Privacy Impact Assessment
for the

Significant Event Notification (SEN) System

July 26, 2010

Contact Point
James Dinkins
Executive Associate Director
Office of Homeland Security Investigations
U.S. Immigration and Customs Enforcement
(202) 732-5100

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

Abstract

The Significant Event Notification system (SEN) is a reporting and law enforcement intelligence transmission capability developed for the Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement (ICE). The ICE Office of Homeland Security Investigations (HSI) initiated the reporting capability 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 ICE Office of Enforcement and Removal Operations (ERO) field offices to field and headquarters managers and the ERO Intelligence Operations Unit. This privacy impact assessment (PIA) is being completed to provide notice of the existence of SEN and to publicly document the privacy protections in place.

Overview

SEN is owned and operated by HSI's Law Enforcement Support and Information Management Division. Information is input into SEN by ICE HSI and ERO personnel. SEN's primary purpose is to disseminate information to relevant management and interdivisional personnel about events to allow them to respond by allocating appropriate resources and facilitating appropriate responses to significant events.

ICE field and headquarters managers require timely information on threats and significant events that involve or impact field staff. Access to timely, critical information allows managers at ICE to effectively react to significant events as they occur, plan for significant enforcement activities, and respond effectively to requests for assistance from other law enforcement agencies.

SEN allows the manual entry, query, and modification of various reports to provide timely information to ICE managers on notable incidents, events, or activities that involve or impact ICE agents and staff in the field, carrying out their law enforcement missions. SEN also facilitates the communication of law enforcement intelligence from ERO field offices to field and headquarters managers and the ERO Intelligence Operations Unit.

SEN allows the creation of various reports that capture relevant information about significant events, requests for assistance, and law enforcement intelligence. Reports remain in draft form while they are being edited. Recipients of the reports may be determined automatically based on the organizational role of the individual who completes the report or manually based on designations by the individual who submits the report. Report recipients have a queue that allows them to see newly submitted reports for them to review. Further, a special queue is designed to give the ICE Response and Operations Center (IROC) access to a rolling list of submitted reports.

SEN includes data on individuals who are the subject of past or anticipated encounters by ICE personnel (such as witnesses, victims, suspects, and detainees) and individuals from other law enforcement agencies who contact ICE requesting assistance. SEN is also used to track news stories regarding ICE and its work. SEN also includes data on individuals who are of interest to ICE, but are not necessarily part of a past or anticipated encounter in support of its law enforcement intelligence function.

For example, SEN may contain data about a gang leader gathered from a detainee during booking, even if ICE has not encountered that individual.

There are seven (7) types of reports that users may create in SEN. Those reports are summarized below:

SIR: ICE field agents/officers fill out a Significant Incident Report (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, significant seizures,[1] etc. Once submitted, SIRs are available to various SEN users including the appropriate ICE HSI Special-Agent-in-Charge (SAC), the appropriate HSI Resident-Agent-in-Charge (RAC), the appropriate ERO Field Office Director (FOD), the appropriate ICE Field Intelligence Group (FIG), and the ICE Reporting and Operations Center (IROC) which analyzes them and sends summaries of them to the appropriate offices and divisions[2], hereafter "field offices."

OPPRED: The Operation PREDATOR (OPPRED) Significant Incident Arrest Report is essentially the same as the SIR but is used only when the incident involves a subject who committed a sexually-based crime against a victim under the age of 18. OPPREDs capture some additional information pertaining to the victim and the suspect to capture more specific information in crimes against children.

SPEAR: ICE field agents/officers fill out a Significant Prospective Enforcement Activity Report (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. The SPEAR may also be used to report future non-enforcement activities such as meetings, trainings, and conferences involving field staff.

LEARA: ICE field and headquarters agents/officers fill out a Law Enforcement Agency Request for Assistance (LEARA) when they receive requests for ICE assistance from non-ICE law enforcement agencies. By logging the requests it receives in a single location, ICE is better able to provide responses to requests for assistance in a timely and appropriate manner. LEARAs are available to various SEN users including the appropriate field office. LEARAs are updated to indicate the disposition of the request for assistance.

