Privacy Impact Assessment

for the

Significant Event Notification (SEN) System

DHS Reference No. DHS/ICE/PIA-023(a)

October 15, 2021

Abstract

The Significant Event Notification system (SEN) is a reporting and law enforcement intelligence transmission capability developed by U.S. Immigration and Customs Enforcement (ICE), a component of the U.S. Department of Homeland Security (DHS). The ICE Office of Homeland Security Investigations (HSI) developed this system to create reports for ICE field and headquarters managers to provide timely information about critical incidents, activities, and events that involve or impact ICE field staff. The system also handles law enforcement intelligence communication from the ICE Office of Enforcement and Removal Operations (ERO) field offices to field and headquarters managers and ERO and HSI intelligence personnel. The original SEN PIA was published in 2010.[1] ICE is updating this PIA to reflect the current configuration of the program and to accurately document that SEN accesses and stores personally identifiable information (PII) gathered in the course of official ICE investigations or other law enforcement activities.

Overview

SEN allows for the creation, manual entry, query, and modification of various reports. Since the publication of the original SEN PIA, ICE has reduced the number of reports users may create, so that SEN only captures the minimum amount of information necessary in furtherance of the system's purpose.[2] The reports no longer used have been discontinued throughout ICE as they were determined to have minimal operational value. The remaining reports are outlined below.

Significant Incident Report (SIR): ICE field agents/officers fill out a SIR to provide information and awareness to ICE field and headquarters managers regarding field events that have already occurred, such as significant arrests, assaults on employees, the discharge of firearms involving employees, and/or significant seizures.[3] Once submitted, SIRs are available to various SEN users including the appropriate ICE HSI Special-Agent-in-Charge (SAC), the appropriate ERO Field Office Director (FOD), the appropriate ICE Field Intelligence Group (FIG), and the

[1] *See* U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement, Privacy Impact Assessment for the Significant Event Notification (SEN) System, DHS/ICE/PIA-023 (2010), *available at* https://www.dhs.gov/privacy-documents-ice.

[2] This reduction applies to reports that are no longer in use: Law Enforcement Agency Requests for Assistance (LEARA); PREDATOR Significant Incident Arrest Reports (OPPRED); and SPOT (not an acronym) reports. This reduction also applies to U.S. Customs and Border Protection (CBP) Air and Marine Operations Reports (AMO), which were not in the original PIA but added since that time. Historical AMO, OPPRED, and LEARA reports are viewable in read only mode. Archived data from these reports may still be accessed, but they no longer actively collect new data. Thus, SEN only captures the minimum information necessary in furtherance of the system's purpose. The SEN business owner decided to streamline SEN because the SEN current business needs do not require the use of the aforementioned historical reports.

[3] A significant seizure is a seizure of goods that warrants immediate notification to headquarters based on quantity and/or circumstance.

ICE Joint Intelligence Operations Center (JIOC) which analyzes the SIRs and sends summaries of them to the appropriate offices and divisions,[4] hereafter "field offices."

Significant Prospective Enforcement Activity Report (SPEAR): ICE field agents/officers fill out a SPEAR to communicate data to ICE field and headquarters managers about anticipated enforcement actions such as planned searches, arrests, or seizures. SPEARs are available to various SEN users including the appropriate field office.

Intelligence Lead Report (iLeads module): In the original SEN PIA, the iLeads module was referred to as the Enforcement and Removal Operations (ERO) LEAD report.[5] ERO personnel submit an iLead report when reporting gathered information they believe might have law enforcement intelligence value. For example, individuals arrested by ICE are typically vetted to assess the level of threat they pose (e.g., violent offenders, non-violent offenders, gang-affiliates) to ensure they are handled appropriately during detention. This assessment may indicate that the individual is connected with a gang or has a warrant out for their arrest. The assessments typically include subject interviews, criminal record reviews, and visual inspections of the individual and/or their possessions. ERO field personnel submit the information they gather (such as an individual's gang status) via SEN. Various SEN users, including the appropriate field office, as well as ERO and HSI personnel are able to access and review the iLeads module. ICE then distributes the law enforcement intelligence it gathers to recipients who have a valid need to know, such as authorized users in HSI.

TAV: ERO personnel submit Third Agency Visit Reports (TAV) when they receive requests to interview ERO detainees from other federal, state, local, tribal, territorial, foreign, and international law enforcement agencies.[6] TAVs can be viewed by various SEN users including the appropriate field office and the JIOC which provides ICE management with the ability to ensure that visits by non-ICE personnel are appropriate and do not impair ICE operations.

