, given that they have met the DHS ISE-SAR Initiative requirements. In some cases, a component may only have querying privileges in the NSI Shared Space.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risks: The privacy risk is that NSI participants may misinterpret or deem the ISE-SAR available in the NSI Shared Space to have greater credibility or weight than is warranted, which may lead to inappropriate action by an NSI participant. Another risk is that users may use the information in ways that are inconsistent with or beyond the scope of the NSI (i.e., use of SAR data for non-criminal background checks or as the sole basis for making a criminal arrest and/or acquiring a search warrant, etc.).

Mitigation: These privacy risks are reasonably mitigated by the mandatory NSI training for all participants which among other things, teaches proper application of the ISE-SAR Functional Standard Version 1.5 and limitations on appropriate use of the data in the system (i.e., for searches consistent with the scope of the ISE-SAR Functional Standard). Accordingly, NSI participants are trained on how to interpret, analyze, and vet SAR. The ISE-SAR Functional Standard Version 1.5 provides for several data fields for participants to fill in appropriate context to the suspicious activities observed so that others may properly interpret them. The NSI has established pre-defined parameters for querying the NSI Shared Space that reduce risks of inconsistent uses by NSI participants. Further, the DHS Privacy Office will conduct a Privacy Compliance Review of the program's NSI participation within nine months of a program's inclusion as an authorized NSI participant. This will include an assessment of whether ISE-SAR contributed by DHS components to the DHS ISE-SAR Server and use of the NSI Shared Space query capabilities adhere to the ISE-SAR Functional Standard.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Given the nature of SAR, individuals are not provided notice as to whether they are a subject of an ISE-SAR. However, there are numerous mechanisms that provide transparency into the NSI including the publication of the ISE-SAR Functional Standard Version 1.5 which is reproduced as Appendix B to this PIA. The PM-ISE has also made several resources, including fact sheets and relevant reports, on the NSI available at www.ise.gov. Authorized DHS components participating in the NSI provide notice of their SAR-related activities (which cover a broader scope of activities than covered by the ISE-SAR Functional Standard) through PIAs and SORNs, as appropriate (See Appendix A for a listing of authorized components and corresponding privacy documentation). DHS is publishing this PIA to provide transparency into DHS' participation in the NSI and on September 10, 2010, DHS published a SORN and associated notice of proposed rulemaking to implement Privacy Act exemptions to provide further notice regarding the maintenance of ISE-SAR data in the DHS ISE-SAR Server. In addition, DHS published its Federal Information Sharing Environment Privacy and Civil Liberties Protection Policy on its website in June 2009.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

The source of ISE-SAR varies as noted in Section 2.1. An individual or private sector organization representative's report of suspicious activities to a designated DHS representative is voluntary, as is submission of their PII (e.g., a suspicious activity may be reported anonymously by a

member of the public to DHS). Individuals who are the subject of ISE-SAR do not supply the information and, because of the nature of the SAR process, they are not given the opportunity to consent to uses, decline to provide information or opt-out of the NSI.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Individuals who are the subject of ISE-SAR are not made aware of the collection of their information.

Mitigation: This privacy risk is inherent to this type of collection given the nature of the SAR process and the fact that individuals who are the subject of SAR are not the suppliers of the information and are therefore not given notice or opportunity to consent to specific uses of their information. However, DHS, DOJ, and the PM-ISE and have taken steps to provide transparency into the NSI as described in 4.1 including DHS publication of this PIA and a SORN, the PM-ISE website, and the NSI[10] website.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

DHS components maintain the authority to withdraw and/or edit any and all SAR data which they have entered into the DHS ISE-SAR Server in accordance with their respective policies. DHS is working with NARA to develop a records retention schedule for DHS ISE-SAR data of no longer than five years. After five years, ISE-SAR data from the DHS ISE-SAR Server will be purged unless a component reassesses and validates that an ISE-SAR continues to meet the ISE-SAR Functional Standard. The DHS functional owner of the data will be notified before the five-year mark, that their data will be purged from the system unless action is taken to re-validate ISE-SAR.