SPOT: SPOT reports are designed to rapidly convey information on imminent threats or critical incidents from the field to ICE Headquarters.

ERO LEAD: ERO personnel submit ERO Intel Reports (ERO LEAD) when they gather 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 versus non-violent offenders, gang-affiliates, etc.) to ensure they are handled appropriately during detention. Often, this assessment (which may involve activities such as an interview of the subject, a review of their

[1] A significant seizure is a seizure that warrants immediate notification to headquarters based on quantity and/or circumstance.
[2] The ICE Reporting and Operations Center (IROC) 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.

criminal record, or a visual inspection of the individual or their possessions) may indicate that the individual is affiliated with a gang or has a warrant out for their arrest. ERO field personnel submit the information they gather (such as the gang status of an individual) via SEN. Various SEN users, including the appropriate field office, as well as ERO's Intelligence Operations Unit, are able to access and review the ERO LEAD. ICE then distributes the law enforcement intelligence it gathers to recipients who have a valid need to know, such as HSI's Office of Investigations, or DHS's Office of Intelligence and Analysis.

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

Typical Transaction

During the course of a criminal investigation, an ICE agent arrests an individual. In addition to other recordkeeping activities associated with the arrest (e.g., writing a report of investigation for the case file), the agent will also logon to SEN and create a SIR within 24 hours of the arrest if the arrest is deemed significant under ICE policy. The agent will enter any information they deem relevant for reporting purposes including notes about the arrest. The agent can elect to have the report reviewed and approved by their supervisor, which is generally required as a matter of policy. When the agent submits the report, it is automatically available to various SEN users including the appropriate field office. It also appears in a queue of recent activities that is constantly monitored by the IROC where it is received by a team of analysts. The analysts review the reports from the field, determine their significance, summarize relevant reports, and send their summaries to the appropriate recipients, such as the directors of ICE's operational offices (e.g., ERO, HSI) and ICE leadership via email. The summaries usually include a reference to the original SEN report which allows the recipients to view further details about an incident in SEN. The SEN reports may also include a reference to the official case record, which allows the recipient to refer to the official case information, when desired.

Section 1.0 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 as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

SIR: SIRs include biographical information on suspects and victims (such as first name, last name, date of birth, age, and country of birth); citizenship, immigration, and residency information (such as address, Alien Registration Number and country of citizenship); a narrative of other relevant information (such as a description of the incident, a description of seized property, a description of injuries sustained, and information about the hospital the injured person has been taken to); and contact

information for the reporting personnel, supervisor, the action officer, and other law enforcement personnel who were notified.

OPPRED: OPPREDs include the same information as the SIR. Additionally, they include criminal history information (such as city and state of arrest, registered sex offender status, Amber Alert association status, PROTECT Act case relevance status, aggravated felon status, fugitive status, prior arrest and conviction information), limited victim information (such as age group, sex, whether the individual was the victim of smuggling or trafficking, offender relationship to victim, country of birth, and country of citizenship), and contact information for the reporting ICE personnel, their supervisor, and the action officer and other law enforcement personnel who were notified.

SPEAR: SPEARs include biographical information on suspects (such as first name, last name, date of birth, age, and country of birth); citizenship, immigration, and residency information (such as address, Alien Registration Number and country of citizenship); a narrative of other relevant information (such as a description of the proposed enforcement activity and program case information), and contact information for the reporting personnel, supervisor, and the action officer.

LEARA: LEARAs include contact information for the requesting party, contact information for the ICE personnel who receive the request, contact information for any officer to whom the request is forwarded, contact information for the relevant duty officer, a narrative describing the request (which may contain subject or victim information), and a narrative describing the disposition of the request (which may contain subject or victim information).

