Privacy Impact Assessment
for the

ICE Subpoena System

March 29, 2011

Contact Point
James A. Dinkins
Executive Associate Director, 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 ICE Subpoena System (ISS) is owned and operated by the Office of Homeland Security Investigations (HSI) within U.S. Immigration and Customs Enforcement (ICE), a component of the Department of Homeland Security (DHS). ISS automates the process of generating, logging, and tracking subpoenas and summonses that ICE issues in furtherance of its investigations into violations of customs and immigration laws. It also supports the generation of Form I-9 notices, which notify employers that ICE intends to inspect their records to determine if they have completed the required employment eligibility forms for their employees. ICE is conducting this PIA because ISS contains personally identifiable information (PII) about the individuals to whom these subpoenas, summonses, and notices are directed as well as the individuals who are the subjects of these legal process documents.

Overview

ICE uses ISS to generate, log, and track administrative subpoenas, summonses, and notice of Form I-9 inspection letters (Form I-9 notices) issued by the agency. ICE uses these documents to collect information during administrative and criminal investigations into violations of various immigration and customs laws, such as employment violations of U.S. immigration law, narcotics violations, financial crimes, and human trafficking and smuggling. ICE policy requires each ICE field office to account for all subpoenas and summonses issued within their areas of responsibility. ISS supports this requirement by allowing field offices to track the subpoenas, summonses, and Form I-9 notices they issue. ISS also allows ICE to track and report the issuance of these documents at an enterprise level. ISS replaces the manual logs previously maintained by individual offices to track this data. ISS also expedites and partially automates the process by which ICE creates and issues subpoenas, summonses, and Form I-9 notices.

Subpoenas and Summonses

Subpoenas and summonses are judicially enforceable demands for records, information, or testimony issued to a specific individual or entity by a government authority. ISS captures PII contained in a subpoena or summons issued by ICE, which consists of: (1) PII about the person to whom the subpoena or summons is directed (if any) and (2) PII about a suspect or other individual involved in the investigation (e.g., witness, victim) whose records, information, or testimony are being demanded (if any). When ICE serves a subpoena or summons on an entity like a corporation, the names of individual points-of-contact in a corporation (e.g., corporate legal counsel, a records custodian) may be included in the subpoena or summons, if known, to help direct the document to the appropriate individual for action. Typically, ISS does not collect or store sensitive information about individuals; the individual's name, title, and work contact information is usually all that is captured in the system. In cases where a subpoena or summons is directed toward an individual and not an entity, ISS is likely to contain the individual's name, home or work mailing address, and other contact information such as email address, home or work telephone number, and/or a fax number.

When the subpoena or summons is demanding testimony or seeking the production of records or information about an identified individual (typically the subject of an investigation or other person involved in the investigation), ISS may contain that individual's name, address, Social Security number

(SSN), date of birth, and or other data that is necessary to place on the subpoena or summons to allow the individual receiving it to identify and collect the information or records being demanded by ICE. The specific information included in ISS and on the subpoena or summons will vary depending on whom the subpoena or summons is being served and the nature of the information or records being sought. For example, a subpoena seeking financial records from a bank may disclose the subject's name, SSN (because financial institutions often use the SSN to identify their account holders), and bank account number, to allow the bank to identify the records demanded. A subpoena seeking information from a state department of motor vehicles may contain an individual's driver's license number, date of birth, SSN, and home address, for the same reason. To protect sensitive PII contained in the subpoena or summons, ICE serves the document in person, by fax, or by mail. Documents are served by fax and sent to the contact information that is on file for the known fax numbers of the recipient. ICE does not serve subpoenas or summonses by electronic means. In cases where the subpoena or summons requests the production of documents, the instructions direct that any records returned electronically to ICE be encrypted if they contain sensitive PII.

