U.S. Department of Transportation

Privacy Impact Assessment

Suspicious Activity Reporting (SAR)

Responsible Official

Lawrence V. Hopkins
Associate Director for Intelligence
Office of Intelligence, Security and Emergency Response
202.366.6528

Reviewing Official

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
privacy@dot.gov

18 October 2011

Executive Summary

The Department of Trasnportation (DOT) Office of Intelligence, Security and Emergency Response (OI), is leading the DOT 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). Overseen by the Department of Justice (DOJ) the NSI supports the sharing of information through the ISE about suspicious activities with a nexus to terrorism defined as, "official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity [related to terrorism]." DOT OI is responsible for developing and supporting a capabilitilty servicing all elements within the Department to share Suspicious Activity Reporting (SAR) determined to have a nexus to terrorism as defined above. DOT conducted this privacy impact assessment (PIA) because ISE-SAR may contain personally identifiable information (PII).

System Overview

The Office of Intelligence, Security and Emergency Response within the Department of Transportation (DOT OI) is responsible for providing all-source intelligence products to the Secretary of Transportation and principal staff. DOT OI ensures they are apprised of current developments and longer range trends as they affect the security of the U.S. transportation system and U.S.- involved international efforts. In addition to providing this intelligence support to the Secretary and principal staff, the DOT OI supports a variety of other DOT consumers of intelligence.

Additional aspects of this mission are:

- Collaboration and coordination with U.S. government Intelligence Community (IC) through meetings and community outreach.
- Perform analytical and coordination functions with the IC and law enforcement community required by the incident at hand, or as tasked by the Secretary and other Department principals.
- Represent DOT on a wide range of Working Groups, Committees, and Task Forces dealing with intelligence and security issues including the National Implementation Plan for the War on Terrorism; the Office of the Director of National Intelligence Customer Service Synchronization, the FBI's National Joint Terrorism Task Force, and the Global Maritime Intelligence Integration Working Group.

Current NSI participants include State and major urban area fusion centers and their law enforcement, homeland security, or other information sharing partners at the Federal as well as the State, local, and tribal (SLT) government agencies. Developed pursuant to Presidential direction, it establishes a nationwide capability to gather, document, process, analyze, and share information about suspicious incidents to enable rapid identification and mitigation of potential threats.

The ISE environment in accordance with Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as well as the Nationwide Suspicious Activity Reporting Initiative (NSI), is to the extent both appropriate and feasible is a decentralized, distributed, and coordinated environment that connects existing systems to share terrorism information. As a NSI participant, the DOT will own and manage proprietary systems that maintain the Department's validated information Sharing Environment (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. In concert with the practices established by the NSI and deployed by other NSI participates, DOT has developed an ISE-SAR environment which supports the ability of authorized individuals within DOT offices and other NSI participants to search the DOT ISE-SAR. In addition, authorized individuals within DOT OI will have access to a federated search capability, available through the NSI, for searching all ISE-SAR available across the NSI enterprise (NSI Shared Space).

Several operational components within DOT regularly observe or otherwise encounter suspicious activities while executing their authorized missions and performing operational duties. Components document those observations or encounters in SARs. Across the Department the operational setting or context for activities reported in SARs are as varied as the Department's regulatory responsibilities.

DOT Operating Administrations that generate SARs do so in accordance with individual component legal authorities and mission responsibilities that relate to the safety and security of the national transportation system. Additionally, in support of the Intelligence Reform and Terrorism Prevention Act of 2004 and Executive Order 13356 of August 27, 2004, Strengthening the Sharing of Terrorism Information to Protect Americans, DOT is obligated to address requirements for the generation and sharing of information with the potential to protect the territory, people, and interests of the United States. Subsequently, DOT reporting efforts must be integrated into a single DOT-wide initiative, and the DOT SAR environment will function as DOT's central repository for SAR information.

The following DOT OST component is responsible for collecting, analyzing, sharing, and/or generating SAR data:

- Office Of the Secretary (OST) Office of Intelligence , Security, and Emergency Response (DOT OI)
    - Regional Emergency Transportation Coordinator/Regional Emergency Transportation Representative (RETCO/RETREP).