SPOT: SPOT Reports include a subject (which may include a suspect name or other identifying information), a summary (which may include a suspect name or other identifying information), contact information on the reporting officer, their supervisor, relevant government points-of-contact, and contact information on the ICE office that authorized the report.

ERO LEAD: ERO LEADs include a report title (which may include a suspect name or other identifying information), subject (which designates the "type" of information included in the lead, such as "narcotics" or "weapons"), source (which describes what form the intelligence came in "staff observation" or "surveillance"), the city and state associated with the lead, information about the business, organization, or person to whom the lead pertains (including name, mother's maiden name, sex, date of birth, age, city and state of residence, city and state of arrest, registered sex offender status, Amber Alert association status, PROTECT Act case relevance status, aggravated felon status, fugitive status, prior arrest and conviction information, citizenship status, country of citizenship, country of birth, immigration status, Alien Registration Number, entry date, fingerprint identification number), contact information on the reporting ICE personnel and their supervisor, and a narrative field for other comments.

ERO TAV: ERO Third Agency Visit Reports include the detainee being interviewed (including name, Alien Registration Number, and fingerprint identification number), official contact information for the law enforcement personnel requesting the interview, contact information on the reporting ICE personnel, contact information on the relevant point of contact at ERO as well as a narrative field for other comments.

1.2 What are the sources of the information in the system?

The information in SIRs, SPEARs, OPPREDs, LEARAs, and ERO TAVs is compiled by ICE field agents/officers conducting their routine daily activities in accordance with their official investigative and law enforcement duties. The PII in SEN is gathered in the course of official ICE investigations or other law enforcement activities from: a) criminal suspects, administrative immigration detainees, associates, victims, witnesses, and informants (including public tips); b) the public and private records of public and private entities such as schools, government agencies, and businesses; c) ICE personnel; d) physical and digital evidence seized from a suspect or crime scene; and e) print and online media sources reporting on ICE events such as an arrest or shooting. Some information may also be collected from other law enforcement agencies that are coordinating with ICE on official investigations or are seeking assistance from ICE. The data that is entered into SEN may be subsequently used by ICE agents when they compile their official case records.

The information in SPOTs is gathered from various sources, including those listed in the paragraph above or from other law enforcement and intelligence agencies. When critical information pertaining to imminent threats or critical incidents is received, ICE personnel write SPOT reports which can be read by all SEN users. The information will likely be synthesized from various intelligence sources, publicly reported information, official case files, unofficial law enforcement communications, tips, etc.

The information in ERO LEADs is compiled by ERO personnel employed at ICE ERO field offices or detention facilities. ERO personnel obtain this information from interviews, interrogations, observation, surveillance, and property seized from suspects, administrative and criminal detainees, their associates, victims, witnesses, and informants.

1.3 Why is the information being collected, used, disseminated, or maintained?

The information stored in SEN is collected, used, disseminated, and maintained primarily to ensure awareness of significant events, to facilitate information sharing about future and past law enforcement operations, and to aid in the administration and management of ICE resources. Some information is also collected, used, disseminated, and maintained to provide relevant law enforcement intelligence to ICE and non-ICE recipients gathered from persons encountered by ERO.

1.4 How is the information collected?

Data in SEN is collected by ICE agents/officers during the course of normal investigative and law enforcement activities, such as interviews of suspects, witnesses, and victims. Some information is drawn from business and administrative records maintained by DHS or from investigative case files. Some information about individuals is collected directly from individuals by interview or interrogation or is obtained from inspection of official records of other agencies, businesses, and other sources. Some information is obtained by approved undercover operations or the execution of a court-approved arrest or search warrant, or authorized warrantless searches. Some information is collected from applications and

supporting documents submitted to DHS to obtain immigration, registration, or other benefits. Some information is collected from other law enforcement agencies with which ICE is coordinating on an investigation, or which are requesting ICE assistance or resources.