Form I-9 Notices

All employers must complete and retain a Form I-9, Employment Eligibility Verification, for each individual they hire for employment in the United States, regardless of the employee's citizenship.[1] The Form I-9 instructions require that the employer examine the employment eligibility and identity document(s) of an employee to determine whether they reasonably appear to be genuine and relate to the individual. The employer must also record the identity document information on the Form I-9 and retain it for three years after the hire date for the employee or one year after employment is terminated, whichever is later. ICE inspects employer records to determine if they have properly completed the Form I-9 for their employees and whether they are in compliance with employment requirements of the Immigration and Nationality Act. This is referred to as an Form I-9 audit. When ICE initiates an Form I-9 audit, ICE generates an Form I-9 notice in ISS and sends it to the employer as advance notice of when ICE will arrive to review the employer's I-9 forms. Form I-9 notices are always directed at employers, which are typically businesses but in some cases may be individuals. For Form I-9 notices directed to a business, ISS contains the name of the company official to whom the notice is addressed (typically the owner or chief executive), company name and address. When the Form I-9 notice is directed to an individual employer, ISS contains that individual's name and business or home address. Form I-9 notices are served by mail or fax.

ICE Subpoena System

ISS contains various tools that assist ICE agents, criminal research specialists, investigative assistants, or other authorized users with generating subpoenas, summonses, and Form I-9 notices. ISS takes the information entered by a user into predefined fields and creates an electronic version of a subpoena, summons, or Form I-9 notice which is then sent via email to the user in PDF format for review, signature, and service on the recipient. ISS also stores the information used to complete the subpoenas, summonses, and Form I-9 notices in tables that allow for statistical reporting for an individual ICE office or on an enterprise-wide basis.

[1] The Form I-9 is issued by U.S. Citizenship and Immigration Services, DHS (OMB No. 1615-0047).

ISS also contains two tools that support the issuance of subpoenas and summonses to telephone service providers (TSPs) when ICE is attempting to identify the owner of a particular telephone number. The first of these is the TSP Portability Tool, which allows ISS to use commercial data to identify in real time the current TSP for any particular telephone number.[2] During the creation of a subpoena or summons, ICE personnel enter the telephone number into ISS and the TSP Portability Tool to query data from a commercial vendor to identify the appropriate TSP. ISS also notifies ISS users when an invalid number is entered into ISS. Invalid numbers are number combinations not used by TSPs. Invalid numbers are written to an error log that is sent to the ISS user requesting the query. Once the proper TSP is identified, this information is automatically included in the subpoena or summons form being created in ISS. Using the TSP Portability Tool increases the accuracy and efficiency of this process by reducing the number of misdirected subpoenas/summonses.

Once the correct TSP for a telephone number is identified by the TSP Portability Tool, ISS uses the second tool, the TSP Locator Tool, to determine the name and contact information for that TSP's subpoena compliance department.[3] ISS then automatically inputs this information into the subpoena or summons form. The TSP Locator Tool uses information from a commercial vendor that is stored locally in the ISS database. ISS receives regular updates to this dataset from the vendor.

Employees in other ICE offices, such as Enforcement and Removal Operations (ERO) deportation officers and immigration enforcement agents, may use ISS as well. These users are given limited privileges in ISS allowing them to use the TSP Portability and Locator Tools only. They are unable to generate or view subpoenas, summonses, or Form I-9 notices. These other users will access ISS to identify the current TSP for any particular telephone number and identify the name and contact information for that TSP's subpoena compliance department.[4]

ISS Process

To begin the process, an ICE agent engaged in a criminal investigation decides to issue a subpoena for business records from a company that is the target of the investigation. The agent assigns this task to a criminal research specialist who logs into ISS, enters the ICE case number for the investigation, and selects the appropriate subpoena form. The specialist enters the company name, address, telephone number, and company official to whom the subpoena is directed, or in some cases the specialist may be able to select the business from an existing list within ISS (if, for example, the business has been served with other subpoenas or summonses in the past). The specialist inputs a description of the specific records demanded by ICE through the subpoena. The specialist then selects from an existing

[2] Telephone number portability allows subscribers to keep their existing telephone numbers when they change service from one telephone service provider to another, regardless whether the service is wireline, wireless, voice over IP (VoIP) or cable. The TSP Portability Tool allows ICE to determine the current TSP for the telephone number of interest, regardless of if and when the number was ported.