SEN's ownership and primary purpose relating to significant events has not changed since the original PIA.[7]

[4] The ICE Joint Intelligence Operations Center (JIOC) is a round-the-clock facility that monitors significant event reports from ICE personnel, distributes information as appropriate throughout ICE, and briefs ICE leadership on important past and prospective events.

[5] The name of the module is Intelligence Lead Reports or iLeads (plural). An individual report in the module is referred to as an iLead (singular). In addition, HSI has eliminated "ERO" in front of iLeads/iLead. Office names change over time. To avoid misalignment between a current office name (e.g., ERO) and iLeads/iLead, HSI prefers omitting "ERO" when using iLeads/iLead. The "iLeads/iLead" name describes the function of the module/report without reliance on an office name.

[6] HSI has eliminated "ERO" from "ERO TAV." Office names change over time. To avoid misalignment between a current office name (e.g., ERO) and the TAV report, HSI prefers omitting "ERO" from the TAV report name which describes the function of the report absent the office name.

[7] Significant events are "momentous or notable incidents, events, or activities that involve or impact ICE agents and

Reason for the PIA Update

SEN has undergone several changes since the original SEN PIA was published in July 2010. The 2021 SEN PIA update more completely and accurately describes the changes in the way PII is collected, used, shared, and stored. The specific changes to SEN are as follows:

- A reduction in the number of reports produced by SEN. As indicated above, SEN used several types of reports when the system was first developed. After evaluating mission needs and the utility of such reports, ICE determined that it will only need to actively use four (4) types of reports going forward.[8] Historical AMO, OPPRED, and LEARA reports will be viewable in read only mode by authorized SEN users for historical purposes; historical SPOT reports are not viewable.

- SEN now shares data with other ICE and DHS systems not documented in the original SEN PIA, including: Repository for Analytics in a Virtualized Environment (RAVEn);[9] ICE's Investigative Case Management system (ICM);[10] FALCON;[11] the Use of Force, Assaults, and Discharges SharePoint Solution (UFAD);[12] and the CBP Analytical Framework for Intelligence (AFI).[13]

- The 2021 SEN update deploys a mobile capability. This is not a mobile application, but rather a method by which SEN users can access the system in the mobile environment. The mobile version of SEN provides the same view that a SEN user would see when the user accesses the system on a computer. This increased mobility is especially helpful for agents/officers in the field, although accessing SEN from a mobile device still requires the

staff in the field in carrying out their law enforcement missions." The SEN Application User Guide, Version 3.8, provide ICE users with further information regarding this categorization.

[8] SEN has a checkbox to indicate if there is a Suspicious Activity Report (SAR) presence within a report, but SAR reports as a whole are not maintained in SEN.

[9] See U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement, Privacy Impact Assessment for the Repository for Analytics in a Virtualized Environment (RAVEn), DHS/ICE/PIA-55 (2020), *available at* https://www.dhs.gov/privacy-documents-ice. https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice055-raven-may2020.pdf.

[10] *See* U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement, Privacy Impact Assessment for the Investigative Case Management (ICM), DHS/ICE/PIA-045 (2016), *available at* https://www.dhs.gov/privacy-documents-ice., https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-icm-june2016.pdf.

[11] *See* U U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement, Privacy Impact Assessment for the FALCON Search and Analysis System, DHS/ICE/PIA-032 (2014 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-ice.

[12] The ICE Office of Firearms and Tactical Programs (OFTP) and the Office of Professional Responsibility (OPR) have developed the Use of Force, Assaults, and Discharges SharePoint Solution (UFAD) to create a central location for the timely and accurate reporting of use of force incidents involving ICE law enforcement personnel.

[13] *See* U.S. Department of Homeland Security, U.S. Customs and Border Protection, Privacy Impact Assessment for the Analytical Framework for Intelligence (AFI), DHS/CBP/PIA-010 (2012 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

user to input the URL and the login credentials that they would normally use if they were at their workstations.