Information is collected on paper, or electronically and then manually entered into SEN by an ICE agent/officer.

1.5 How will the information be checked for accuracy?

Typically, an ICE agent/officer's supervisor reviews SIRs, OPPREDs, and SPEARs before they are submitted. In some cases, supervisor review may be mandatory. The information in LEARAs and ERO TAVs may be checked for accuracy when they are acted upon. For example, an agent may contact the law enforcement agency that requested assistance (leading to a LEARA) to get further details and to provide assistance, if appropriate.

The information in SIRs, OPPREDs, SPEARs, LEARAs, and ERO TAVs is primarily used to ensure awareness of significant events, to facilitate information sharing about future and past law enforcement operations, and to aid in administration and management of ICE resources. It is not used to make decisions that will affect individuals and it is not relied upon as evidence in court; therefore, the risks posed to individuals by inaccurate information that may be in the system are minimized.

In some cases, certain PII entered into a ERO LEAD is not relevant to the ultimate recipient of the law enforcement intelligence (often a third agency), and it is removed before the information is passed forward, which limits the impact on individual privacy. Further, information that is relied upon to take adverse action against an individual must meet the appropriate legal standard. In cases where a ERO LEAD contains such information, the law enforcement agency must refer to the original, admissible evidence, which prevents any inaccurate information in a ERO LEAD from negatively impacting an individual.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

DHS has been authorized to collect information 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.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy Risk: There is a risk that ICE collects more information in SEN than is necessary for the purpose of the system.

Mitigation: Information included in SEN reports typically summarizes information that is already being gathered and compiled for a law enforcement investigation or other law enforcement activity. The existence of the SEN reporting system therefore does not introduce additional data

collection to ICE's normal business operations. SEN reports are appropriately secured through access controls and are distributed within the secured ICE network.

Privacy Risk: There is a risk that inaccurate information about individuals may be stored in SEN.

Mitigation: SEN reports are not used to make decisions about individuals and they are not relied upon as evidence in court. SEN reports contain a snapshot-in-time summary of a particular incident or matter only; more complete records exist concerning the investigation or law enforcement activity the report pertains to and these records are used when any action is being considered that will affect an individual. This limited use of SEN reports reduces the risk associated with any inaccurate data they may contain.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The information in SEN is collected, used, disseminated, and maintained for the use of ICE field and headquarters staff to provide a means of communication between field staff and management on notable field events, incidents, threats, and activities. SEN provides a capability that does not exist in ICE's case management systems. By creating a systematic way to record and share information about these events and notifications, it provides more structure, access, and accountability than simply relying on email to transmit this information among ICE personnel.

The primary recipients and users of SEN information (including SIRs, SPEARs, OPPREDs, LEARAs, ERO LEADs, and ERO TAVs) are field offices who use the information to manage resources, address critical issues, and maintain situational awareness of the operations they oversee. Various other managers (such as the HSI and ERO Executive Associate Directors and Assistant Directors) and ICE leadership also receive SEN reports and use them for situational awareness and to manage their areas of responsibility.

In addition to field office review, the IROC analyzes all the SIRs that are submitted by the field to identify significant events of the past 24 hours and sends summaries of their contents to the appropriate personnel. The IROC also reviews SPEARs which keep them informed of prospective events. They do not typically summarize and distribute the information contained in SPEARs due to the fact that most of these operations are sensitive and inadvertent leakage of information may compromise the effectiveness of the operations or the safety of ICE personnel.

Likewise, ERO Intelligence Operations Unit analyzes all ERO LEADs that are submitted by ERO field agents to identify significant law enforcement intelligence. ERO flags relevant law enforcement intelligence for ICE's HSI which distributes the law enforcement intelligence as appropriate. For example, a ERO LEAD may suggest the time and location of an attempted illegal border crossing. ICE will share information from that report with U.S. Customs and Border Protection (CBP) to facilitate CBP's enforcement of U.S. law at the border. Often, PII is not relevant to the non-ICE recipients of the

law enforcement intelligence and in such cases ICE removes the PII from intelligence products before they are disseminated. ERO Intelligence Operations Unit must authorize the dissemination of all law enforcement intelligence derived from its sources.