[3] ICE may also use the TSP Locator Tool to identify the TSP for an owner of a particular telephone number but as the information for the TSP Locator Tool is only updated on a monthly basis in almost all cases the TSP Portability Tool is used to access the real time TSP for any owner of a particular telephone number.

[4] ERO will use this information to generate and serve subpoenas or summonses on TSPs to obtain information regarding the owner of a particular telephone number, such as the owner's address, to facilitate ERO's service of court orders, grand jury subpoenas, or other documents related to administrative immigration matters. At this time, ERO does not use ISS to generate or track subpoenas or summonses that it issues.

list the name of the ICE agent and the name of the authorizing ICE official who will sign the subpoena.[5] ISS assigns a unique tracking number to the subpoena and emails the unsigned subpoena electronically in PDF format to the specialist, who prints the document and delivers it to the agent. After reviewing the subpoena to ensure it is correct, the agent presents it to the authorizing ICE official for signature.[6] Once approved and signed, the subpoena is served on the company by the ICE agent. Finally, when the records demanded in the subpoena are provided to ICE, the date of that record production, known as the "return date," is entered into ISS by the specialist or agent.

Section 1.0 Authorities and Other Requirements

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

ICE's legal authority for the issuance of subpoenas, summonses, and Form I-9 notices are 50 U.S.C. App. § 2411(a) for the Export Subpoena; 21 U.S.C. § 967 for the Controlled Substance Enforcement Subpoena; 19 U.S.C. § 1509 for the Customs Summons; Immigration and Nationality Act (INA) § 235(d)(4)(A) for the Immigration Subpoena; and INA § 274A(e)(2)(C) for the Form I-9 notice.

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

The applicable SORN is the DHS/ICE-009 External Investigations SORN (January 5, 2010, 75 FR 404).

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

The Certification & Accreditation process is currently in progress and expected to be completed in October 2011.

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

No. ICE is developing a proposed retention schedule consistent with the retention periods described below for submission to NARA.

[5] The process for the I-9 notice is similar. The I-9 notice is a form letter completed by the ISS user by providing the name of an individual and the company name to be served the I-9 notice. The ISS user then selects the inspection date, case agent name and the signer name.

[6] At ICE, the authorizing official for a subpoena is the Assistant Special Agent in Charge or above, and for a summons the Special Agent in Charge or designee. For I-9 notices, the issuing authority is a Group Supervisor or above.

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

The information collected during the process described in this PIA is not covered by the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

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

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

ISS retains the following categories of records containing PII:

(1) ICE Employee and Case Data: ISS maintains the name, badge number, business address, telephone number and email address for the ICE agent and criminal research specialist who created the subpoena, summons, or Form I-9 notice, the authorizing ICE official who signs the subpoena, summons, or Form I-9 notice, and the ICE official who will receive the records or information demanded in the subpoena/summons. In most cases, the ICE agent will be designated to receive the documents demanded in the subpoena/summons. ISS also maintains the name of the proceedings, if any, and the ICE case number of the investigation for which the subpoena, summons, or Form I-9 notice is being issued.

(2) Recipient Data: For subpoenas and summonses, ISS maintains the name, mailing address, telephone number, fax number, and/or email address of the person or entity to which the subpoena/summons is directed (i.e., the recipient). When directed to an entity such as a corporation, ISS typically will also retain the name of the individual in the subpoena/legal compliance department to whom the subpoena or summons is specifically addressed and their contact information. For Form I-9 notices, ISS retains the name of the company official, company name, and address.

(3) Target Data: For subpoenas and summonses that seek records or information about an identified individual, ISS maintains PII about the target, i.e., the person whose information, records, or testimony are demanded from the recipient of the subpoena or summons.[7] This information varies in content, but could include PII such as name, addresses, SSN, Tax Information Number, importer numbers, exporter numbers, Alien Registration Number, date of birth, email address, Internet protocol (IP) addresses, uniform resource locators (URLs), bank account numbers, telephone numbers, other personal identification numbers,[8] device identifiers and serial numbers, and other information that could

[7] Not all subpoenas and summonses demand information about an individual.
[8] Personal identification numbers are account numbers or other unique identifiers associated with financial accounts, communication devices, telephone calling cards, and other similar items. ICE administrative and criminal investigations into violations of various immigration and customs laws, such as employment violations of U.S. immigration law, narcotics violations, financial crimes, and human trafficking and smuggling may require the

be linked to individuals whose information is demanded. ISS stores this information in tables and uses the information to fill in the narrative field of the subpoena or summons form. Form I-9 notices do not collect or use this type of information.