The following DOT Operating Administrations are capable of and are responsible for observing and reporting SAR data:

- Federal Aviation Administration (FAA);
- Federal Highway Administration (FHWA);
- Federal Motor Carrier Safety Administration (FMCSA);
- Federal Railroad Administration (FRA);
- Federal Transit Administration (FTA);
- Maritime Administration (MARAD);
- National Highway Traffic Safety Administration (NHTSA);
- Pipeline and Hazardous Materials Safety Administration (PHMSA);
- Research and Innovative Technology Administration (RITA); and
- Saint Lawrence Seaway Development Corporation (SLSDC).

The following DOT OST offices are capable of and responsible for observing and reporting SAR data:

- Office of Inspector General (OIG); and
- Office of the Secretary (OST):
    - S-80 - Chief Information Officer;
    - M-40 – Security

Engagement with the NSI will alter neither those underlying mission functions nor upset the current methodologies employed by DOT components collecting information on suspicious activities and issuing SARs. Rather, the NSI will facilitate the more effective sharing and discovery—both internally and between DOT and external NSI participants—by incorporating a standardized technological and functional approach for recording and storing ISE-SARs throughout DOT. As stated in the December 2008 NSI Concept of Operations, the NSI is not a single monolithic program, but is rather a coordinated effort that leverages and integrates all SAR-related activities into a unified nationwide SAR capability.1 The NSI strategy is to develop, evaluate, and implement common processes and policies for gathering, documenting, processing, analyzing, and sharing information about terrorism-related suspicious activities.

Once trained in the NSI program and the application of these technical and functional standards, DOT OI will review DOT Operating Administration (OA) SARs and submit the data only from those that contain a nexus to terrorism in accordance with ISE-SAR Functional Standard will be entered into the DOT ISE-SAR environment and made available to those authorized to access the NSI Shared Space. For purposes of applying the ISE-SAR Functional Standard 1.5, SAR is generally defined in the first instance as "official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity." Only a suspicious activity meeting that definition that is likewise determined to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism) is considered to be an ISE-SAR. 2

In keeping with NSI standards, whenever DOT SAR contain information indicative of suspicious activity with a potential nexus to terrorism, DOT OI will extract data from the SAR and input that data in a standardized format to the DOT ISE-SAR environment. Once in the DOT ISE-SAR environment the data will be accessible by NSI participants. NSI participants may access DOT ISE-SAR or any other NSI ISE-SAR data in the NSI Shared Environment responsive to defined search criteria; however all DOT ISE-SAR data made available to the NSI are maintained within the DOT ISE-SAR environment and the results of each user's search or query cannot be downloaded or edited.

The content of an ISE-SAR varies and may or may not contain PII. For example, the ISE-SAR Summary Format, used by DOT for ISE-SAR obtained from an external agency, does not contain PII. SAR data that is entered into the DOT ISE-SAR environment 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 A for a full listing)

[1] *Nationwide Suspicious Activity Reporting Initiative Concept of Operations (NSI CONOPS), Version 1,* Washington, D.C.: Program Manager, Information Sharing Environment, December 2008: 3-5, available at http://www.ise.gov/docs/sar/NSI_CONOPS_Version_1_FINAL_2008-12-11_r5.pdf

[2] *Information Sharing Environment Functional Standard, Version 1.0*, Washington, D.C.,: Program Manager, Information Sharing Environment.

DOT will identify standards and processes to support the reporting, tracking, processing, storage, analysis, integration, retrieval, and dissemination of terrorism-related suspicious activity reports that comport with the ISE-SAR Functional Standard. Those standards and established processes will be applied to all ISE-SAR made available by DOT OI to the NSI community via the NSI Shared Environment.