DHS based the five-year retention schedule on both the operational needs of the Department as well as the five year retention period used by many state NSI participants who link their use to a system governed by 28 CFR Part 23.[11] This retention schedule does not alter the retention schedules of the information identified in existing components' retention schedules for their underlying SAR data.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: What qualifies as an ISE-SAR today may no longer qualify in the future.

Mitigation: DHS recognizes that information determined to be an ISE-SAR today, may, at some point, no longer meet the ISE-SAR Functional Standard. Given the nature of SAR, however, it is not

[10] http://www.nsi.ncirc.gov
[11] 28 CFR Part 23 is a regulation that governs federally-funded interjurisdictional and multijurisdictional criminal intelligence systems that are operated by or on behalf of state and local law enforcement agencies.

always feasible to specifically identify relevancy. Accordingly, DHS has issued a notice of proposed rulemaking proposing exemptions from the accuracy, relevancy, timeliness, and completeness requirements of the Privacy Act. Notwithstanding, DHS has proposed retention schedule of no more than five years that will meet the operational needs of the DHS components contributing ISE-SAR to the DHS ISE-SAR Server. Currently, each component is responsible for managing their data submitted to the DHS ISE-SAR Server and is responsible for to deleting or editing previously submitted SAR respectively based upon evidence that the data is now erroneous or newly discovered information related to the SAR has been discovered and appropriate editing is required. ISE-SAR data will be purged after five years. The DHS functional owner of the data will be notified before the five-year mark that their data will be purged from the system unless action is taken to re-validate ISE-SAR data.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Yes. When components contribute ISE-SAR to the DHS ISE-SAR Server, they make this information available to other authorized NSI participants who have query access through the NSI Shared Space for uses consistent with the ISE-SAR Functional Standard. This may include federal, state, tribal, local, international, or foreign law enforcement agencies or other appropriate public or private sector organizations.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

DHS is sharing its ISE-SAR in the NSI Shared Space with authorized NSI participants ina manner that is compatible with the purpose of the DHS/ALL-031 ISE-SAR Initiative SORN. This SORN was created to allow DHS components that produce, receive, and store SAR pursuant to their existing authorities, responsibilities, platforms, and programs to compile and share report data that also meet the ISE-SAR Functional Standard Version 1.5 with authorized participants in the NSI. This includes sharing with federal departments and agencies, state, local and tribal law enforcement agencies, and the private sector. Routine use G of the DHS/ALL-031 ISE-SAR Initiative SORN authorizes sharing of ISE-SAR to the NSI Shared Space.

6.3 Does the project place limitations on re-dissemination?

Yes. NSI participants querying the NSI Shared Space are not able to download ISE-SAR for re-dissemination. Once ISE-SAR data are submitted to the DHS ISE-SAR Server, they are available in a read-only format to authorized NSI participants who have access to the NSI Shared Space. Should an NSI participant want to re-disseminate a DHS ISE-SAR they would need to contact the ISE-SAR

contributor to acquire the record, provide context for the perceived terrorism nexus, and obtain permission for its onward dissemination.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

When a record is viewed by another NSI participant, this information will be logged into the DHS ISE-SAR Server so that DHS is aware of which user/organizations have reviewed a particular record. As noted earlier, ISE-SAR residing on the DHS ISE-SAR Server will be available to other NSI participants in a read-only format.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk of access or disclosure of DHS-ISE SAR data by unauthorized recipients.

Mitigation: The NSI has established a privacy framework by which only authorized participants may query the NSI Shared Space. The framework requires that participants be properly trained and requires that the NSI participants have a privacy, civil rights, and civil liberties policy that has been determined by the PM-ISE to be at least as comprehensive as the Privacy Guidelines. In addition, data entered by DHS obtained from an external agency will entail the use of the Summary ISE-SAR Information format, which excludes privacy fields or data elements that contain PII as identified in Section IV of the ISE-SAR Functional Standard Version 1.5 thus mitigating risk of unauthorized access or disclosure of PII.