(4) TSP Portability Data: Real time commercial data provided by a vendor that contains information about the current TSP for a particular telephone number. TSP Portability Data is a separate database maintained by the vendor that is queried by ISS. The information ISS receives in response to a query of a particular telephone number is limited to the name of the current TSP.

(5) TSP Locator Data: Commercial data provided by a vendor, downloaded to ISS on a monthly basis, that contains the name and contact information for the subpoena compliance departments for relevant TSPs. This information is updated on a monthly basis by a vendor and is retained locally in the ISS database.

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

The ICE Employee Data is manually input by the ICE employees themselves or by their colleagues. The Recipient Data and Target Data are typically derived from ICE criminal and administrative investigations and may be retrieved from ICE investigative case files and other ICE law enforcement recordkeeping systems. This information is derived from various investigative sources, such as telephone records requested at an earlier date; witness interviews; confidential informant debriefings; other government agencies; evidentiary documents obtained by subpoena, inspection, search warrant, or authorized electronic surveillance; and public records. This information is input manually into the system by an ISS user. If a TSP is the recipient of a subpoena or summons, the Recipient Data may also be obtained in whole or in part from the TSP Locator Data and the TSP Portability Data.

The TSP Locator and TSP Portability Data are obtained from a commercial vendor. The TSP Locator Data is stored in the ISS database and is updated electronically on a monthly basis by the vendor. This update is completed manually when an ICE employee downloads the most recent update from the commercial vendor's website. ISS accesses but does not download the TSP Portability Data when it sends a telephone number query over the Internet via a Secure Socket Layer (SSL) connection to the vendor's database.

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

Yes. As described above, the TSP Locator and TSP Portability Data are obtained from a commercial vendor. TSP Portability Data is used by ICE to identify the TSP for a particular telephone number when ICE is seeking to identify the owner of that number. TSP Locator Data is used to determine the name and contact information for the subpoena compliance departments for TSPs so that a subpoena or summons can be served on the TSP.

---

collection of personal identification numbers for investigative purposes.

2.4 Discuss how accuracy of the data is ensured.

The accuracy of information used in ICE subpoenas, summonses, and Form I-9 notices must be verified by the user, agent, criminal research specialist or any other ISS user. Subpoenas, summonses, and Form I-9 notices containing incorrect information can be voided and reissued by ICE.. Although ICE agents are the requestors of this information, ICE criminal research specialists, investigative assistants, and contract employees often perform the ISS query and subpoena generation activities at the request of the ICE agent. These duties include manual entry of Recipient and Target Data as well as entering a description of the records or information ICE is demanding, in the case of a subpoena or summons. They also identify the preferred method(s) for responding to a subpoena or summons.

For a subpoena or summons seeking the identity of a telephone number owner, ISS uses the TSP Portability Tool to identify the TSP that is currently servicing the telephone number of the subject of the subpoena or summons. ISS uses commercial data obtained from a vendor and found in the ISS Locator Tool to identify the subpoena compliance department contact information for the TSP that is servicing that telephone number. ISS also notifies ISS users when an invalid number is entered into ISS. Invalid numbers are number combinations not used by TSPs. These invalid numbers are written to an error log that is sent to the ISS user that requested the query.