ICE also uses the information in SEN to generate statistical reports that contain no PII to track the effectiveness of various ICE programs.

2.2 What types of tools are used to analyze data and what type of data may be produced?

SEN does not perform analytical tasks, data matching, relational analysis, scoring, or pattern analysis. SEN facilitates the generation of statistical reports because it structures the entry of various data. For example, SEN allows ICE to easily track numbers and types of arrests, shootings, etc. reported. These statistical summaries do not contain PII and therefore do not have any significant privacy impact.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

SEN does not have interfaces to obtain commercial or publicly available data. However, some reports may be derived from an ICE agent/officer's examination of commercial or publicly available data sources, such as telephone directories or Internet websites, in the course of an official investigation or other authorized law enforcement activity.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Privacy Risk: There is a risk that the information contained in these reports may not be relevant to the recipients when disseminated.

Mitigation: The IROC and ERO Intelligence Operations Unit, which are the primary disseminators of SEN information, ensure that only the minimum amount of PII is contained in the reports they write. For example, the ERO Intelligence Operations Unit often removes all PII (such as the name, age, or date of birth of the interviewee who provided the information) from law enforcement intelligence products it generates because the PII is not directly relevant to the law enforcement intelligence that is being disseminated.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

All of the records entered into SEN are retained for several years (see Question 3.2) to ensure that they are available for analysis, reporting, and review.

3.2 How long is information retained?

SIR, SPEAR, and OPPRED Reports are proposed to be retained for a total of 75 years after the end of the fiscal year during which the incident, event, or activity occurred. After 25 years, these reports will be transferred to the Federal Records Center and destroyed 50 years thereafter.

LEARAs are proposed to be retained for a total of 15 years after the end of the fiscal year during which the response to the request is completed. LEARAs would be transferred to the Federal Records Center after ten (10) years and destroyed five (5) years thereafter.

ERO LEAD and ERO TAV Reports are proposed to be retained for a total of 25 years after the end of the fiscal year during which the reports were created. These reports would be transferred to the Federal Records Center after ten (10) years and destroyed 15 years thereafter.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

ICE is in the process of obtaining NARA approval for the SEN retention schedule.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Privacy Risk: Retaining SEN data longer than necessary would violate the Fair Information Principle of minimization which requires systems and programs to retain only the information necessary and relevant to complete the task associated with its initial collection.

Mitigation: The information in SEN will be retained for the timeframes outlined in Question 3.2 of this PIA to ensure that data is available to ICE for an appropriate period. The retention periods for SEN data are tailored to the types of reports SEN maintains to ensure that reports are maintained for a period of time that is appropriate to their purpose and use.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Most SEN reports are not shared with other DHS components and ICE does not give SEN user accounts to any personnel outside of ICE. SIRs, SPEARs, OPPREDs, LEARAs, and ERO TAVs are primarily designed to provide situational awareness within ICE and are not meant for a broader audience. In some limited cases, such as investigations where ICE is coordinating with CBP or another component of DHS, it is possible that ICE may share one of these reports (or a summary derived from one of these reports) within DHS. If SEN data is shared, it is only shared when the recipient has a need to know the information to carry out their mission. In cases where ICE does share case information outside of ICE, it is typically derived from the official case management systems rather than from SEN.

Unlike the reports mentioned above, ERO LEADs are specifically designed to facilitate the efficient gathering, analysis, and dissemination of law enforcement intelligence from ERO field agents with other agencies. As such, the ERO Intelligence Operations Unit, which receives ERO LEADs, shares information from ERO LEAD reports with the appropriate agency. For example, a ERO LEAD may suggest the time and location of an attempted illegal border crossing. ICE will share the information from that report with CBP to facilitate their mission of border security.