Privacy Risk: There is a risk that the information will be accessed by NSI participants and used in ways that are beyond the scope of the ISE-SAR Functional Standard.

Mitigation: This privacy risk is mitigated by mandatory NSI training for all participants which among other things, teaches proper application of the ISE-SAR Functional Standard Version 1.5 and appropriate use of the NSI Shared Space query capabilities. Accordingly, NSI participants are trained on how to interpret, analyze, and vet SAR. The ISE-SAR Functional Standard Version 1.5 provides for several data fields for participants to fill in appropriate context to the suspicious activities observed so that others may properly interpret them. In addition, the NSI has established pre-defined parameters for querying the NSI Shared Space that reduce risks of risks of inconsistent uses by NSI participants.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

Although individuals may request access to information about themselves contained in a DHS system of records through DHS Privacy Act/Freedom of Information Act (FOIA) procedures, DHS ISE-SAR related records are exempt from the access and correction provisions of the Privacy Act. Individuals may also request access to information about themselves contained in component specific SAR-related records subject to applicable exemptions under the Privacy Act (see SORNs referenced in Appendix A). Concurrent with the publication of the DHS/ALL-031 Information Sharing Environment Suspicious Activity Reporting (SAR) SORN, DHS published a notice of proposed rulemaking to propose exemptions from the access provisions of the Privacy Act. The DHS/ALL-031 SORN is a law enforcement system and such an exemption is necessary to ensure that the subjects of SAR are not made aware of their inclusion in the report or the source of the report.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

As discussed above, individuals may request access to and correction of their information under DHS Privacy Act/FOIA procedures; however, DHS ISE-SAR data may be exempt and DHS component-specific SAR data may also be exempt from access and correction provisions under the Privacy Act and therefore access to such records will be restricted.

7.3 How does the project notify individuals about the procedures for correcting their information?

Pursuant to a Privacy Act request, an individual who is the subject of a record in this system may access those records that are not exempt from disclosure. A determination whether a record may be accessed will be made at the time a request is received. After conferring with the appropriate component or agency, the agency may waive applicable exemptions in appropriate circumstances where it would not appear to interfere with or adversely affect the law enforcement or national security purposes of the systems from which the information is recompiled or in which it is contained. Privacy Act requests for access to an individual's record must be in writing and may be addressed to the DHS FOIA/PA, The Privacy Office, U.S. Department of Homeland Security, 245 Murray Drive SW, STOP-0550, Washington, D.C. 20528-0550 or to the appropriate component, if the individual knows which component holds the record. Requests should conform to the requirements of 6 CFR Part 5, Subpart B, which provides the rules for requesting access to Privacy Act records maintained by DHS. The request should include a description of the records sought, the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: Given that individuals are not generally permitted to access or correct records about themselves available in the DHS ISE-SAR Server, there is a risk that an inaccurate or erroneous DHS ISE-SAR could be used by DHS or other NSI participants.

Mitigation: Given the nature of ISE-SAR data, it would not be practical to allow individuals to gain access to or permit correction of records about themselves. Notwithstanding, DHS and the NSI have taken several process and policy steps to mitigate risks of inaccurate data. The DHS Federal Information Sharing Environment Privacy and Civil Liberties Protection Policy outlines a number of these steps. For example, the policy states that prior to making information available to ISE recipients, DHS will provide notice to the recipient sufficient to allow that recipient to determine the nature of the information, including any limitations on the quality of the data. If DHS determines that information it originates is inaccurate or erroneously shared, it will take appropriate steps to notify the ISE participant(s) who received the information and request the correction or deletion of the inaccurate data. Recipients of DHS ISE-SAR have a reciprocal duty to notify DHS (and others with whom they shared the data) if information it provided to them is later determined to be inaccurate. DHS then has an obligation to make changes to its data to resolve reported inaccuracies.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

