Privacy Impact Assessment
for the

Exodus Accountability Referral System (EARS)

May 6, 2010

Contact Point
James Dinkins
Director, Office of 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

In order to enforce U.S. federal export control laws, U.S. Immigration and Customs Enforcement (ICE) and U.S. Customs and Border Protection require information from federal regulatory agencies that grant export licenses on controlled items, specifically whether a license is required and whether a license has been granted. The ICE Exodus Command Center operates the Exodus Accountability Referral System, an ICE database that initiates, tracks, and manages requests to regulatory agencies for this information. The purpose of this Privacy Impact Assessment (PIA) is to document the system's collection and use of personally identifiable information (PII).

Overview

The Exodus Accountability Referral System (EARS) is owned by the ICE Office of Investigations. EARS is an intranet-based tool that supports efforts by ICE and U.S. Customs and Border Protection (CBP) to enforce U.S. federal export control laws, including the Arms Export Control Act and the Export Administration Act. Only ICE and CBP personnel have direct access to EARS.

Many commodities and services[1] require licenses in order to be exported from the United States. The authority to license the export of these commodities and services rests with a number of federal regulatory agencies, such as the Department of State's Directorate of Defense Trade Controls, which licenses military use items such as missile systems and grenades and the Commerce Department's Bureau of Industry and Security which licenses dual use items such as civilian aircraft and tooling machines. Criminal enforcement of violations of these export laws falls primarily to ICE and CBP. ICE special agents initiate criminal investigations into possible export violations, as well as make arrests and obtain indictments for export-related criminal violations. In addition, ICE and CBP conduct thousands of seizures of arms, military weaponry, and other sensitive commodities related to illegal export schemes. These efforts significantly contribute to preventing sensitive U.S. technologies and weapons from reaching the hands of terrorists, hostile countries, and violent criminal organizations.

During the course of law enforcement investigations or border enforcement activities, ICE agents and CBP officers may identify potential violations of U.S. export control laws. To determine whether the export of a particular commodity, service, or brokering activity[2] is controlled, ICE and CBP must consult with the relevant federal regulatory agency (hereafter, licensing agency). Those agencies will advise whether the commodity, service or brokering activity at issue is "export controlled" (i.e., whether an

[1] "Services" is defined as the furnishing of assistance (including training) to foreign persons, whether in the United States or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of licensable for export commodities. An example of a service that would require an export license is providing maintenance, design, or training support for an export controlled commodity such as a missile system.

[2] Brokering activity" is defined as acting as a broker and includes the financing, transportation, freight forwarding, or taking of any other action that facilitates the manufacture, export, or import of a defense article or defense service, irrespective of its origin.

export license is required), and whether a license has been granted. ICE and CBP request this information from licensing agencies using EARS to initiate, track, and manage the request. These requests for information are called referrals.

An ICE agent or CBP officer creates a referral by entering information into EARS about the commodity, service, or brokering activity in question along with identifying information about the Principal Party in Interest, which is typically a business entity or individual who is a registered importer, exporter, or broker. Then a manager in the ICE Exodus Control Center (ECC) must review and approve the referral in EARS. ECC personnel will print out the approved referral from EARS and send to the licensing agency in paper form or will email it in electronic form. The EARS database assigns a unique identifier to each referral for tracking purposes.

The licensing agencies that receive referrals through EARS are:

- Department of State (DOS) Directorate of Defense Trade Controls - Controls exports of single-use military components and services
- Department of the Treasury Office of Foreign Assets Control - Administers embargoes and sanctions (Iranian embargo)
- Department of Commerce (DOC) Bureau of Industry and Security - Controls exports of dual-use components (dual-use components are items that have both military and civilian uses)
- Department of Justice (DOJ) Bureau of Alcohol Tobacco, Firearms and Explosives (ATF) - Controls imports of firearms
- Department of Energy (DOE) Nuclear Regulatory Commission (NRC) - Controls exports of goods used in nuclear reactors

The most common types of referrals are:

- **License Determination**. This is a request for a determination by the licensing agency as to whether an export of a commodity or service would require a license.
- **License History**. This is a request for information on whether a particular individual or company has registered or obtained any licenses from a licensing agency.
- **License Verification**. This is a request for a check on a particular license number to determine if it is valid, expired, or counterfeit.
- **Government Jurisdiction**. This initiates a review by licensing agencies of a particular commodity or service in cases where a commodity or service may be subject to the authority or jurisdiction of more than one licensing agency. The licensing agencies will make a final determination about which agency has ultimate jurisdiction.
- **Pre-trial and Trial Certification**. This is a request for an in-depth examination by the licensing agency of a commodity, service, or brokering activity to verify the agencies jurisdiction prior to an indictment, plea agreement, or judicial proceeding. Pre-trial

Certifications verify whether a commodity, service or brokering activity is within the jurisdiction of the International Traffic in Arms Regulations and the Arms Export Control Act,[3] while Trial Certifications involve a DOS Directorate of Defense Trade Controls commodity that reaches the stage of a trial and has an actual trial date.

Licensing agencies send responses to the ECC by mail, fax, or email. ECC personnel scan and upload the responses into EARS with the information received from licensing agencies, including the agencies' determinations on whether or not an item in question is controlled and, if so, under what authority and on the existence or histories of licenses. ECC personnel perform these tasks for both ICE and CBP EARS matters. Information about or responses to EARS referrals are also captured in the TECS system.[4] ICE agents include this information in their reports of investigation (ROIs), which are saved to the ICE case management system within TECS.[5] CBP officers include this information in the narrative section of the seizure report they file in TECS. Paper copies of the responses are most often kept in the investigation or seizure file. The responses from the licensing agencies may be used as evidence in court procedures and become part of court records.

EARS data includes contact and identification information about ICE agents, CBP officers and other ECC personnel, information pertaining to the various types of referrals described above, descriptive and technical information on export items, as well as information about suspected violators (hereafter, "Principal Party in Interest") in question.

For access to EARS, authorized personnel must first establish a user account, as well as provide identification and contact information, such as name telephone number(s), email address, and office/port location. All users access EARS through the Visual Investigation and Intelligence System (VIIS), a portal through which ICE personnel can access various investigative software applications. This system provides user profile management and requires users to read and acknowledge the rules of behavior for systems linked to VIIS, such as EARS. Once users log in to VIIS, they are able to access EARS without an additional login.

Only ICE Special Agents and CBP Officers, System Administrators, and ECC Program Managers have access to EARS. Only ECC Program Managers and the agent or officer requesting information have full read/write access to the information related to a specific referral in EARS. ICE and CBP users have a "view only" option for closed referrals that they may use to view records when conducting criminal investigations and inspections. EARS does not interface with any other information systems.

[3] Arms Export Control Act, 22 U.S.C. § 2778 (2009); International Traffic in Arms Regulations, 22 C.F.R. §§ 120 – 130 (2009).
[4] *See* DHS/CBP-011 TECS System of Records Notice, Dec. 19, 2008, 73 FR 77778.
[5] ICE's investigative case records are maintained in the TECS system, but are covered by a separate Privacy Act System of Records Notice. *See* DHS/ICE-009 External Investigations System of Records Notice, Jan. 5, 2010, 75 FR 404.

Section 1.0 Characterization of the Information

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

EARS collects and maintains PII about individuals who are the Principal Party in Interest into possible criminal violations of U.S. federal export control laws. The PII includes name, address, country of import, license type and number, and type of Principal Party in Interest. License type and number references various license classifications issued by the regulatory agencies. Each regulatory agency has different license types and its own numbering set that reference a particular type of export item. License types can refer to whether an export license is permanent or temporary, cleared for exporting classified or unclassified items or technical data, controlled substances, and other types of export items. The Principal Party in Interest type refers to whether the party is an exporter, manufacturer, or target of the investigation.

EARS also collects and maintains information about the referral including type of request, date of request, associated case number and/or CBP violation code, type of transaction, previously submitted referral number(s), item or commodity (description, technical data, specifications, photographs), destination country, regulatory agency to which the referral is directed, agency determination, determination received date, and U.S. Munitions List category (if any).

Licensing agencies that receive EARS requests send paper or email responses to the ICE ECC, which are uploaded into EARS. Depending upon the type of request, responses may include agencies' determinations on whether or not an item in question is controlled and, if so, under what authority, whether a license is required, the license numbers of existing licenses or past licenses, the U.S. Munitions List category (if applicable), and licensing officer name and title. This information is scanned by ICE ECC personnel and entered into EARS. In addition, EARS collects and maintains information about criminal or civil actions that result from the associated investigation or inquiry, including search warrant date, grand jury date, indictment date, plea date, conviction date, disbarment/sanction date and monetary penalty.

EARS collects and maintains contact information for ICE agents/CBP officers, Licensing Officers, and U.S. Attorneys involved or related to the investigation or inquiry. The collected information consists of name, title, agency, office location, office code, e-mail address, cell/pager number, office telephone and facsimile number. EARS collects and maintains user account information on ICE and CBP personnel consisting of username, name, telephone number, cell/pager number, e-mail address, office code and location and assigned user role.

Finally, EARS has the capability to produce a variety of summary reports for use by management, such as the number of requests for information submitted to licensing agencies, types of requests, and the number of requests that are pending a decision. These reports are used for internal management and statistical purposes only.

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

ICE agents and CBP officers gather information on items or commodities and suspected violators during the course of law enforcement investigations or law enforcement activities at ports of entry. Commodity information includes but is not limited to technical data, specifications, photographs of the item, and manufacturer's certification forms. This information is usually obtained directly from a manufacturer or through Internet searches by agents or officers. ICE and CBP obtain relevant information from a number of other sources, such as business records and publicly available information from the Internet, to develop sufficient knowledge of the pertinent transaction, commodity, business entity or individual. This information is used by the licensing agencies to check against their records to determine if the Principal Party in Interest has the proper license/authorization to conduct the export activity in question.

Federal licensing agencies that receive EARS referrals provide information based on their internal records on determinations on the need for licenses and information on licenses and licensing history in response to EARS referrals from ICE. Responses from the licensing agencies are scanned and uploaded into EARS by ICE ECC personnel for review by the requesting ICE agent and/or CBP officer.

EARS itself is the source of statistical reports generated by the system.

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

ICE and CBP use the information that is collected through EARS to aid investigations and inquiries into criminal violations of U.S. federal export control laws. The data entered into EARS allows agents/officers to send queries to the federal agencies that grant licenses to importers, exporters, and brokers to determine if a license if required, if a license has been granted and is valid, and to determine and verify which agency has jurisdiction over violations.

Information on license determinations and commodities that is maintained in EARS on past referrals is used by agents and officers to provide background information and prior history for current investigations and inspections.

1.4 How is the information collected?

ICE agents and CBP officers directly collect commodity and/or a Principal Party in Interest information. ICE agents and CBP officers gather information during the course of law enforcement investigations or law enforcement activities at ports of entry. Information may also be obtained from source reports, public websites regarding technical specifications of certain export items, analysis and evaluation techniques, and other law enforcement methods performed. Correspondence on referrals/requests is received from the regulatory agencies in paper form. ECC personnel scan and upload those responses into EARS.

1.5 How will the information be checked for accuracy?

As federal law enforcement officers, ICE agents and CBP officers are trained to fully check all original data sources and further investigate or inquire to resolve any anomalies that are detected. Standard operating procedures for ICE agents emphasize the importance of verifying information that is obtained during the course of an investigation. Information from a referral is provided by a federal regulatory agency.

The information that is provided to ICE by the licensing agencies in response to an EARS referral is obtained or maintained by those agencies under specific legislative authority. The original data collector is responsible for maintaining and checking the accuracy of its own data and has various means to do so.

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

The legal authorities that authorize the collection of information are the primary federal export control laws enforced by ICE and CBP, specifically the Arms Export Control Act (22 U.S.C. § 2778), the Export Administration Act (50 U.S.C. § 2410), the International Emergency Economic Powers Act (50 U.S.C. § 1701), and the Smuggling of Goods from the United States (18 U.S.C. § 554). ICE and CBP law enforcement personnel are authorized to enforce these laws pursuant to 22 C.F.R. § 127.4.

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 the information collected could be misused and or accessed by unauthorized persons.

Mitigation: The data collected and maintained in EARS is collected in the course of normal investigative and inspectional duties. Standard access controls are in place to prevent misuse of the system and only authorized ICE and CBP personnel have access. EARS system users are assigned individual user IDs and passwords and the system is only available via a DHS local area network. Management controls are in place to ensure that only complete and necessary inquiries are sent to the responsible federal regulatory agency(ies) that grant licenses.

Privacy Risk: There is a potential risk for a lack of accurate and complete information collected and maintained.

Mitigation: The ECC Program Manager must review and approve each new referral before it is submitted to the responsible licensing agency. This helps to ensure the referrals are complete and contain the necessary information. While EARS referrals support ICE investigations and CBP inquiries, they are only one component of a complete criminal investigation. ICE agents fully investigate suspected criminal violations of federal export control laws to ensure they have complete information before taking any

action against an individual or entity. Information that is used against any individual or entity in court is subject to challenge for accuracy and completeness under the rules of evidence and due process standards.

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.

ICE uses information in EARS to support efforts to determine whether an export commodity, service, or brokering activity is controlled and requires authorization from the U.S. Government licensing agencies, whether or not an authorization or export license has been granted, as well as to verify the license history of an individual or an organization. EARS information is also used to support other referrals detailed in the Overview section. These referrals assist in effectively carrying out criminal investigatory and enforcement activity aimed at addressing export-related criminal violations. A closed referral can be accessed by users as a "read only" file for use as guidance and provide assistance in continuing investigations and inspections.

ICE agents and CBP officers use EARS information to request and verify certain information about commodities/services and groups of exporters to determine if further inspection and investigation are necessary. U.S. Government licensing agencies use EARS information to retrieve and verify requested information by ICE and/or CBP and to provide agents with a determination about export items and or activity in question. Finally, the Department of Justice uses information from EARS to prosecute violations of U.S. federal export control laws.

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

The EARS system includes several methods of querying system information including: queries based on fixed fields, free-text matrix search, and statistical reports. Statistical reports are pre-defined, standardized reports that return the number of referrals submitted, referral type, to which agency the referral was submitted, and whether ICE or CBP submitted the referral. The statistical reports can identify patterns in the types of EARS referrals in process based on report counts by the various groupings listed above. These reports are used for management purposes.

The fixed-field query and free-text matrix search allows users to search for specific referrals. The fixed-field query allows users to enter specific criteria to return a set of referrals that match the criteria entered such as date, office, and referral number. An advanced search can be conducted by submitting a word, phrase, or part number into a free text field which will search all referral fields for matches. By doing this, the user can find previous referrals and utilize them as a reference or guidance in an investigation or inspection. Users must still submit a determination for their current item as laws can

change. The EARS system does not include functions for identifying further technical analysis beyond the capabilities already enumerated. EARS has no capability to do data analysis or identify non-obvious relationships.

A report can be generated and will show the number of referrals submitted, referral type, to which agency the referral was sent, and whether ICE or CBP submitted the referral.

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

The Internet is used to access publicly available information that may be available, such as specifications for commodities and services. Information regarding specifications for commodities and services, obtained on the Internet, may be uploaded into EARS. EARS does not otherwise use commercial data.

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.

EARS is hosted on a DHS-controlled network and is only available via ICE's local area network (LAN). EARS must be accessed via the VIIS platform (described in the Overview section) which features rules of behavior for all information accessible through its portal. Policies and procedures are in place to ensure that only authorized users have access to the system. User access is determined by the user's job role and duties. Use is limited to those ICE agents and CBP officers whose job responsibilities require that they have direct access to EARS to submit referrals or research referrals. Additionally, user auditing captures information about user activity that can help identify inappropriate use. These auditing measures are described further in Section 8. Any person who accesses EARS without authorization or who exceeds authorized access or use could be subject to one or more of the following: warning, fine, or loss of employment or imprisonment based on the extent of unauthorized and/or unlawful activity discovered.

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?

ICE retains primary EARS records consisting of pre-investigatory, investigatory, and judicial proceedings information regarding export items, commodities and/or licenses, and Principal Parties in Interest. ICE also retains user account management records, summary/statistical management reports, backup files, and audit files.

3.2 How long is information retained?

ICE is in the process of drafting a proposed record retention schedule for the information maintained in EARS. ICE anticipates maintaining primary EARS records for 25 years after the referral is closed (i.e., complete). In addition, ICE is proposing to retain user account management records and audit files for ten (10) years from the user's last date of employment, summary/statistical management reports for 15 years, and backup files for three (3) months.

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

No. ICE is drafting a retention schedule for EARS records that will include the proposed retention periods described above.

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: There is a risk that the information collected is retained longer than the time period needed.

Mitigation: The retention periods proposed for EARS are appropriate given the law enforcement purpose of the system. ICE and CBP need to retain these records for a sufficient period of time to allow for the data to support ongoing investigations and any criminal prosecution that may ensue, including any judicial appeals. A 25-year retention period for investigatory records is consistent with retention periods at DHS and other Federal agencies for similar records.

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?

EARS information is shared with CBP officers who work in conjunction with ICE agents to enforce U.S. federal export control laws and require access to the data in EARS to generate referrals for that purpose.

4.2 How is the information transmitted or disclosed?

CBP officers have direct access to EARS via a secure connection using the CBP Intranet.

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: There is a risk of unauthorized access to and the improper usage of EARS information.

Mitigation: User actions in the system are recorded and maintained in the audit trail in the system database. Security measures also mitigate this risk; for example, EARS data is encrypted during transfer between the CBP user's computer to the application server. Additionally, user access is based on a user's job role, proper authorization, and a need-to-know. Access to EARS is limited to authorized individuals with a need to access EARS records to perform assigned duties.

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?

EARS data is shared with various U.S. Government regulatory agencies that may be queried during the course of an ICE or CBP law enforcement activity to provide information about the licensing status of a particular commodity, service, or brokering activity. These agencies include the Department of State, Directorate of Defense Trade Controls, the Department of Commerce Bureau of Industry and Security, the Department of the Treasury's Office of Foreign Assets Control, the Nuclear Regulatory Commission and the Department of Justice ATF. These agencies receive referrals from the ECC and respond to the ECC with information that is passed forward to the requesting ICE agents and CBP officer.

Information is also provided to technical experts consisting of various scientists and engineers at the Department of Energy (DOE), including the DOE National Labs, for the purpose of conducting technical evaluations and providing technical opinions on various export items and commodities. This normally takes place during the execution of pre-trial and trial certifications as indicated in the Overview section.

Additionally, information is provided to the U.S. Department of Justice to prosecute violations of the U.S. export laws.

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 described above is compatible with the original purpose for collection, namely to support law enforcement efforts of U.S. federal export control laws by addressing export-related violations. All external sharing falls within the scope of published routine uses in DHS/ICE-009 External Investigations SORN (75 FR 404, Jan. 05, 2010), published in the *Federal Register*.

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

External organizations do not have direct access to the EARS system. Referrals are submitted electronically to regulatory/licensing agencies via e-mail or hand delivery for review as needed. E-mails containing PII are encrypted and hand deliveries occur through secure means. There are designated receivers in each agency and established protocols for transmitting and receiving information. This ensures that information is provided to the appropriate, responsible, and intended parties.

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

Privacy Risk: There is a potential risk of EARS information being misused and/or disclosed to unauthorized parties.

Mitigation: This risk is mitigated by the fact that EARS information shared with external entities is tailored to contain only information that is required by the receiving agency in order to provide ICE Agents and CBP Officers with a determination on the types of referrals described in Question 1.1. This risk is also mitigated by the fact that only ICE and CBP personnel have direct system access to EARS.

Section 6.0 Notice

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

This PIA and the External Investigations SORN serves as notice to the public of the existence of this system and the collection of this information. Given the law enforcement context in which this information is collected, affected individuals are typically not notified of the collection of their information. Applicants for export licenses may have received notice from the licensing agency at the time of the application that their information may be shared with law enforcement agencies.

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

Given the law enforcement context in which this information is collected, there is no opportunity for the individual to decline to provide information.

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

Given the law enforcement context in which this information is collected, there is no right to consent to the particular uses of the information.

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 unaware of the existence of EARS or that individuals may be unaware that their information may be maintained in this system.

Mitigation: Notice is provided by the publication of this PIA and the External Investigations SORN, which provides a detailed description of the types of information maintained and its uses. As previously noted, due to the law enforcement nature of these collections, individuals may not be provided with advance notice of the collection of their information. However, the safeguards described in this PIA pertaining to the collection, sharing and access to this data mitigate these risks.

Section 7.0 Access, Redress and Correction

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

Individuals may request access to records about them in EARS by following the procedures outlined in the External Investigations SORN. 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 EARS 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 these systems, or seeking to contest its content, may submit a request to the ICE FOIA Office. 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. Individuals may also submit requests by fax at 202-732-0310 or by email at ice-foia@dhs.gov. 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 EARS pursuant to the procedures outlined in the External Investigations SORN, 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 SORN. 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.

In addition to the procedures above, individuals seeking notification of and access to any record contained in these systems, or seeking to contest its content, may submit a request to the ICE FOIA Office. 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. Individuals may also submit requests by fax at 202-732-0310 or by email at ice-foia@dhs.gov. 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 SORN 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: There is a potential risk that an individual may be provided limited options to access and correct information about them in EARS.

Mitigation: 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. While EARS data supports ICE investigations and CBP inquiries, it is only one component of a complete criminal investigation. ICE agents fully investigate suspected criminal violations of federal export control laws to ensure they have complete information before taking any action against an individual or entity. EARS information that is used against any individual or entity in court is subject to challenge for accuracy and completeness under the rules of evidence and due process standards.

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?

EARS access must be authorized in writing by the ICE or CBP user's supervisor first and then granted by an EARS administrator designated by the ICE Section Chief who oversees both ICE and CBP requests through ECC. This process ensures that access is appropriate and related to the individual's official duties. Based on the user's role, the user's ability to view and edit information is restricted. The following user roles are applied to EARS users:

- **ICE Special Agents and CBP Officers:** These users may create new referrals and view responses from regulatory agencies entered into EARS by authorized users. This user role has the ability to view other users' submitted referrals and responses in a "read only"

mode. Users in this role may only view referrals within their area of responsibility (i.e., respective field office(s) based on user's role) and may only make edits to their own matters. The system separates these users into either ICE Special Agents or CBP Officers, but the user privileges are identical.

- **ECC Program Manager:** The ECC program manager reviews and approves each new referral before it is sent to the responsible licensing agency, and will upload responses from the agency. In this role, the user has the ability to view and edit all EARS records.
- **System Administrator:** EARS administrators prepare and process requests to access EARS and upload returned responses from the regulatory agencies. These users can view and edit all EARS records.

Although EARS administrators are able to view and edit all EARS requests, any user actions, including those made my EARS administrators are captured in the audit log in the database.

8.2 Will Department contractors have access to the system?

Yes, contractors have access to the EARS system. They are comprised of technical staff that perform system maintenance and updates/upgrades and trouble-shoot the EARS system. Contractors are required to hold security clearances in order to have access to the EARS system. Just as ICE and CBP government personnel, contractors are granted access to EARS based on their job role.

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

All ICE and CBP personnel and contractors complete annual mandatory privacy and security training and training, the Culture of Privacy Awareness and the Information Assurance Awareness Training. In addition, prior to accessing VIIS, users are required to acknowledge its rules of behavior/user agreement.

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

The Certification and Accreditation process is in progress but is expected to be completed in June 2010.

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

EARS uses database-level auditing to capture information associated with viewing, querying, adding, updating, or deleting of records in the dataset, and the user that performed the activity. EARS tracks user's logon and logoff activities, including the date and time, failed login attempts, pages

accessed, and any modifications that users make to the system. If the user attempts and fail to login to the EARS multiple times in a short period, the user's account will be permanently disabled until the user contacts an administrator or Security Control Officer (SCO) to reactivate the account.

EARS maintains an audit trail with processes that include monitoring, analysis, and reporting. Audit logs are reviewed by technical support if misuse is alleged or suspected. Additionally, EARS runs within the DHS network and is protected by DHS network firewalls. EARS can only be accessed via the DHS ICE/CBP networks. Users can access those networks via VPN connection. However, Secure Socket Layer (SSL) encryption is employed to mitigate unauthorized remote access.

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 personal information will be accessed and used inappropriately.

Mitigation: The privacy risk cited above is mitigated by the use of audit mechanisms that log and monitor user activity. Security training that discusses how to protect sensitive information also mitigates these risks. The extent of users' access is based upon users' functions and information needs to mitigate unauthorized access to and the misuse of sensitive data. Additionally, DHS has procedures in place to ensure that all information system resources, including the EARS and VIIS go through a system security certification and accreditation process that reviews security mechanisms and procedures in place, and ensures they are operating in accordance with established policies. Lastly, only ICE and CBP personnel are granted access to the EARS which allows ICE to underscore and promote essential privacy principles amongst ICE and CBP personnel, including limited use and disclosure.

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?

EARS is an operational system that is a web based application accessible via the ICE and CBP intranets.

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

The DHS ICE EIU/MO Exodus Accountability Referral 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 copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security