4.2 How is the information transmitted or disclosed?

In most cases copies of reports from SEN, which may include PII, are transmitted by internal e-mail on the DHS network, an unclassified, secured wide-area network. In some cases, physical copies of reports may be faxed or hand delivered by ICE personnel to other DHS recipients with a need-to-know.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Privacy Risk: A risk exists that information from SEN may be shared with other DHS components without a need-to-know.

Mitigation: If and when SEN information is shared with other DHS components, it is only shared with recipients when they have a need to know the information to carry out their mission. SEN access is strictly limited to only ICE personnel. In addition, intelligence information from ERO LEAD reports is reviewed to remove any irrelevant or unnecessary PII before that information is passed on to other DHS personnel.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

ICE does not typically share SIRs, SPEARs, OPPREDs, LEARAs, and ERO TAVs with external organizations. SIRs, SPEARs, OPPREDs, LEARAs, and ERO TAVs are meant to provide information for internal use only. In some limited cases, such as investigations where ICE is coordinating with other law enforcement agencies, ICE may share these reports with these agencies to ensure they are kept apprised of important developments.

Unlike the reports mentioned above, ERO LEADs are specifically designed to facilitate the efficient gathering, analysis, and dissemination of law enforcement intelligence from ERO field agents with other agencies. As such, the ERO Intelligence Operations Unit, which receives ERO LEADs, shares information from ERO LEAD reports with the appropriate agency. For example, if a ERO LEAD may reveal the location of a Federal fugitive, ICE will share the information from that report with the U.S. Marshals Service to facilitate the apprehension of the fugitive.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

The sharing of SIRs, OPPREDs, SPEARs, LEARAs, and ERO TAVs with parties outside of DHS is compatible with the purpose of the original collection and is authorized under the existing routine uses in the External Investigations SORN (DHS/ICE-009, January 5, 2010, 75 FR 404). ICE only shares information from SIRs, OPPREDs, SPEARs, LEARAs, and ERO TAVs in cases of when ICE is coordinating with another agency on an investigation. Typically, ICE shares information from the official case record systems via established interagency procedures rather than from SEN.

The sharing of information from ERO LEADs with external law enforcement agencies is compatible with the purpose of the original collection and is authorized under the existing routine uses in the ICE Intelligence Records System (IIRS) SORN (DHS/ICE-006, December 9, 2008, 73 FR 74735). ICE routinely shares information from ERO LEADs with the appropriate law enforcement agency via established law enforcement intelligence dissemination channels.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

In the rare cases when SIRs, SPEARs, OPPREDs, LEARAs, and ERO TAVs are shared, they are transmitted via government e-mail systems or hand delivery. Reports shared outside DHS are encrypted as a matter of policy and they are labeled to indicate their level of sensitivity.

The ERO Intelligence Operations Unit works with HSI Office of Intelligence Investigations to disseminate information gathered in ERO LEADS via ICE's Law Enforcement Intelligence Fusion System (IFS), in which law enforcement intelligence reports would be generated and then disseminated through established law enforcement intelligence channels.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Privacy Risk: Recipients may use SEN data for inappropriate purposes.

Mitigation: The privacy risk is mitigated by the fact that dissemination of information from SEN is controlled by trained law enforcement personnel who are sensitive to the adverse consequences for individual privacy and ongoing law enforcement operations that could result if the information was misused by the recipient party. The recipients of SEN information are typically other law enforcement agencies who are also trained on the proper handling and use of law enforcement information.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

Yes, notice is provided through this PIA and the External Investigations and IIRS SORNs. In cases where information is collected directly from suspects, witnesses, victims, or other persons in the course of official law enforcement investigations, law enforcement agents generally identify themselves and the interviewees are aware that their responses are being recorded for law enforcement purposes. In cases where information is collected from an individual other than the person to whom the information pertains, the individual may not be aware that information is being collected about them. In some cases, due to the nature of law enforcement investigations, individuals may not be aware that information is being collected about them.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