This PIA describes the practices that must be employed by the component in order to become an authorized component contributor to the DHS ISE-SAR Server and to obtain query rights to the NSI Shared Space. Upon confirming adherence to these practices, applicable component programs will be added to Appendix A of this document. In addition, the DHS ISE-SAR Server will maintain a transaction log to ensure appropriate use. Further, the DHS Privacy Office will conduct a privacy compliance review of the program's NSI participation within nine months from the start of its participation. The review will include an assessment of whether ISE-SAR available in the DHS ISE-SAR Server and DHS' use of the NSI query capabilities are consistent with the ISE-SAR Functional Standard.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All DHS employees are required to take basic privacy training. In addition, all individuals who are interacting with the NSI are required to take specialized training through the NSI on the use and submission of ISE-SAR data.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

The NSI has established a privacy framework by which only authorized participants may query the NSI Shared Space. The framework includes participants being properly trained on the ISE-SAR Functional Standard Version 1.5 and the organization participating having a privacy and civil liberties policy that has been determined by the PM-ISE to be at least as comprehensive as the Privacy Guidelines. Each participant agency has a responsibility to identify those who are authorized to contribute and/or query ISE-SAR data in the NSI Shared Space. DHS has conducted DHS component assessments to identify potential authorized contributors of ISE-SAR to the DHS ISE-SAR Server and authorized users of the NSI Shared Space query capabilities. In order to participate as a contributor of ISE-SAR data to the DHS ISE-SAR Server and/or obtain query privileges to the NSI Shared Space, DHS personnel must attend NSI PMO Analyst training.[12]

DHS will use the SAR Vetting Tool, a solution developed by the NSI, to manage the creation, editing, and contribution of ISE-SAR to the DHS ISE-SAR Server. DHS will assign password-protected SAR Vetting Tool logins to trained DHS personnel to either an Analyst or Supervisor role. At least one Supervisor will be assigned for each program to approve and submit ISE-SAR to the DHS ISE-SAR Server. The Analyst role permits the user to create, edit, recommend ISE-SAR for submission to the DHS ISE-SAR Server, and forward ISE-SAR for Supervisor review. The Supervisor role permits the user to approve, modify, return ISE-SAR to an Analyst, and submit ISE-SAR to the DHS-ISE SAR Server. These roles ensure that proper reviews of potential ISE-SAR are conducted prior to their submission to the DHS ISE-SAR Server. In order to query the NSI Shared Space, a user must have either a Regional Information Sharing System (RISS) or Law Enforcement Online (LEO) account and request access to the NSI Shared Space from the NSI Project Management Office. The NSI PMO reviews grants access to the NSI Shared Space to only those who have taken the requisite training. Authorized NSI participants may query the NSI Shared Space and view matching ISE-SAR, from DHS and other authorized NSI participants in a "read-only" format. NSI participants will not be able to view PII for external ISE-SAR entered by DHS as this data utilizes the ISE-SAR Summary format.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

The DHS Office of Intelligence and Analysis, primarily through the State and Local Program Office and in coordination with the Office of Operations Coordination Planning serves as the DHS liaison to NSI participation and enables new access to the system by organizations within DHS. In addition, to ensure privacy protections, the DHS Privacy Office will review DHS organizations and programs to ensure they meet the rules established in this PIA prior being granted access to contribute ISE-SAR to the

[12] http://nsi.ncirc.gov/documents/NSI_Training_Overview.pdf.

DHS ISE-SAR Server as well as obtain query access to the NSI Shared Space. As new organizations/programs within DHS are approved for access, they will be added to Appendix A.