Fair Information Practice Principles (FIPPs) Analysis

The fair information practice principles (FIPPs) are rooted in the tenets of the Privacy Act are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs, are common across many privacy laws and provide a framework that will support DOT efforts to appropriate identify and mitigate privacy risk. The FIPPs based analysis conducted by DOT is predicated on the privacy control families articialted in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3, sponsored by the National Insitute of Standars and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council[3]*.*

Transparency

Due to the nature of the SAR mission, it is individualized or specific notice to individuals as to whether they are a subject of an ISE-SAR is not possible. However, there are numerous transparency mechanisms that inform the public on the NSI effort generally and DOT activities specifically in support of the ISE.

The ISE-SAR Functional Standard Version 1.5, containing the specific criteria for and limitations on the development of ISE-SAR and population of the NSI environment, as well as other resources such as fact sheets, and reports, are available for review on the ISE public website.4

DOT has provided generalized notice to the public of its participation in the NSI environment through the DOT/ALL—23 Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) Initiative System of Records, System of Records Notice (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 DOT ISE-SAR Server. (September 11, 2011, 76 FR 55334) The publication of this PIA furthers demonstrates DOT's commitment to provide appropriate transparency into the Departments participation in the NSI. Furthermore DOT published its Federal Information Sharing Environment Privacy and Civil Liberties Protection Policy on its website in October 2011. In accordance with PM-ISE direction and applicable law, all notices were provided prior to DOT's sharing of information to the NSI.

Owing to the decentralized nature of DOT and the specific missions of its various operating administration, each OA whose information may be provided to the NSI through the DOT ISE-SAR initiative must provide notice of their SAR-related activities through PIAs and SORNs, as appropriate. Only those SAR generated by the OAs that meet the ISE Functional Standard 1.5 will be shared with the NSI. Appendix B provides a brief summary of each DOT program authorized to participate in the NSI as well as links to the specific SORN and PIA published for each activity.

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. Draft policies are submitted to the PM-ISE for review and approval before participants are permitted

[3] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf

[4] Http://www.ise.gov

to post or access PII (i.e., Privacy Fields) in the NSI Shared Space. DOT's Privacy Policy for the Federal Information Sharing Environment was published in October 2011.

Individual Participation and Redress

Subject to the limitations of the Privacy Act, individuals may request access to information about themselves contained in a DOT system of records through DOT's Privacy Act/Freedom of Information Act (FOIA) procedures. Concurrent with the publication of the DOT/ALL—23 Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) Initiative System of Records, SORN, DOT published a notice of proposed rulemaking to propose exemptions from the access provisions of the Privacy Act. The claimed exemptions are necessary to ensure that subject individuals of records within the system are not are not made aware of their inclusion in the report or the source(s) of information in those records.

DOT will review all Privacy Act requests on an individual basis and may as appropriate, waive applicable exemptions if the release of information to the individual would not detrimentally impact the law enforcement or national security purposes for which the information was originally collected or is subsequently being used.

As a matter of policy, DHS extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DOT by complying with DOT Privacy Act regulations, 49 CFR Part 10. Privacy Act requests for access to an individual's record must be in writing either handwritten or typed, may be mailed, faxed or emailed. DOT regulations require that the request include; 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. Additional information and guidance regarding DOT's FOIA/PA program may be found on the DOT website.5 Privacy Act requests may be addressed to;

Claire W. Barrett
Departmental Privacy Officer
1200 New Jersey Ave., SE
E31-312
Washington, DC 20590
Email: privacy@dot.gov
Fax: (202) 366-7024

Individuals may also request access to information about themselves contained in OA specific SAR-related records subject to applicable exemptions under the Privacy Act (see SORNs referenced in Appendix B).

Purpose Specification

DOT Operating Administrations have occasion to collect and report SAR in the course of executing authorized mission and operational responsibilities in accordance with individual component legal authorities. The contexts in which suspicious activities may be observed and/or encountered and the methods for report the same are unique to each Operating Administration. Common to all elements of the Department is the requirement to support the prevention of terrorist attacks within the United States and overall reduction of terrorist-related vulnerability. The DOT SAR initiative

[5] http://www.dot.gov/foia/

serves as the point of integration of the myriad of DOT suspicious activity reporting processes and outcomes and serves as the sole authoritative means of identifying and making available through the ISE SAR meeting the ISE Functional Standard 1.5 for terrorism related SAR across the DOT enterprise as well as with the wider law enforcement and intelligence community

Engagement with the NSI will alter neither an Administration's stated mission nor their current operational methodology for collecting and recording suspicious activities.

