Privacy Impact Assessment Update
for the

Department of Homeland Security
Information Sharing Environment (ISE)
Suspicious Activity Reporting (SAR) Initiative

DHS/ALL/PIA-032(a)

May 12, 2015

Contact Point
David Sobczyk
Program Manager
Office of Intelligence and Analysis
(202) 447-4232

Reviewing Official

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

This Privacy Impact Assessment (PIA) updates a previously published PIA describing the Nationwide Suspicious Activity Reporting Initiative, a key aspect of the federal Information Sharing Environment (ISE) created by Congress in the Intelligence Reform and Terrorism Prevention Act of 2004. The NSI supports intergovernmental sharing of "official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity [related to terrorism]," known as Suspicious Activity Reports (SAR). As a result of the NSI's successes, the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) will continue the effort and transition the management to a jointly managed program. DHS is conducting this PIA update because SARs contain personally identifiable information (PII).

Overview

The Department of Homeland Security (DHS or Department) Office of Intelligence and Analysis, primarily through the State and Local Program Office in coordination with the Office of Operations Coordination Planning, leads the DHS effort to implement the Nationwide Suspicious Activity Reporting Initiative (NSI).[1] 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).[2] The NSI is a collaborative effort by DHS, the Federal Bureau of Investigation (FBI), and state, local, tribal, and territorial law enforcement partners. It 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]."[3]

The ISE is designed to facilitate the sharing of terrorism information among all relevant entities through the combination of information sharing policies, procedures, and technologies. 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

[1] For additional information about the Nationwide SAR Initiative, please visit http://nsi.ncirc.gov/default.aspx.
[2] *Intelligence Reform and Terrorism Prevention Act of 2004*, Pub. L. 108-458 (December 17, 2004).
[3] ISE-SAR Functional Standard v. 1.5.5, *available at* http://nsi.ncirc.gov/documents/SAR_FS_1.5.5_PMISE.pdf. This definition was developed after critical input from several privacy, civil rights, and civil liberties advocacy groups, including the American Civil Liberties Union (ACLU). The SAR process is critical to sharing information about suspicious activity with a potential nexus to terrorism, which can help prevent terrorist attacks and other related criminal activity from occurring. In developing the standards and processes, the NSI leveraged the guidance and expertise provided by the Global Justice Information Sharing Initiative (Global), which serves as a Federal Advisory Committee and advises the U.S. Attorney General on justice information sharing and integration initiatives. This includes leveraging the National Information Exchange Model (NIEM), which allows the interoperability and seamless exchange of information.

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.[4] The long-term goal is for most federal, state, local, and tribal law enforcement organizations to participate in a standardized, integrated approach to gathering, documenting, processing, analyzing, and sharing information about suspicious activity that is potentially related to terrorism. In addition to government agencies, private sector organizations responsible for critical infrastructure and foreign partners are also potential sources for ISE-SARs.

Reason for the PIA Update

On October 1, 2013, DHS and the FBI, in coordination with the Bureau of Justice Assistance (BJA), directed the nationwide transition of the NSI Shared Space to a new technology platform in support of the seamless sharing of SARs. Consequently, DHS and the FBI assumed responsibilities as co-executive agents for the NSI. Training, technical assistance, and outreach are now the responsibility of DHS, while the FBI is responsible for NSI technology. These changes strengthen the core mission of the NSI, which remains to assist agencies with adopting compatible processes, policies, and standards that foster broader sharing of SARs, while ensuring that privacy, civil rights, and civil liberties are protected. Primary functions of the NSI executive agents include advocating on behalf of the initiative, providing guidance to participants at all levels, and coordinating various efforts within the NSI.

Section 1016 of IRTPA and the NSI direct that, to the greatest extent possible, the ISE should be a decentralized, distributed, coordinated environment that connects existing systems to share terrorism information. Previously, each of the NSI participants owned or administered proprietary servers that maintained their validated ISE-SARs and against which other NSI participants would be able to conduct federated searches. This set of servers, although maintained by different participants, was referred to as the NSI Shared Space.

As described in the original 2010 PIA, [5] like each NSI participant, DHS developed its own server to maintain its ISE-SARs (known as the DHS ISE-SAR Server), to enable authorized DHS components and other NSI participants to search DHS ISE-SARs. In addition, authorized DHS components had access to a federated search capability, available through the NSI, for searching all ISE-SAR available in the NSI Shared Space.

---

[4] THE NATIONAL STRATEGY FOR INFORMATION SHARING (October 2007), *available at* http://nsi.ncirc.gov/documents/National_Strategy_for_Information_Sharing.pdf. *See also* THE NATIONAL STRATEGY FOR INFORMATION SHARING AND SAFEGUARDING (December 2012), *available at* http://nsi.ncirc.gov/documents/NSISS_2012_White_House.pdf.