Responsible Officials

Ronald Athmann
Office of Intelligence and Analysis
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Appendix A – Authorized DHS Component Program Participants in NSI

The following components are currently authorized participants in the NSI initiative. Below is a description of component programs SAR programs, associated IT systems, and method of connection to the DHS ISE-SAR Server. As additional components meet the requirements for participation in the NSI, they will be added to this appendix. This appendix was last updated on November 17, 2010. In addition, the DHS Privacy Office will conduct privacy compliance reviews of each of the programs listed in this Appendix within nine months from the start of their participation. The results of these privacy compliance reviews will be made available on the DHS Privacy Office website.

Transportation Security Administration (TSA)

Date Approved: November 17, 2010

Program Name/Description: TSA Federal Air Marshals (FAMS), as part of the TSA Administrator's authority to "receive, assess, and distribute intelligence information related to transportation security" as well as to "assess threats to transportation," (Section 114 of the Aviation and Transportation Security Act (ATSA) (Pub. L. 107-71, November 19, 2001, 115 Stat. 597)), collect suspicious activity reports. These reports, referred to as Surveillance Detection Reports (SDRs), may include information that meets to requirements of the ISE-SAR Functional Standard. As such, this program is a DHS participant in the NSI.

Applicable IT Systems and Privacy Documentation:

TSA's existing collections of PII are covered by the following PIA and SORN:

- PIA: DHS/TSA/PIA – 015 Tactical Information Sharing System (TISS) PIA, published March 27, 2007 and updated on June 1, 2008
- SORN: DHS/TSA- 001, Transportation Security Enforcement Record System, published May 19, 2010 69 FR 71828.

Analysts Training Complete: Yes, initial training was completed in December 2009 and June 2010.

Method of Connection to DHS ISE-SAR Server: Information will be manually input by trained analysts using the SAR Vetting Tool.

Planned Use of the NSI Query Capabilities: TSA will use the ISE-SAR data available in the NSI Shared Space consistent with its authorities in Section 114 of the ATSA Pub. L. 107-71, November 19, 2001, 115 Stat. 597.

National Protection and Programs Directorate (NPPD)

Federal Protective Service

Date Approved: November 17, 2010

Program Name/Description: NPPD Federal Protective Services (FPS)'s mission is to render Federal properties safe and secure for Federal employees, officials, and visitors in a professional and cost

effective manner by deploying a highly trained and multi-disciplined police force. The authority to collect this information is 40 U.S.C. § 1315, "Law Enforcement Authority of Secretary of Homeland Security for Protection of Public Property." As part its mission, FPS creates suspicious activity reports that it uses to identify and mitigate potential threats to federal facilities, to include those related to terrorism. These reports may contain information related to the identity of suspects, victims, witnesses or other persons pertinent to the suspicious activity report in addition to the report details. As such, this program is a DHS participant in the NSI.

Applicable IT Systems and Privacy Documentation:

- PIA: Federal Protective Service Dispatch Incident Records Management Systems published on September 16, 2009.
- SORN: DHS/All 025 - Law Enforcement Authorities in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security System of Records (75 FR 5614, published February 3, 2010).

Analysts Training Complete: Yes, initial training was completed on November 16, 2010.

Method of Connection to DHS ISE-SAR Server: Information will be manually input by trained analysts using the SAR Vetting Tool.

Planned Use of the NSI Query Capabilities: FPS will use the ISE-SAR data available in the NSI Shared Space consistent with its authorities in 40 U.S.C. § 1315, "Law Enforcement Authority of Secretary of Homeland Security for Protection of Public Property."

Office of Operations Coordination and Planning

Date Approved: December 15, 2010

Program Name/Description: The National Operations Center (NOC) in the Office of Operations Coordination and Planning (OPS) operates the NOC Patriot Report Database. The NOC Patriot Report Database is a repository for reports generated to record and track suspicious activity that may implicate terrorism-related or criminal activity. The NOC Fusion Desk officer writes a NOC Patriot Report when information received from federal, state, local, tribal, and territorial agencies and organizations, foreign governments and international organizations, domestic security and emergency management officials, private sector entities, or individuals, is determined to be credible and either possibly linked to terrorism and/or criminal behavior. As such, this program is a DHS participant in the NSI.