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

- Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002);
- (Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004);
- Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266 (2007); and
- Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans* (Oct. 27, 2005)

Data Minimization & Retention

DOT with the support of the National Archives and Records Administration (NARA) is working to develop a records retention schedule for records maintained as part of the DOT ISE-SAR initiative. DOT anticipates that once a retention schedule is approved that it will retain records in the DHS ISE-SAR environment for not more than five years, unless an active decision, supported by analysis, is made on the part of the OA nominating the record for inclusion in the ISE-SAR environment that the data continues to meet the requirements of the Functional Standard. If the sponsoring OA does not provide necessary rationale for retaining the data beyond the five year mark the records will be automatically removed from the system. OAs may remove nominated SAR from the system at any time prior to the conclusion of the five year period. DOT's proposed retention period is in keeping with other federal and state NSI participants. DOT records in the ISE-SAR environment will not be deleted until the proposed retention schedule is approved by NARA. The retention schedule for the DOT ISE-SAR environment does not impact established the retention schedules of the source systems maintained by the OAs from which the ISE-SAR data originates.

Use Limitation

DOT OI is responsible for providing analysis with regional and national perspectives. Regionally, the analytical process may provide an integrated understanding of a broader topic, region, or mission. Nationally, the analytical process may integrate traditional national intelligence with local and national law enforcement and the private sector to provide a unique view of homeland security threats. Designated DOT OI analysts will review and analyze SAR as part of their daily functions to detect indicators which can establish trends, patterns, and baselines of activity. These reports, which provide possible indicators of preoperational activity, help to inform private and public sector authorities and officials regarding security decisions and related activities. These reports also assist security officials to prioritize security related efforts such as training, funding, and equipment purchasing decisions. DOT OI will fully integrate SAR information into all-source products for Federal and SLT customers as necessary. The aforementioned access to DOT ISE-SAR by DOT OI will be bound by the following stipulations:

The sharing practices related to ISE-SAR shall meet applicable legal, regulatory, programmatic, and oversight obligations. Access to DOT ISE-SAR or to individual data-elements within specific ISE-SAR must be linked to a user's lawfully defined duties that directly support the affected agency's mission.

If, after viewing the content of a particular DOT ISE-SAR, that NSI participant determines it is relevant to its authorities as a result of the established nexus to terrorism, he/she is required to contact DOT OI and request permission to incorporate the ISE-SAR with their data. In many instances the information garnered from the NSI Shared Space will be statistical in nature and not require sharing the actual record.

Data Quality and Integrity

Information in the DOT ISE-SAR environment has been exempted from the Privacy Act's requirements for accuracy, timeliness, relevancy, and completeness. The rationale for these exemptions stems from the very nature of suspicious activity reporting in that information is regularly collected through observation and/or third party and/or unverified sources.

DOT staff responsible for reviewing candidate SAR for inclusion in the NSI Shared Space are required by the Department of Justice to take NSI training on applying the ISE-SAR Functional Standard to ensure that only those SAR with indicia of a terrorism nexus are made available for use by NSI participants. Once an authorized DOT OI staff member's completes the requisite training that individual is eligible to review all SAR data in the DOT SAR environment and nominate those SAR meeting the definition of having nexus to terrorism to the NSI Shared Space.

DOT SAR made available through the NSI Shared Space remains at all times under the exclusive control of DOT. NSI participants will be able to view all of the content of available ISE-SAR meeting their search criteria, including available PII and contextual narrative. If, after viewing the content of a particular ISE-SAR, that participant determines the ISE-SAR is relevant to the participant agency's authorities as a result of the established nexus to terrorism, DOT may grant permission to incorporate the DOT ISE-SAR into the requestor's system.