[5] *See* DHS/ALL/PIA-032 Department of Homeland Security Information Sharing Environment Suspicious Activity Reporting Initiative (November 17, 2010), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-dhswide-sar-update-20101117.pdf.

The new technical solution is based on best practices of both the FBI's eGuardian[6] system and the NSI's Shared Space technologies. DHS will continue to submit SARs to the DHS internal SAR Vetting Tool (SVT), and then to the NSI SAR Data Repository (NSI SDR). The SDR is based on best practices from both the FBI's eGuardian system and the NSI's Shared Space technologies. Previously, DHS submitted ISE-SARs to the Shared Space, as opposed to directly to the NSI SDR, because the NSI Shared Space provided a robust auditing and accountability framework, and supported the five year retention period for DHS ISE-SARs submitted to NSI.[7] The NSI SDR was created to mirror the privacy protections developed in the NSI Shared Space. Now these protections will apply to all submitted SARs, including from state, local, tribal, and territorial and federal law enforcement partners. Since NSI SDR was created to implement the best practices from the NSI Shared Space, DHS will now submit ISE-SARs directly to the NSI SDR for access in the FBI's eGuardian system.

Since the publication of the original PIA, NSI developed the SDR to mirror the auditing and retention requirements embedded in the Shared Space for the use of all NSI participants. Therefore, the NSI SDR replaced the Shared Space and removed the need for duplicate reporting within two separate systems. Now, DHS submits ISE-SARs directly to the NSI SDR. However, to query the NSI SDR, participants (including DHS) use eGuardian.

The NSI's policy, training and outreach were transitioned to the DHS Office of Intelligence and Analysis as of October 1, 2013, and the NSI's technology solution was transitioned to the FBI on January 31, 2014. DHS is updating this PIA to address the impact of the technology transition on the DHS process for sharing ISE-SAR data with other NSI partners.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

No change from 2010 PIA.

---

[6] For a full privacy assessment of the eGuardian system, please visit http://www.fbi.gov/foia/privacy-impact-assessments/eguardian-threat/#section4.

[7] The Federal Protective Service (FPS) submits SAR directly through eGuardian. Although not all SARs submitted directly to eGuardian may have met the functional standard to be included in the NSI (Report vs. Share). FPS will continue to contribute to ISE-SAR primarily through manual entries made within eGuardian. This allows FPS to participate in the investigation of the reported SAR through assigned Joint Terrorism Task Force (JTTF) Officer(s) and through our Regional Intelligence Agents. Submitting SAR directly to eGuardian allows FPS to leverage the JTTFs as a force multiplier by routing SAR reports directly to the appropriate FBI JTTF location responsible for conducting an assessment into the SAR.

Characterization of the Information

No change from 2010 PIA.

Uses of the Information

The DHS internal processes have remained the same since the publication of the 2010 PIA; however, with the elimination of the NSI Shared Space, DHS now submits SARs directly to the NSI SDR. By submitting directly to the NSI SDR, which then feeds eGuardian, DHS eliminates the need for duplicate submissions to multiple systems. The original SAR vetting process is outlined below as background.

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 1.5.5 (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 trained analyst then inputs the SAR meeting the criteria into the SVT.

Using the SVT, the second step in the process is for a separate DHS 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 NSI SDR.

Notice

No change from the 2010 PIA. However, note that the FBI has published new privacy compliance documentation about eGuardian to provide further transparency about the NSI SDR and SAR process.[8]

Data Retention by the project

The previously published PIA noted that DHS was in the process of developing a records retention schedule for the Shared Space with NARA. DHS has since determined that a records schedule is not needed because the Shared Space has been abandoned. All ISE-SARs submitted to the NSI SDR must still follow the retention schedules of the information identified in existing components' retention schedules for their underlying ISE-SAR data. DHS components still maintain the authority to withdraw or edit any and all ISE-SAR data that they have entered into

[8] For a full privacy assessment of the eGuardian system, please visit http://www.fbi.gov/foia/privacy-impact-assessments/eguardian-threat/#section4.

the NSI SDR in accordance with their respective policies.

Information Sharing

Despite the technical changes from the Shared Space to the SDR, there are no changes regarding external information sharing from 2010 PIA. The technical changes merely enhance the existing information sharing initiatives.

Redress

No change from 2010 PIA.

Auditing and Accountability

The internal process for reporting and storing SAR information has not changed. DHS now sends information considered to meet the threshold of the ISE-SAR Functional Standard directly from the SVT to the NSI SDR. The NSI SDR was created to have the same auditing and accountability requirements as the previous Shared Space, for use by all participants in the NSI.

Responsible Official

David Sobczyk
Program Manager
Office of Intelligence and Analysis
U.S. Department of Homeland Security

Approval Signature

Original signed copy on file with DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
U.S. Department of Homeland Security