Applicable IT Systems and Privacy Documentation:

- PIA: NOC Patriot Report Database PIA published on December 7, 2010.
- SORN: DHS/OPS – 003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion System of Records (75 FR 69689, published November 15, 2010).

Analysts Training Complete: Yes, initial training was completed on November 14, 2010.

Method of Connection to DHS ISE-SAR Server: Information will be manually input by trained analysts using the SAR Vetting Tool.

Planned Use of the NSI Query Capabilities: OPS/NOC, pursuant to Section 515 of the Homeland Security Act (6 U.S.C. § 321d(b)(1)), will use the NSI "to provide situational awareness and establish a common operating picture for the entire federal government and for state, local, and tribal governments as appropriate, in the event of a natural disaster, act of terrorism, or other manmade disaster; ensure that critical terrorism and disaster-related information reaches government decision-makers."

National Protection and Programs Directorate (NPPD)

National Infrastructure Coordinating Center

Date Approved: December 15, 2010

Program Name/Description: NPPD National Infrastructure Coordinating Center (NICC) is the coordinating center within the Office of Infrastructure Protection (IP). The mission of IP is to lead the national effort to mitigate the terrorism risk, and to strengthen the protection of and enhance the all-hazard resilience of the Nation's critical infrastructure (6 U.S.C. § 321d(b)(1), Section 515, Homeland Security Act of 2002, as well as 6 U.S.C. § 121(d)(1), Directorate for Information Analysis and Infrastructure Protection). The NICC creates suspicious activity reports collected from Critical Infrastructure and Key Resources (CIKR) community members or the general public that it uses to identify and mitigate potential threats, to include those related to terrorism. These reports may contain information related to the identity of suspects, victims, witnesses or other persons pertinent to the suspicious activity report in addition to the report details. As such, this program is a DHS participant in the NSI.

Applicable IT Systems and Privacy Documentation:

NPPD's existing collection of PII are covered by the following PIA and SORN:

- PIA: National Infrastructure Coordinating Center Suspicious Activity Reporting Initiative

  PIA published on December 29, 2010
- SORN: DHS/NPPD 001 – NICC Records System

Analysts Training Complete: Yes, initial training was completed in November 14, 2010.

Method of Connection to DHS ISE-SAR Server: Information will be manually input by trained analysts using the SAR Vetting Tool.

Planned Use of the NSI Query Capabilities: NPPD will use the ISE-SAR data available in the NSI Shared Space consistent with its authorities under 6 U.S.C. § 121(d)(1), Directorate for Information Analysis and Infrastructure Protection.

Immigration and Customs Enforcement (ICE)

Date Approved: January 13, 2011

Program Name/Description: ICE agents, officers, and employees collect SAR data as they fulfill ICE's mission to identify criminal activities and eliminate vulnerabilities that pose a threat to our nation's borders, as well as enforce economic, transportation, and infrastructure security. For example, during the apprehension, arrest, and removal of illegal aliens, ICE employees may collect SAR data. In addition, during the investigation of activities such as immigration crimes, human smuggling, the smuggling of narcotics, weapons, and other types of contraband, financial crimes, cybercrime, and export enforcement violations, ICE employees may also collect SAR data. Finally, the public may provide SAR data through ICE's tip line. As such, this program is a DHS participant in the NSI.

Applicable IT Systems and Privacy Documentation:

- PIA: ICE will use the SAR Vetting Tool, to manage creation, editing, and storage of all of its SAR data. Raw SARs will be vetted by trained analysts to determine whether they meet the ISE-SAR Functional Standard; those that do will be populated in the DHS ISE-SAR Server and made available to other DHS personnel. Only ICE personnel will be permitted to access raw SARs or vetted SARs that do not meet meet the ISE-SAR Function Standard. Accordingly, the DHS Information Sharing Environment Suspicious Activity Reporting PIA published on November 17, 2010 covers ICE's participation in the DHS ISE-SAR Initiative.