In most cases, due to the nature of the law enforcement investigations or operations for which the information is being collected, individuals may not have the opportunity to decline to provide information. In cases where the individual is being interviewed or interrogated in custodial setting during a criminal investigation, however, they are advised of their rights under the Fifth Amendment to decline to answer questions. In other cases, compulsory legal process may be used (e.g., subpoenas) that would not provide the individual the opportunity or legal right to decline to provide the information sought.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

In most cases, because of the DHS law enforcement, immigration, or intelligence purposes for which the information is collected, opportunities for the individual to consent to the particular uses of information may be limited or nonexistent.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Privacy Risk: A risk exists that the public is not aware of SEN or that individuals may not be aware that their information may be contained within SEN.

Mitigation: The public is provided notice of the information maintained in SEN through this PIA, the External Investigations SORN, and the IIRS SORN. As part of this PIA and SORN process, DHS reviewed the applicable SORNs to ensure that SEN information is used appropriately, given the notice provided. Further, because SEN is a system where many law enforcement contexts apply, notice or the opportunity to consent to use would compromise the ability of ICE to perform its missions and could put law enforcement officers at risk. Thus, notice of collection and consent to specific uses are not available in most cases for SEN.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

Individuals may request access to records about them in SEN by following the procedures outlined in the External Investigations and IIRS SORNs. All or some of the requested information may be exempt from access pursuant to the Privacy Act (5 U.S.C. § 552a) in order to prevent harm to law enforcement investigations or interests. Providing individual access to records contained in SEN could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension.

In addition to the procedures above, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the ICE FOIA Office. Individuals may also submit requests by fax at 202-732-0310 or by email at ice-

foia@dhs.gov. Please contact the ICE FOIA Office at (866) 633-1182 or see the ICE FOIA Office's website (http://www.ice.gov/foia) for additional information on how to submit a FOIA. If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0550, Washington, D.C. 20528.

7.2 What are the procedures for correcting inaccurate or erroneous information?

If individuals obtain access to the information in SEN pursuant to the procedures outlined in the External Investigations and IIRS SORNs, they may seek correction of any incorrect information in the system by submitting a request to correct the data. The data correction procedures are also outlined in the External Investigations and IIRS SORNs. All or some of the requested information may be exempt from amendment pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Amendment of the records could interfere with ongoing investigations, ongoing criminal procedures and law enforcement activities and may impose an impossible administrative burden on investigative agencies.

In addition to the procedures above, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the ICE FOIA Office. Individuals may also submit requests by fax at 202-732-0310 or by email at ice-foia@dhs.gov. Please contact the ICE FOIA Office at (866) 633-1182 or see the ICE FOIA Office's website (http://www.ice.gov/foia) for additional information on how to submit a FOIA. If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0550, Washington, D.C. 20528.

7.3 How are individuals notified of the procedures for correcting their information?

The procedure for submitting a request to correct information is outlined in the External Investigations and IIRS SORNs and in this PIA in Questions 7.1 and 7.2.

7.4 If no formal redress is provided, what alternatives are available to the individual?

As stated, individuals may submit Privacy Act requests for information and correction, which will be reviewed and corrected on a case-by-case basis.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Privacy Risk: A risk is presented that individuals are not aware of their ability to make record access requests for records in SEN.

Mitigation: This risk is mitigated by the publication of this PIA, and the External Investigations SORN, and the IIRS SORN which describes how individuals can make access requests under the FOIA or Privacy Act. Redress is available through requests made under the Privacy Act as described above; however, providing individual access and/or correction of the records may be limited for law enforcement reasons as expressly permitted by the Privacy Act. Permitting access to the records contained in SEN could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible administrative burden on investigative agencies.

Section 8.0 Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system and are they documented?

ICE HSI management is responsible for ensuring that all DHS personnel granted direct access to SEN are appropriately trained and monitored. ICE HSI works with the SEN system administrator to establish user accounts as users are assigned to access SEN, and to update user identification, role, and access profiles as changes are needed. All users requesting access must be approved through the SEN administrator. Most SEN users are ICE agents/officers. Other individuals may have access, including ICE leadership, support staff, and contractors working with ICE who are responsible for maintaining the system and information technology operations.

User privileges are assigned based on the user's job responsibility. User roles exist for agents, supervisors, office managers, IROC staff, Headquarters agents, HSI Intelligence Investigations personnel, Public Affairs Officers, and Office of Professional Responsibility personnel, as well as the system administrator. Certain user types only have the ability to view certain types of reports (e.g., SIRs) in the system but cannot create or edit reports (i.e., create or edit data in the system). Other user types can only run reports that contain statistical information. The user roles are appropriately tailored to provide the functions needed without exposing data to those without a need to know or risking modification of data by those who have no need to create or edit information in the system.

8.2 Will Department contractors have access to the system?

Yes, contractors have access to the system for the purposes of performing IT maintenance and related administrative tasks. They are subject to the same background checks and suitability requirements as government employees who have access to SEN.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All ICE personnel and contractors complete annual mandatory privacy and security training. The ICE Office of the Chief Information Officer (OCIO) requires all system users to read and acknowledge the ICE/DHS User Rules of Behavior (RoB) before granting initial system access to any ICE system, including SEN. SEN requires all users to review and acknowledge the ICE RoB at the user's initial log in after the user account is created. From that date, the user is required to review/acknowledge the RoB every 90 days (in conjunction with mandatory password resets).

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Certification and Accreditation (C&A) has been completed for the SEN system with formal Approval to Operate (ATO) obtained in July 2009.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

SEN uses database-level auditing to capture information associated with any viewing, insert, update, or delete of records in the dataset, and the user that performed the activity. SEN's application-specific audit trail provides adequately detailed information to facilitate reconstruction of events if compromise or malfunction occurs. The audit trail is protected from actions such as unauthorized access, modification, and destruction that would negate its forensic value. HSI reviews audit trails when there is indication of system misuse and at random to ensure users are accessing and updating records according to their job function and responsibilities.

All failed logon attempts are recorded in an audit log and periodically reviewed. The SEN System Administrator and Information System Security Officer will review audit trails regularly. SEN and supporting infrastructure audit logs will be maintained as part of and in accordance with the existing ICE system maintenance policies and procedures for ICE.

ICE also has a process in place for investigating and responding to suspicious activities on the system. That process includes automated tools to assist the administrators in their monitoring, analysis,

and reporting. Additionally, SEN operates within the DHS network and is protected by DHS network firewalls. There are no real-time interfaces between SEN and other systems.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Privacy Risk: There is a risk that PII in SEN will be accessed and used inappropriately.

Mitigation: This risk is mitigated by privacy and security training that discusses the user's obligation to protect sensitive information and the consequences for failing to do so. The risk is also mitigated by the use of audit mechanisms that log and monitor user activity. The assignment of roles to users to establish access requirements, based on their functions and regular review of those roles, mitigates the risk that unauthorized users will be able to access information they are not required to access. All systems have been through a system security certification and accreditation process that reviews those security mechanisms and procedures that are in place, and ensures they are in accordance with established policy.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

SEN is a web-based application that is accessible via the ICE Intranet to users subject to applicable background checks, suitability requirements, and official need to access based on their assigned duties.. The system allows users to manually submit records of events by filling out pre-defined fields and allows users to generate reports summarizing the records that have been submitted.

9.2 What stage of development is the system in and what project development lifecycle was used?

The SEN system is currently in the Operational and Maintenance phase of the ICE System Development Lifecycle.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No.

Responsible Officials

Lyn Rahilly
Privacy Officer
U.S. Immigration and Customs Enforcement
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security