Security

The DOT ISE-SAR environment received its authority to operate based on certification and accreditation requirements of the Federal Information Security Management Act (FISMA) and National Institute of Standards and Technology (NIST) requirements documented in Special Publication 800-53 – Recommended Security Controls for Federal Information Systems and Organizations in October 2011. DOT has implemented technical, physical, and administrative controls including role based access, encryption, training, and card-key access to limit the access to ISE-SAR data to those with an authorized need. Additionally, the DOT ISE-SAR environment will maintain a transaction log to ensure verify that only authorized users access the system and that those users behave in accordance with DOT policy.

Accountability and Auditing

DOT OI personnel authorized to enter ISE-SAR data into the DOT ISE-SAR environment will receive "ISE-SAR Analyst" training, which is provided by the Department of Justice, Office of Justice Programs, Bureau of Justice Assistance as part of the NSI. The "ISE-SAR Analyst" training provides analysts with a clear understanding of the ISE-SAR Functional Standard, addresses privacy concerns, and introduces technical capabilities that facilitate the entry of ISE-SAR data into the Shared Space.

In order for an OA to actively participate in the DOT ISE-SAR environment as either a contributor of ISE-SAR or access to the NSI Shared Space it must conform to the precepts outlines in this PIA. Once the DOT ISE has determined that the OA meets the minimum threshold requirements for participation applicable component programs will be added to Appendix A of this document. The DOT Privacy Office will conduct regular periodic privacy compliance reviews of the DOT ISE-SAR environment to include but not limited to adherence to the controls established in the Functional Standard, this PIA, and the DOT/ALL-23 SORN.

DOT maintains the authority to withdraw or edit any and all ISE-SAR data entered or provided for entry into the NSI Shared Space in accordance with DOT policies. This provides for more control over the data and ensures that the data is as accurate as possible. If an ISE-SAR previously entered into the NSI Shared Space is later found to be incompatible with the ISE Functional Standard, DOT will remove the affected SAR data from the NSI Shared Space.

Responsible Official

Lawrence V. Hopkins
Associate Director for Intelligence
Office of Intelligence, Security and Emergency Response

Approval and Signature

Original signed and on file with the DOT Privacy Office

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer

Appendix A – Privacy Fields in DOT ISE SAR Environment

As described in the ISE-SAR Functional Standard Version 1.5 published in May 2009, the below information related to individuals identified as "privacy field" that may be maintained in the DOT ISE-SAR environment. Additional fields not discussed below but not identified as "privacy fields" may also be included.

- Aircraft descriptions, including:
  - [cir] Aircraft engine quality.
  - [cir] Aircraft ID (privacy field).
  - [cir] Aircraft tail number (privacy field).
- Driver License:
  - [cir] Expiration date (privacy field).
  - [cir] Driver license number (privacy field).
- Location:
  - [cir] Location description (privacy field).
- Location Address:
  - [cir] Street number (privacy field).
  - [cir] Unit ID (privacy field).
- Location Coordinates:
- Observer:
  - [cir] Person employer ID (privacy field).
- Owning organization:
  - [cir] Organization ID (privacy field).
- Other Identifier:
  - [cir] Person identification number (PID) (privacy field).
  - [cir] PID effective date (privacy field).
  - [cir] PID expiration date (privacy field).
- Passport:
  - [cir] Passport ID (privacy field).
  - [cir] Expiration date (privacy field).
- Person:
  - [cir] AFIS FBI number (privacy field).
  - [cir] Date of birth (privacy field).
  - [cir] State identifier (privacy field).
  - [cir] Tax identification number (privacy field).
- Person Name:
  - [cir] First name (privacy field).
  - [cir] Last name (privacy field).
  - [cir] Middle name (privacy field).
  - [cir] Full name (privacy field).
  - [cir] Moniker (privacy field).

- Registration:
    - [cir] Registration number (privacy field).
- Vehicle:
    - [cir] Vehicle identification number (privacy field).
    - [cir] US DOT number (privacy field).
- Vessel:
    - [cir] Vessel official Coast Guard number identification (privacy field).
    - [cir] Vessel ID (privacy field).
    - [cir] Vessel IMO number identification (privacy field).
    - [cir] Vessel serial number (privacy field).

Appendix B – Systems/Programs Engaged in SAR Initiative