- ICE is also updating this PIA to clarify that SEN will maintain previously collected Social Security numbers (SSN), but will no longer collect SSNs.[14] SEN used SSNs to identify individuals tied to SEN reports which includes both witnesses and targets. The SEN team is incorporating additional privacy protections to ensure the safeguarding of previously-entered SSNs, (discussed below in the Privacy Impact Analysis section).
    - SEN has used SSNs since the system deployed in 2007. As of the publication of this PIA update, only the iLeads module within SEN will contain masked legacy SSNs (i.e., SSNs that were collected and stored in the original SEN system), which may be shared with FALCON and CBP's AFI.
    - Prior to this PIA update, some iLead reports (formerly ERO LEAD) contained SSNs in order to identify individuals who provide ERO with intelligence.[15] In the updated SEN, legacy SSNs will be masked. However, authorized ICE personnel with a need to know may request to view the legacy, unmasked SSNs for performance of their duties. Attempts to unmask a SSN are documented in the audit logs, recording the identity and the time that the individual viewed the SSN. SEN users who wish to unmask a legacy SSN must have a need to know and such unmasking must be in accordance with the user's job responsibilities.
- Lastly, the SEN system is re-written in the latest DHS approved version of Angular technology, a platform for building web applications. This technology better suits the needs of ICE personnel who use the system by offering advances in security and functionality and decreases in technical requirements, such as coding. The Angular technology does not by itself present any privacy risk.

Privacy Impact Analysis

Authorities and Other Requirements

DHS is authorized to collect information for SEN under 5 U.S.C. § 301; 8 U.S.C. §§1103, 1357(a), and 1222; 19 U.S.C. § 1589a; 40 U.S.C. § 1315; 42 U.S.C. § 249; and 44 U.S.C. § 3101.

[14] ICE has authority to collect SSNs pursuant to the Homeland Security Act of 2002 (Pub. L. 107-296, Nov. 25, 2002) and DHS Delegation Number 7030.2. Further, ICE HSI has the authority to enforce and investigate laws residing in Title 8, 18, 19, 21, 22, 31 and 50 of the U.S. Code.

[15] Other identifying information, such as name, date of birth, and A-Numbers may still be used in iLead reports.

The DHS/ICE-006 Intelligence Records System (IIRS) SORN[16] and DHS/ICE-009 External Investigations SORN[17] apply to the collection and maintenance of information in SEN. These SORNs cover information collected and used in the course of disseminating information about significant events to necessary personnel. For example, the Intelligence Records System SORN covers information (including documents and electronic data) collected by DHS from or about individuals during investigative activities and border searches.

A system security plan (SSP) has been completed for this SEN update. The SSP was last completed on November 19, 2020.

SIR, SPEAR, iLeads, and TAV data maintained in SEN fall under Records Control Schedule n1-567-11-004.[18] This system does not collect information directly from the public and therefore it is not subject to the requirements of the Paperwork Reduction Act. No forms are used to input data into SEN.

Characterization of the Information

SEN collects and retains information about members of the public, ICE personnel, and members of other law enforcement agencies that have coordinated with ICE on official investigations or sought assistance from ICE. Since 2010, there has been a change to the Characterization of Information, particularly regarding how SSNs are used. As stated above, the initial SEN system collected and stored SSNs. SEN will no longer collect SSNs, but previously entered SSNs are still maintained should ICE agents, officers, or analysts need to view them for the performance of their duties. Presently, SEN has no designated SSN data field, and SEN's interface disclaimer advises personnel not to enter SSNs anywhere within the system, including free-text data fields.

Privacy Risk: There is an increased risk as SEN continues to maintain legacy SSNs.

Mitigation: This risk is partially mitigated. First, SEN will no longer actively capture SSNs and there is no specific data field within SEN that offers users the capability to input an SSN. As an additional mitigation, ICE has incorporated a warning banner within the iLead report advising users "you may not enter SSNs into the system." SSNs should only be accessed on a need-to-know basis in accordance with the user's job responsibilities. Third, SEN masks SSNs by default until an authorized user clicks a button to unmask the SSN. For example, a previously entered legacy SSN appears with bullet points as: "•••••••••." Only ICE authorized personnel with a need

[16] *See* DHS/ICE-006 Intelligence Records System (IIRS) System of Records, 85 Fed. Reg. 74362 (November 20, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.
[17] *See* DHS/ICE-009 External Investigations System of Records, 85 Fed. Reg. 74362 (November 20, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.
[18] The retention schedule can be found here: https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0567/n1-567-11-004_sf115.pdf.

to know may view SSNs. To view an SSN, authorized personnel must click a "view SSN" button which reveals the SSN; in turn, the unmasking is automatically logged in the SEN audit log**.**

Privacy Risk: There is a risk that SEN users without a need to know may be able to access information about individuals.