If the vendors provide ICE with inaccurate data concerning the TSPs, ICE will discover such inaccuracies when the TSPs on whom the subpoenas or summonses are served respond to the demands for information. If ICE obtained and acted on inaccurate information from the commercial data sources, it could serve the wrong TSP with a subpoena for records seeking the identity of the owner of a particular telephone number, which would result in ICE not obtaining the information it seeks in a timely manner. This would cause ICE to reissue the subpoena to the correct TSP, but it would not result in the proliferation of incorrect PII or in prejudice to any individual. If through experience, ICE finds that the information provided by the vendor contains an unacceptable number of errors, ICE will have recourse to address these data quality issues with the vendor through remedies provided for in the contract, or to terminate the contract and seek an alternative source of information.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: ISS could present a risk of the over-collection of PII.

Mitigation: ICE only collects the information necessary to generate, log, track, and maintain copies of administrative subpoenas, summonses, and Form I-9 notices issued by the agency. All PII entered and collected is necessary for the purpose of generating, logging, tracking, and maintaining these documents properly. The information returned to ICE in response to a subpoena or summons, or collected during an Form I-9 audit, is not entered into ISS because maintenance of that data in the ISS system would be inconsistent with its limited purpose of tracking and generating the subpoenas, summonses, and Form I-9 notices.

Privacy Risk: The use of commercial data could present a risk of data inaccuracy.

Mitigation: ICE promotes data accuracy and integrity when using commercial sources by using credible commercial sources to increase the probability of identifying valid, relevant information about individuals. If such sources provide ICE with inaccurate data concerning the TSPs, ICE will discover such inaccuracies when the TSPs on whom the subpoenas or summonses are served respond to the demands for information. If ICE obtained and acted on inaccurate information from the commercial data sources, it could serve the wrong TSP with a subpoena for records pertaining to the owner of a particular telephone number, which would result in ICE not obtaining the information it seeks in a timely manner. This would cause ICE to reissue the subpoena to the correct TSP, but it would not prejudice any individual. If through experience ICE finds that the information provided by the vendor contains an unacceptable number of errors, ICE will have recourse to address these data quality issues with the vendor through remedies provided for in the contract, or to terminate the contract and seek an alternative source of information.

Section 3.0 Uses of the Information

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

3.1 Describe how and why the project uses the information.

As noted in Section 1.0, ICE has statutory authority to issue administrative subpoenas, summonses, and Form I-9 notices for the enforcement of immigration and customs laws. The primary function of the ISS is to generate, log, and track administrative subpoenas and summonses during criminal and administrative investigations, and Form I-9 notices issued by the agency during administrative investigations. Administrative subpoenas and summonses are issued to compel testimony or the production of documents or information, in aid of conducting an investigation into the possible violations of law including immigration and customs laws. Form I-9 notices are issued to provide advance notice to an employer that ICE has scheduled an inspection of the employer's I-9 Forms.

ISS also allows each ICE Special Agent in Charge to account for all subpoenas and summonses issued within their respective area of responsibility (i.e., HSI field office), as is required by ICE policy. In addition to accounting for all subpoenas and summonses issued, ISS also accounts for all Form I-9 notices issued. Thus, ISS replaces the separate logs formerly maintained by individual offices and tracks the information on an enterprise level.

ISS takes the information that is entered by a user into predefined fields and creates an electronic version of a subpoena, summons, or Form I-9 notice which is then sent via email to the user in PDF format for review, signature, and service on the recipient. Target and Recipient Data is entered and used to actually issue the subpoena/summons or Form I-9 notice so that it is received by the intended recipient and, in the case of summonses and subpoenas, to ensure the relevant information/records are returned to ICE in response. The TSP Locator Data and the TSP Portability Data are both used by ICE and the ISS system to identify the appropriate TSP that should be the recipient of a subpoena or summons seeking to identify the owner of a particular telephone number, and to verify that the telephone number is valid.

ISS also provides certain ICE employees, who do not work in HSI, with Basic User accounts. These Basic Users will include ERO deportation officers and immigration enforcement agents who will

use ISS to identify the current TSP for any particular telephone number and identify the name and contact information for that TSP's subpoena compliance department. ERO will use this information to generate and serve subpoenas or summonses on TSPs to obtain information regarding the owner of a particular telephone number, such as the owner's address, to facilitate ERO's service of court orders, grand jury subpoenas, or other documents related to administrative immigration matters, such as a notice to appear. However, Basic Users will not have the ability to generate or view subpoenas, summonses, or Form I-9 notices and may only use ISS to identify the current TSP for a particular telephone number and to determine the name and contact information for the subpoena compliance department at a particular TSP.

There are several tools within ISS that are used to process and/or analyze data. These tools enhance the ability of ISS users to organize and track the status of subpoenas, summonses, or Form I-9 notices they generated. The logs and reports generated by ISS are designed to be used by the ICE agent, the criminal research specialist and the investigative assistant to manage document generation, identify duplication, and to enhance the ongoing investigation.

(1) Batch Processing of Telephone Numbers: Data files containing lists of telephone numbers can be imported into the application. ISS correlates the numbers to the correct service provider using the TSP Locator Tool and the TSP Portability Tool and then generates the subpoena/summons documents for records pertaining to those telephone numbers.

(2) Duplicate Requests: ISS automatically blocks telephone numbers from appearing on multiple subpoenas/summons for the same ICE case number. This prevents ICE from making duplicate requests for the same information in the same investigation. All blocked information is written to a log file that is emailed to the person who entered the information into the ISS.

(3) Subpoena Logs: ISS generates logs of subpoenas and/or summonses issued by a particular ICE office. Logs can be generated by telephone number, case number, range of subpoena numbers, and date.

(4) Reports: ISS can produce a number of reports such as the subpoena log; telephone cross reference report; case number report; and outstanding subpoena report. The outstanding subpoena report captures the subpoenas/summonses that have been served where a response from the recipient remains outstanding.

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

ISS does not use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly.

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

There are no other DHS components with assigned roles and responsibilities within the system.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk of unauthorized access to the information maintained in ISS.

Mitigation: To mitigate this risk, ISS employs appropriate role-based access controls so only authorized users have access to the system. The access roles are assigned by the ISS System Administrator based on the requestor's employing agency (HSI, ERO), which ensures users are only granted access to information necessary to perform their official duties. Only System Administrators can access and change all fields in the database. ISS users must read and acknowledge the ICE/DHS User Rules of Behavior (RoB) before gaining access to the ISS application All database users complete annual agency mandated privacy and security training, which stresses the importance of appropriate and authorized use of personal data in government systems.

Section 4.0 Notice

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

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

This PIA provides notice to the general public as to the collection and use of information for this purpose, however, the public is already aware that in the course of criminal or civil law enforcement activities, government agencies generally may collect information using subpoenas or other similar compulsory process. Advanced notice of the collection of their information to investigative targets or others involved in the investigation generally is not provided as it would compromise ongoing law enforcement investigations.

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

Because subpoenas, summonses, and Form I-9 notices are tools used in the course of criminal and administrative law enforcement investigations, opportunities for individuals to consent to the collection and uses of their information, or to opt out, are limited or non-existent. In cases where a subpoena or summons is issued to an individual for their own records, the individual may decline to respond to the subpoena or summons. Where an individual declines to respond, ICE would file an appropriate action in District Court to enforce the subpoena or summons and the individual could raise all available defenses at that time.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals are not aware of the existence of ISS and the data it collects and maintains.

Mitigation: This PIA serves as public notice of the existence of ISS and the data it collects and maintains. The information is used only for the purpose for which it was provided through the public notice of this PIA.

Section 5.0 Data Retention by the project

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

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

ISS retains information as follows:

(1) Subpoena/Summons/ Form I-9 Notice Content: ISS retains information contained in the narrative of the subpoena or summons linked to individuals, business or entities that are the subject of the subpoena/summons. This information may include: name, address, telephone number, fax number, SSN, tax information number, importer number, exporter number, alien registration number, date of birth, email address, internet protocol address, uniform resource locator, bank account number, telephone calling card number, personal identification number, device identifiers and serial numbers. This information will be retained for a period of ten (10) years after the end of the fiscal year in which the narrative was created.

(2) ICE Agent and Designated Official Information: ISS contains the information of ICE agents, authorized approving officials, and ICE officials designated to receive information or documents requested in a subpoena or summons. This information may include: name, badge number, business address, telephone number, email address and fax number. This information will be retained for ten (10) years after the end of the fiscal year during which the employee separated from DHS.

(3) Business/Entity Contact Information: ISS maintains general and/or subpoena compliance department contact information for businesses and entities. This information may include: name, mailing address, telephone number, fax number, company name, contact and email address. This information will be retained until it is determined to be out of date, at which point it will be updated or deleted.

(4) Subpoena and Summons Logs: ISS creates logs containing data for each subpoena, summons, and Form I-9 notice issued in order to prevent duplicates from being created and provide a method to track outstanding subpoenas and summons. These logs contain the following information pertaining to the subpoena and summons: title of the proceedings, if any, for which the subpoena or summons is issued; individual or entity on which the subpoena or summons is served; issuing official; whether the subpoena or summons was issued to compel the appearance of a witness to provide testimony, the production of books, papers, or documents, or both; the date and means of service; and the ISS-assigned tracking number for each subpoena or summons (tracked by office and fiscal year, e.g., NY-08-001; NY-08-002,

etc.). This information will be retained for five (5) years after the fiscal year cutoff of the year the log was created.

(5) Subpoenas, Summonses, and Form I-9 Notices: ISS takes the information that is entered by the user into predefined fields and creates an electronic version of a subpoena, summons, or Form I-9 notice which is then sent via email to the user in locked PDF format. The PDF document is not retained in ISS but is retained by the user on his or her computer until a hard copy has been printed, signed by the issuing authority, and placed in the physical case file. Once a signed paper copy of the PDF document has been made part of the case file the electronic PDF is no longer needed and should be deleted by the recipient.

(6) Audit Logs: ISS creates audit logs to track user activities and provide accountability. These activities include users' logon, session information (such as queries and subpoena, summons, or Form I-9 notice creation), account modifications, and account profile deletions. Only authorized personnel have access to audit logs and they are kept for a minimum of 90 days. Audit logs are periodically reviewed by ISS System Administrators or the Information System Security Officer to identify suspicious or inappropriate activity.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that information will be retained for longer than necessary to accomplish the purpose for which the information was originally collected.

Mitigation: The information in ISS will be retained for the timeframes outlined in Question 5.1 to allow ICE to properly generate, log, and track administrative subpoenas, summonses, and Form I-9 notices issued by the agency. The retention period is also consistent with general law enforcement system retention schedules and is appropriate given ICE's mission and the importance of the law enforcement data pertaining to customs, immigration and other violations.

Section 6.0 Information Sharing

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

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

Subpoenas, summonses, and Form I-9 notices generated by ISS are served on the recipient once signed by the ICE authorizing official. These records may also be shared with other law enforcement agencies for a law enforcement purpose (e.g., an investigation) or with prosecutorial agencies like the U.S. Department of Justice for prosecution. Otherwise the data in ISS is not shared outside of DHS.

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

The External Investigation SORN contains routine uses that permit the sharing of final subpoenas, summonses, or Form I-9 notices with the recipients in order to obtain information about a third party, or on law enforcement or prosecutorial agencies as described above. This sharing is compatible with the law enforcement purpose for which ICE originally compiled and used this information.

6.3 Does the project place limitations on re-dissemination?

Sharing with other law enforcement or prosecutorial agencies is done on an ad hoc basis. There are typically no limitations on re-dissemination of this information and sharing is permitted as authorized by the recipient agency's SORN or information sharing policies.

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

As a matter of course, information sharing with other law enforcement agencies or the Department of Justice would be noted in the investigative case file from which the subpoena, summons, or Form I-9 notice was disclosed. In addition, the ISS logs would reflect the identity of the recipient on whom the subpoena, summons, or Form I-9 notice was served.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: The privacy risks associated with this external sharing relates to the unauthorized access to and disclosure of the information maintained in ISS.

Mitigation: The sharing of information described above is in accordance with appropriate routine uses and legally mandated sharing. As noted above, subpoenas, summonses, and Form I-9 notices generated by ISS are sent to their intended recipient only once they are signed by the ICE authorizing official. Once approved and signed, the subpoena is served on the company by the ICE agent in person, by fax, or by mail. Further, for any subpoena or summons requesting documents, ICE requests that any electronic response containing sensitive PII be encrypted to protect the information. In addition, ISS and individual investigative case files contain a record of which persons have been the recipient of any external disclosures of information maintained in ISS.

Section 7.0 Redress

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

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

Individuals may request access to records about them in ISS. All or some of the requested information may be exempt from access pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Providing individual access to records contained in ISS could inform the subject of an actual or potential investigation or reveal investigative interest on the part of DHS. 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.

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 component's FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "contacts." 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 procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

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 and law enforcement activities and may impose an impossible administrative burden on investigative agencies.

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 component's FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "contacts." 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 does the project notify individuals about the procedures for correcting their information?

The procedure for submitting a request to correct information is outlined in this PIA in Questions 7.1 and 7.2.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that that an individual may not have access or the ability to correct their information.

Mitigation: Individuals can request access to information about them under the FOIA and Privacy Act and may also request that their information be corrected. The nature of ISS and the

information it collects and maintains is such that the ability of individuals to access or correct their information will be limited.

Section 8.0 Auditing and Accountability

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

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

Audit logs track user activities and provide accountability. These activities include session information, account modifications, account profile deletions, and telephone number based queries of the TSP Locator and Portability data. ISS user activity logs allow System Administrators to view basic session information. Such session information includes events such as logon/logoff, password errors, time-outs, event times, and IP addresses. This information is automatically recorded by ISS in the user activity log and may be reviewed by System Administrators. Auditing of the subpoenas generated by users is not part of the standard audit trail but can be independently recreated and reviewed by System Administrators if needed. Only authorized personnel have access to audit logs, which are kept for a minimum of 90 days. Audit logs are periodically reviewed by System Administrators or the Information System Security Officer (ISSO) to identify suspicious or inappropriate activity. Violations are reported to the Office of the Information System Security Manager in accordance with DHS security standards, as well as the ICE Office of Professional Responsibility.

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

All ICE employees and contractors complete annual agency mandated privacy and security training, specifically the Culture of Privacy Awareness Training, Information Assurance Awareness Training and Basic Records Management Training. ISS users must also read and acknowledge the ICE/DHS User Rules of Behavior before gaining access to the ISS application.

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

All accounts are assigned to individual users and privileges are assigned based on job roles and responsibilities. Specifically, there are three levels of access:

(1) Basic Users: ICE employees who require ISS access but do not work in HSI are issued basic user accounts only. Typically, these are ERO deportation officers and immigration enforcement agents. Some HSI personnel are also issued basic user accounts, including analysts in the Field Intelligence Groups and contractors tasked with processing transactional telecommunications information. Basic Users do not have permission to generate or view subpoenas, summonses, or Form I-9 notices. Basic

Users may use the ISS Portability and Locator Tools only. Basic users' access credentials uniquely identify them so that user activity is always traceable to a particular individual.

(2) Standard Users: Standard Users have privileges to use the TSP Portability and Locator Tools, generate and view subpoenas, summonses, and Form I-9 notices, and to review subpoena logs and reports. Standard users may only view data for documents generated in their own HSI field office. Standard users' access credentials uniquely identify them so that user activity is always traceable to a particular individual.

(3) System Administrators: Create user accounts and assign users to the appropriate access privileges within ISS based on job roles and responsibilities. System Administrators have access, edit, and delete privileges for all records in the system to provide oversight, quality control and security of the application. System Administrators may also access user profiles, activate accounts, reset passwords and generally administer the system. System Administrators are permitted to view and report on the subpoenas, summonses, and Form I-9 notices issued on an enterprise level. System Administrators' access credentials uniquely identify them so that user activity is always traceable to a particular individual.

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

Currently, the system owner (HSI) does not have any information sharing agreements concerning this information, nor does it envision the expansion of the users of ISS or the intended uses of the information collected and maintained in the system. In the event that such changes were considered, HSI would engage the ICE Privacy Office to discuss the intended expanded users and/or uses of this information and update the relevant privacy compliance documentation (including this PIA) as appropriate.

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