ICE's existing collection of PII is covered by the following SORNs:

- SORN: DHS/ICE – 011 – ICE Intelligence Records System (75 FR 9233, March 1, 2010).
- SORN: DHS/ICE – 009 – External Investigations (75 FR 45081, January 5, 2010).
- SORN: DHS/ICE – 007 – Alien Criminal Response Information Management System (75 FR 8377, February 24, 2010).

Analysts Training Complete: Yes, initial training was completed on November 15-19, 2010.

Method of Connection to DHS ISE-SAR Server: Information will be manually input by trained analysts using the SAR Vetting Tool.

Planned Use of the NSI Query Capabilities: ICE will use the ISE-SAR data available in the NSI Shared Space consistent with authorities in Section 701 of the Uniting and Strengthening America by Providing Appropriate Tools Requiring to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), PL 107-56 (2001 HR 3162); 8 U.S.C. § 1103(a)(4); 8 U.S.C. § 1357(a); 19 U.S.C. § 1589a; Presidential Decision Directives 39 and 62; and Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans, dated October 27, 2005.

United States Coast Guard (USCG)

Date Approved: June 9, 2011

Program Name/Description: The Coast Guard protects the maritime economy and the environment, defends our maritime borders, and saves those in peril. As part of USCG mission its personnel report information of potential law enforcement and/or intelligence value. These reports are referred to Field Intelligence Report (FIR). The USCG's authority for the Law Enforcement Intelligence Element is 14 U.S.C. § 89. The USCG's authority for the National Intelligence Element is the National Security Act of 1947 as amended (50 U.S.C. § 401 *et. seq*.) and Executive Order 12333 as amended. FIRs provide information on foreign or U.S. activities to support CG operations, mission and intelligence requirements of other federal law enforcement or Intelligence Community (IC) analyst. As such, this program is a DHS participant in the NSI.

Applicable IT Systems and Privacy Documentation:

- USCG will use the SAR Vetting Tool, to manage creation, editing, and storage of all of its SAR data. Raw SARs will be vetted by trained analysts to determine whether they meet the ISE-SAR Functional Standard; those that do will be populated in the DHS ISE-SAR Server and made available to other DHS personnel. Only USCG personnel will be permitted to access raw SARs or vetted SARs that do not meet the ISE-SAR Function Standard. Accordingly, the DHS Information Sharing Environment Suspicious Activity Reporting PIA published on November 17, 2010 covers USCG's participation in the DHS ISE-SAR Initiative.

USCG's existing collections of PII are covered by the following PIA and SORN:

- PIA: DHS/ALL/PIA-012 Department of Homeland Security Directory Services Electronic Mail System (DSES), January 14, 2009
- PIA: DHS/USCG/PIA-004 United States Coast Guard Law Enforcement Information Data Base (LEIDB)/Pathfinder, March 31, 2008 specifically cites FIR.
- SORN: DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) Records.
- SORN: DHS/USCG-062 Law Enforcement Information Database (LEIDB)/Pathfinder September 30, 2008, 73 FR 56930 cites FIR.

Analysts Training Complete: Yes, initial training was completed in November 14, 2010.

Method of Connection to DHS ISE-SAR Server: Information will be manually input by trained analysts using the SAR Vetting Tool.

Planned Use of the NSI Query Capabilities: USCG will use the ISE-SAR data available in the NSI Shared Space query capabilities to allow intelligence analyst the ability to use data for analysis and research for various USCG intelligence products consistent with its authorities under 6 U.S.C. § 121(d)(1), Directorate for Information Analysis and Infrastructure Protection.