Mitigation: This risk is partially mitigated. SEN contains specific security controls that require database accounts in order to access the system on a need to know basis. Prior to gaining access to SEN, users must obtain approval through an Access Control Manager (ACM).[19] SEN does not independently manage access to the servers, but rather applies permissions based on DHS data center security practices outlined in the DHS 4300A, *Sensitive Systems Handbook.*[20] SEN Access Control Managers are in charge of granting access and employ role-based controls to ensure that the appropriate user groups can only access the information required for their job responsibilities.

This risk may arise in the context of SEN users who need to access reports outside of their specific Area of Responsibility (AOR). However, because of the nature of ICE investigations, SEN users may need to access information and reports outside of their specific AORs as cases and subjects frequently move from one jurisdiction to another.

Privacy Risk: There is a risk that SEN will collect more information about individuals than is needed for conducting the analysis and decision-making the system is designed to support.

Mitigation: This risk is partially mitigated. The SEN team annually reviews the data elements collected from various sources discussed herein (see Information Sharing section) to ensure data remains relevant for reporting needs. If certain PII is deemed no longer necessary for reporting needs, then SEN will no longer capture those data attributes going forward, as was the case with SSNs.

Uses of the Information

ICE has not identified any new uses of the information, nor any corresponding privacy risks.[21]

[19] The existing SEN users with a need to know are being kept active when carried over to the 2021 updated SEN system.

[20] *See* DHS 4300A, Sensitive Systems Handbook, *available at* https://www.dhs.gov/sites/default/files/publications/4300A%20Sensitive-Systems-Handbook-v12_0-508Cs.pdf. DHS 4300A has a rules of behavior (ROB) which all employees have to sign before they can have IT access to ICE systems.

[21] The 2021 SEN update includes the addition of an additional role of "HQ User" which will have "read only" privileges. Additionally, the System Control Officer (SCO) role has been changed to only have the capability to modify user profiles; it can no longer modify all reports in SEN.

Notice

Since the publication of the original PIA, ICE has not identified any changes to how SEN provides notice.

Data Retention by the Project

Data retention remains unchanged since the original SEN PIA. There are no changes to the risks and associated mitigations.

Information Sharing

SEN shares data internally with both ICE and DHS systems.

(i) ICE Internal: Within ICE, SEN shares data with RAVEn, ICM, FALCON, and UFAD.[22] SEN is able to import/pull data from an Investigative Case Management case as ICM sends SEN case information that corresponds with existing SEN report fields. Through the iLeads module, ICE distributes the law enforcement intelligence it gathers to recipients who have a valid need to know, such as HSI personnel.

(ii) DHS Internal: SEN has very limited interconnections among internal DHS components. However, SEN does have a CBP interconnection through the Analytical Framework for Intelligence. Through the CBP interconnection, CBP-AFI sends requested date ranges to SEN which then produces corresponding SEN reports for CBP-AFI.[23] The SEN-CBP/AFI interconnection is not a bi-directional data flow; SEN reports are a one-way data pull from SEN. ICE's RAVEn/FALCON also receive SEN reports by sending requested report date ranges to SEN.[24]

Privacy Risk: There is a risk that when data is shared, it is not appropriately secured and could be accessed by unauthorized parties.

Mitigation: This risk is partially mitigated. Appropriate security measures are taken during electronic transmission so that the risk of compromise is minimal. Any parties who have access to SEN data (i.e., ICE, CBP) maintain strict security controls which render unauthorized access very unlikely. The SEN update will also ensure SSNs contained in legacy reports are masked before being shared. Moreover, data sharing within DHS occurs behind the DHS firewall which protects the data from unauthorized access. All personnel with access to SEN data are also required to complete DHS Annual Privacy Training.

[22] UFAD is not an automated interconnection. However, where applicable, SEN may share data with UFAD manually on a case-by-case basis.

[23] CBP-AFI receives only the iLeads data through daily iLeads module requests.

[24] RAVEn receives SIR and SPEAR reports. FALCON receives SIR, SPEAR and iLead reports.

Redress

Since the publication of the original PIA, ICE has not identified any changes to redress, and there are no additional privacy risks.

Auditing and Accountability

The auditing and accountability measures remain unchanged from the previous PIA.

Contact Official

Patrick J. Lechleitner
Acting Executive Associate Director
Office of Homeland Security Investigations
U.S. Immigration and Customs Enforcement
U.S. Department of Homeland Security
(202) 732-3991

Responsible Official

Jordan Holz
Privacy Officer
U.S. Immigration and Customs Enforcement
U.S. Department of Homeland Security

Approval Signature

Original, signed copy on file at the DHS Privacy Office.

____

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717