United States Secret Service (USSS)

Date Approved: July 27, 2011

Program Name/Description: The Protective Intelligence and Assessment Division of the Secret Service records information on persons who are showing undue or unusual interest in a protectee or a protected venue. Information is gathered from observation of suspicious activity by officers or special agents who are trained to investigate, research, and follow-up on reported information in order to resolve or provide further details about the situation, subject or activity encountered. Occasionally, information originates from an information tip from a concerned citizen. That information will only be used if trained personnel vet the information and determine it is credible and necessary in the furtherance of the agency's protective mission. As such, this program is a DHS participant in the NSI. This collection of information is authorized by the Secret Service's protective authority contained in 18 U.S.C. §§ 3056 and 3056A.

Applicable IT Systems and Privacy Documentation:

USSS will use Counter Surveillance Unit Reporting (CSUR) database. The CSUR database is a central repository of information concerning Secret Service agents' and officers' observations of suspicious activity or surveillance directed against Secret Service protectees, events, or facilities. CSUR is covered by the July 27, 2011 Counter Surveillance Unit Reporting PIA and the DHS/USSS – 004 Protection Information System SORN, 73 F.R. 77733 (Dec. 19, 2008).

Analysts Training Complete: Yes, initial training was conducted in November 17, 2010 and February 2, 2011. USSS plans on assigning additional staff to SAR Analyst duties, and training has already been requested for those staff so that it will be completed prior to start.

Method of Connection to DHS ISE-SAR Server: Information will be manually input by trained analysts using the SAR Vetting Tool.

Planned Use of the NSI Query Capabilities: Personnel may use the NSI query capability to conduct searches to determine if the subject(s) or activity has been encountered previously.

Federal Emergency Management Agency (FEMA)

Date Approved: August 8, 2011

Program Name/Description: FEMA's mission is to support citizens and first responders and ensure that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards. As part of FEMA's mission its personnel report information of potential law enforcement and/or intelligence value. These reports are referred to as Field Intelligence Reports (FIR). FEMA's authority for the Law Enforcement Intelligence Element is 14 U.S.C. § 89. FEMA's authority for the National Intelligence Element is the National Security Act of 1947 as amended (50 U.S.C. § 401 *et seq*) and Executive Order 12333 as amended. FIRs provide information on foreign or U.S. activities to support FEMA mission, operations, and the intelligence requirements of other federal law enforcement or Intelligence Community (IC) partners. As such, this program is a DHS participant in the NSI.

Applicable IT Systems and Privacy Documentation: FEMA will use the SAR Vetting Tool to manage creation, editing, and storage of all of its SAR data. Raw SARs will be vetted by trained analysts to determine whether they meet the ISE-SAR Functional Standard. Those that meet the standard will be populated in the DHS ISE-SAR Server and made available to other DHS personnel. Only FEMA personnel will be permitted to access raw SARs or vetted SARs that do not meet the ISE-SAR Function Standard. Accordingly, the DHS ISE SAR PIA published on November 17, 2010 covers FEMA's participation in the DHS ISE-SAR Initiative.

FEMA's existing collection of PII is covered by the following PIAs and SORN:

- DHS/ALL/PIA-012 DHS Directory Services Electronic Mail System (DSES), January 14, 2009.

- DHS/ALL/PIA-032, DHS Information Sharing Environment Suspicious Activity Reporting (ISE-SAR) Initiative, November 17, 2010.

- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) Records, 74 FR 49882, September 29, 2009.

Analysts Training Complete: Yes, initial training was completed in November 14, 2010.

Method of Connection to DHS ISE-SAR Server: Information will be manually input by trained analysts using the SAR Vetting Tool.

Planned Use of the NSI Query Capabilities: FEMA will use the ISE-SAR data available in the NSI Shared Space query capabilities to allow intelligence analyst the ability to use data for analysis and research for various FEMA intelligence products consistent with its authorities under 6 U.S.C. § 121(d)(1), Directorate for Information Analysis and Infrastructure Protection.

Appendix B – ISE-SAR Functional Standard Version 1.5 (May 2009)

(http://nsi.ncirc.gov/documents/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf)