Privacy Impact Assessment
for the

Electronic Surveillance System (ELSUR)

November 2, 2010

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 Electronic Surveillance System (ELSUR) is owned by U.S. Immigration and Customs Enforcement (ICE), a component agency within the Department of Homeland Security (DHS). ELSUR allows ICE to track and search for ICE applications for court orders that authorize ICE to intercept oral, wire, or electronic communications during the course of a criminal investigation. ICE conducted this Privacy Impact Assessment (PIA) because ELSUR contains personally identifiable information (PII) and to publicly document the privacy protections that are in place.

Overview

ELSUR is owned by the ICE Office of Homeland Security Investigations (HSI). ELSUR allows ICE to capture and search for information included in applications for court orders authorizing ICE to intercept oral, wire, or electronic communications, such as telephone conversations and emails. These intercepts are commonly referred to as "electronic surveillance" and are always authorized by either a court order or the consent of a party to the communications.[1] Federal agency requests to perform electronic surveillance are governed by Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"). Title III established specific protocols and standards for the issuance of a federal court order authorizing electronic surveillance during the course of a federal criminal investigation.[2]

ICE requests court orders to conduct electronic surveillance during the course of ICE criminal investigations. When ICE is engaged in joint investigations with state or municipal law enforcement agencies, ICE agents may also support requests filed with state courts for electronic surveillance under the applicable state's electronic surveillance laws. These requests will be captured in ELSUR as well. ELSUR tracks these federal and state electronic surveillance requests whether or not they are granted by the court. ELSUR also supports the sharing of this information within ICE and with other federal investigative agencies as required by Title III.

With the publication of this PIA, ICE is modernizing the ELSUR system by replacing the existing system with a new, web-based system. The new ELSUR system is scheduled to be deployed in early 2011. Once deployed, ICE will migrate data from the previous version of ELSUR and retire the legacy system.

Title III Requirements Generally

Electronic surveillance is a search under the Fourth Amendment to the U.S. Constitution, therefore the government must obtain a warrant based on probable cause or the consent of at least one of the parties to the communication. Title III requires federal investigative agencies, including ICE, to obtain judicial authorization to conduct real-time interception of "oral, wire, or electronic communications" during the course of a criminal investigation. Under Title III, the term "electronic communications" is defined broadly and includes voice, e-mail, fax, and Internet communications. Title

[1] ELSUR only captures information about electronic surveillance requested by court order, not consensual intercepts.
[2] 18 U.S.C. §§ 2510-22.

III establishes procedures agencies must follow to obtain a federal court order to authorize electronic surveillance (known as a Title III order) and regulates how law enforcement agents can use and further disclose information obtained under a Title III order. All federal agency requests for Title III orders are presented to the U.S. Attorney's Office for approval and ultimately submitted to a federal judge for decision.

To request a Title III order, an application package is prepared by the investigating agency and the local U.S. Attorney's Office in the federal judicial district in which the order will be sought. The application package consists of an affidavit prepared by the federal agent(s), the contents of which are sworn to under oath, an application, and a proposed court order authorizing the intercept. The affidavit and application describe the probable cause that exists to believe that the target device is being used to facilitate illegal activity, explain that the requested interception is necessary to support the investigation, and address other requirements outlined in Title III.[3]

The Title III affidavit must: (1) identify the specific federal crimes for which probable cause exists; (2) contain a particular description of the nature and location of the facilities or place from which the interception is to occur; (3) identify specifically the persons involved in committing the offenses and whose communications are to be intercepted ("subjects"); and (4) describe the type of communication to be intercepted such as cell phones, voice mail, pagers, faxes, email, computer transmissions, etc. The Title III affidavit also must describe all previous Title III requests (including those made by other federal law enforcement agencies) pertaining to any of the same named subjects, target devices, locations/facilities, vehicles, or things (shipping container, etc.). The affidavit must disclose any such requests even if the court did not authorize the intercept. To satisfy this last requirement, federal agents must be able to search previous Title III requests made by their own agency and other federal investigative agencies. Accordingly, federal investigative agencies have established databases – such as ICE's ELSUR system – to make the process of searching previous Title III requests easier and more efficient.

Occasionally, when ICE conducts a joint investigation with a state or municipal law enforcement agency, an ICE agent participating in the investigation may support that agency's request for electronic surveillance made under applicable state laws.[4] In such cases, the ICE agent executes an affidavit in support of the electronic surveillance request, which then becomes part of the application filed with the state court. State electronic surveillance requests are handled by the local prosecutor's office, not the U.S. Attorney's Office. The specific procedures and requirements for these requests vary by state. ICE includes in ELSUR any state law requests which ICE supports so they can be searched and reported in future Title III affidavits filed by ICE.

[3] The "target device" is the specific communication device that is the target of the intercept. For example, a target device could be an email address, telephone, cell phone, pager, fax machine, or Voice Over Internet Protocol (VOIP) address.

[4] For example, the State of California's electronic surveillance law is defined by the California Penal Code, Title 15, Chapter 1.4.

ELSUR

The purpose of ELSUR is to store and search electronically all previous ICE Title III requests and ICE-sponsored state requests described above (collectively, "electronic surveillance requests") to support the preparation of new Title III requests by ICE and other federal agencies conducting criminal investigations. ELSUR maintains information about subjects, target devices, locations, vehicles, and things named in previous electronic surveillance requests, regardless whether the request was approved or denied by the court.

Data is input into ELSUR by personnel at the HSI Technical Operations Unit (TechOps Unit) at ICE Headquarters, who receive information about electronic surveillance requests from ICE field agents. The data captured in ELSUR includes information about the subject, target device, location, vehicle or thing that was the target of the electronic surveillance request; whether the request was approved; the duration of the approved intercept; court order number, judge's name, and date/time order was signed; court and judicial district; whether it was a joint case and with what agency; prosecutor/Assistant U.S. Attorney's name; and the name of the ICE agent signing the affidavit. By policy HSI field offices are required to forward copies of electronic surveillance requests within 48 hours of approval or denial by the judge to the TechOps Unit, whose personnel manually enter the data into ELSUR.

The TechOps Unit staff run queries in ELSUR (also known as an "ELSUR check") when they receive a request from an ICE agent or other federal agent who is preparing to file a new Title III request. The ELSUR check request contains basic information, such as the subject and target device, about the new Title III request being prepared, TechOps Unit staff use this information to query ELSUR for any possible matching records. The TechOps Unit provides the requesting agent the results of the check, and if any matches are identified, also provides an ELSUR Title III Report produced by the ELSUR system containing information about the matching electronic surveillance request(s).

During the course of a criminal investigation, an ICE agent prepares a new Title III request and submits an ELSUR check using the "Request for Indices Checks for Prior Applications of ELSUR Activity Form" via fax or email to the TechOps Unit. The agent requests to be informed of all previous electronic surveillance requests on the same subject/vehicle/device/location/thing that is the proposed target in the current Title III request. TechOps Unit personnel then search ELSUR to identify previous ICE electronic surveillance requests for the same subject/place/device/location/thing. If the ICE ELSUR check reveals a positive match, the TechOps Unit generates an ELSUR Title III Report in ELSUR that identifies the date the court order was signed approving or denying the intercept; duration of the intercept if approved; judicial district and judge; and the specific subject of the intercept.

In addition to searching ELSUR, the TechOps Unit transmits the ELSUR check form via fax to other federal law enforcement investigative agencies such as the Federal Bureau of Investigation (FBI) and Drug Enforcement Agency (DEA) to request that they identify all previous Title III requests on the same target, and to notify the TechOps Unit of the results of the search. If checks by the other federal agencies reveal a positive match, then those agencies provide the TechOps Unit with a similar Title III Report providing the same information. TechOps personnel send the ELSUR Title III Reports via fax or e-mail to the requesting ICE agent and his office. If no matching records are found, then a copy of the request form with "NR" (i.e., No Response) written on it is sent to the requesting ICE agent and his

office. Possible matches on subjects that cannot be ruled out using other identifiers (such as a date of birth) are sent to the requesting office and agent for resolution.

The ICE agent includes any positive results of the ELSUR check in the affidavit and submits it to the local U.S. Attorney's Office. An Assistant U.S. Attorney then prepares the Title III application and drafts a proposed court order authorizing the intercept for presentation to a federal judge. The ICE agent submits a copy of the affidavit to the TechOps Unit, which tracks all affidavits to ensure field agents provide copies of the electronic surveillance requests/orders once the judge has made a decision. Once the U.S. Attorney's Office approves the application package, the Assistant U.S. Attorney and ICE agent appear before a federal judge to present the request. The agent swears to the contents of the affidavit in front of the judge and signs it, and the Assistant U.S. Attorney signs the application in the presence of the judge. If the judge approves the Title III request, he/she will sign a court order to that effect for 30 days. Regardless whether the judge approves or denies the Title III request, the ICE agent sends either a copy of the Title III order or the denied request and the application package (includes the affidavit and application) to the TechOps Unit, which enters information from these documents into the ELSUR system, and then retains the information in a hard copy file at the TechOps facility.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

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

ELSUR collects, uses, and maintains information pertaining to requests for court orders authorizing intercepts of oral, wire, or electronic communications (electronic surveillance) during the course of a criminal investigation conducted by ICE, or a joint investigation conducted by ICE and another federal, state, or municipal law enforcement agency.[5] These electronic surveillance requests may be made in federal court under Title III or in state courts under applicable state electronic surveillance laws. ELSUR captures information about all such electronic surveillance requests, regardless of the outcome.

Electronic surveillance requests target a person (i.e., "subject"), device (such as a cell phone), location, vehicle, or thing. ELSUR stores the following information about the target of the Title III request:

- Subject: subject name, date of birth, social security number (SSN), address information, phone number, email address, and alias(es).

[5] The system also maintains information about Title III applications and orders made by ICE's legacy agencies, the U.S. Customs Service (USCS) and the U.S. Immigration and Naturalization Service (INS).

- Device: type of device (cell phone, pager, etc.), device identification number, device phone number, international mobile subscriber identity (IMSI), urban fleet mobile identifier (UFMI) (push to talk code), email address, IP address, electronic serial number (ESN), manufacturer identification number (MID), international mobile equipment identifier (IMEI), subscriber's address.
- Location (business, residence, or other): business name, resident or owner's name, and address of the named subjects.
- Vehicle: registration information, owner's name and address, vehicle make, vehicle model, vehicle color, vehicle year, and vehicle serial number.
- Thing or Object (could be a shipping container, box, etc.): description and address if applicable.

ELSUR also contains information about the electronic surveillance request and any order issued by the court, such as the court order number, judge's name, whether the request was approved or denied, date/time order was signed, court or judicial district, state, country, if it was a joint case and with what agency, the Assistant U.S. Attorney's last name, duration of approved intercept, and the name of the ICE agent that signed the affidavit.

Requests from other law enforcement investigative agencies and from ICE field agents for ELSUR checks contain identifying information about the proposed subject, device, location, vehicle and/or thing (as described above) of the Title III request. Information about the requesting agent is not input into the ELSUR system, nor does the system maintain an electronic copy of the ELSUR check request form. For ELSUR checks where a record is found, ICE will retain a hard copy of the Title III report sent to the requestor (e.g., DEA, FBI) in a file by the requesting agency's name. ICE does not have a Title III report if a record is not found. ICE will send the ELSUR check form back to the requesting agency with a note stating no records were found and destroy the form. ELSUR creates ELSUR Title III Reports when an ELSUR check reveals a potential match. ELSUR Title III Reports contain the subjects, devices, locations, vehicles, or things named in any previous electronic surveillance requests, whether the request was granted or denied, the dates and location of the intercept (if approved), and the judge's name and judicial district. The ELSUR Title III Report states that on (date) Judge of (District) approved a court order for 30 days allowing the interception of (target description). ELSUR also enables users to generate aggregate reports by HSI Field Office and case categories.

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

Information contained in the ELSUR system is obtained from federal and state electronic surveillance requests and orders. ICE agents provide the application package and any order issued by the state or federal judge to the TechOps Unit for manual entry into ELSUR. The information about the targets of these electronic surveillance requests is obtained by ICE agents through the course of their criminal investigations, and from other federal, state and municipal law enforcement agencies that may be assisting or joining in the investigation. Agents may obtain this information from witnesses, victims, confidential informants, public and business records, and other sources. Typically, information is not

collected directly from the individual who is the subject of the electronic surveillance request because the effectiveness of the electronic surveillance depends on the individual remaining unaware of the intercept.

ICE receives information used to conduct ELSUR checks from ICE field agents and from other federal investigative agencies. ELSUR is the source of the ELSUR Title III Reports described in Question 1.1 above.

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

ELSUR collects and maintains this information to allow ICE to identify previous requests for electronic surveillance when ICE or other federal agencies are preparing new Title III applications during criminal investigations. Title III requires federal agencies that are seeking a court order authorizing electronic surveillance to search their own records of previous Title III requests and those of other agencies that may have investigated those same subjects in the past. Any previous applications for electronic surveillance of the same proposed target (i.e., subject, vehicle, device, location, thing) are to be identified and reported to the judge in the Title III application. To comply with this requirement, ICE and other federal agencies that conduct criminal investigations created "electronic surveillance indices" like ELSUR to allow for electronic searches of previous Title III requests.

1.4 How is the information collected?

ICE agents collect information about individuals in the course of criminal investigations of federal customs, immigration, and other criminal laws enforced by ICE. If an ICE agent decides to seek court authorization to conduct electronic surveillance of an oral, wire, or electronic communication, he or she prepares the supporting affidavit and includes any relevant information from the investigative case file. This information is obtained using law enforcement investigative techniques, tools, and authorities, such as witness interviews, subpoenas, records checks, and search warrants. Once the court grants or denies the electronic surveillance request, the ICE agent sends a copy of the request, including the affidavit and court order, by fax or e-mail to the TechOps Unit at ICE Headquarters. TechOps Unit personnel manually enter the relevant information (described in Question 1.1 above) into ELSUR, and store the Title III request and court order in a secure area.

Requests for ELSUR checks received from ICE agents and other federal investigative agencies are sent to ICE's TechOps Unit by fax or via email. Information from the requests is not retained within ELSUR, but is used to query ELSUR for possible matching targets from previous electronic surveillance requests.

1.5 How will the information be checked for accuracy?

ELSUR information is input into the system directly from an ICE Title III application package presented to a federal or state court judge. These documents contain information the accuracy of which must be sworn to under oath by the presenting government officials (the ICE agent and Assistant U.S. Attorney). Because the presentation of inaccurate information to the court can carry serious

consequences, wherever possible these officials verify the accuracy of this information through appropriate investigative means (e.g., subpoena to obtain business records, verification through multiple sources).

To minimize data entry errors, information keyed into the ELSUR system is reviewed against the court order or the affidavit by the TechOps Unit personnel entering the data. ICE agents in the TechOps Unit periodically review data entered into ELSUR to verify it was entered accurately.

When an ELSUR check is conducted by searching on a person's name, the system identifies matches on the results screen and produces the ELSUR Title III Report. The TechOps Unit will review the matches produced by the system and use additional details, such as date of birth and SSN, to verify the validity of the match. The TechOps Unit provides the ELSUR Title III Report to the requesting agent containing any verified or possible matches. Negative matches are not provided. If no verified or possible matches are identified, a negative response is noted on the requestor's form and returned to the requesting agent. It is the responsibility of the requesting agency to determine whether the report of a positive or possible match is an actual match of their target.

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

Title III refers to the federal laws (18 U.S.C. §§ 2510-2522) that regulate the non-consensual interception of oral, wire, and electronic communications. Title III requires that a federal agency's request for authorization to perform electronic surveillance be made in writing and under oath and that the request establish probable cause for the search. The application must reveal all previous surveillance requests and must be submitted to the U.S. Attorney's Office for approval. To respond to inquiries concerning previous ICE Title III requests from ICE agents and other law enforcement officers, ICE must maintain a database of the information which will be queried upon request by another federal criminal investigating agency. ICE is authorized by 19 U.S.C. § 1589a to investigate all federal crimes and by 8 U.S.C. § 1357 to investigate immigration-related crimes. These authorities likewise authorize ICE to collect information in the course of the investigation of such crimes. Such collection may include the interception of oral, wire and electronic communications in accordance with Title III.

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 privacy risk of collecting more information than is necessary to accomplish the purposes of the Title III ELSUR check.

Mitigation: ELSUR collects only a limited amount of information about subjects of criminal investigations and other named individuals in the Title III request. The collection of information is narrowly tailored to allow agencies to identify actual and possible matches to current targets of proposed Title III intercepts. The limited scope of information collected mitigates the risk information that is not

necessary to the conduct of successful ELSUR checks will be maintained or used for improper or unrelated purposes.

Privacy Risk: ELSUR could present a risk of unauthorized access to sensitive PII.

Mitigation: ELSUR access is limited to TechOps Unit personnel only. The information is not stored or managed by any other field office, agency, or outside entity. Any law enforcement officer who needs information stored in ELSUR must submit an ELSUR check request. This manual process along with the limited number of system users mitigates the risk that unauthorized persons will access or improperly use the sensitive PII contained in ELSUR.

Privacy Risk: There is a privacy risk that information about a particular subject or target could be inaccurately input into ELSUR.

Mitigation: This risk is mitigated by ELSUR users reviewing information keyed into ELSUR against the court order or the affidavit. Additionally, ICE agents in the TechOps Unit periodically review data entered into ELSUR to verify it was entered accurately, and make any necessary corrections.

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.

ELSUR is used to identify and share information about prior ICE electronic surveillance requests with requesting ICE agents and other federal agents that are preparing a Title III request to intercept the same target. Information from the Title III requests and orders is used to electronically search and identify actual and possible matches when an ELSUR check is conducted. This information is also used to generate the ELSUR Title III Reports, which are provided to the agency requesting the ELSUR check. The information in the ELSUR Title III Reports is used by federal agents in the Title III affidavit to inform the court of previous requests on the same target, as required by law.

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

ELSUR conducts electronic searches for targets that are an exact or close match to a search query input by the user. The searches identify matches to names, phone numbers, addresses, and other target information provided by the agent requesting the ELSUR check. ELSUR permits users to generate an ELSUR Title III Report when the ELSUR system returns a positive or possible match result. The ELSUR Title III Report includes information about persons whose names match the name provided in the ELSUR check request and are identified as a possible match. The ELSUR Title III Report identifies the date, duration, district, and judge who authorized or denied the intercept of the person, place, or thing. The specific target of the intercept is also identified. ELSUR also enables users to generate aggregate reports by HSI Field Office, and/or case category identifying the number of intercepts conducted.

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

The system does not use commercial or publicly available 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.

Privacy Risk: There is a privacy risk of unauthorized access to data maintained in ELSUR.

Mitigation: ICE mitigates this risk by implementing role-based user access. Only authorized personnel or contractors assigned to the ICE TechOps Unit have direct access to the system and system use is audited. Personnel who have ELSUR access must have a current ICE background check and complete annual privacy and security training. Personnel outside the TechOps Unit may only access information in ELSUR by submitting the appropriate form to request an ELSUR check, and the information shared with those individuals is limited to the information provided in the ELSUR Title III Reports generated by the system. Only federal agents conducting criminal investigations are authorized to submit ELSUR check requests, and typically must do so through their agency's ELSUR Unit, which reduces the risk that an unauthorized or fabricated request will be sent to ICE.

Section 3.0 Retention

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

3.1 What information is retained?

All information about ICE electronic surveillance requests and orders entered into ELSUR is retained in the system. The paper copy of the electronic surveillance requests and orders received by the ICE TechOps Unit for input into ELSUR are maintained in a secure room in the TechOps Unit's facilities. The audit trail for system activity recording all activity by specific users is also retained. ICE maintains hard copies of ELSUR Title III Reports generated by the system. Finally, ICE maintains paper copies of requests from ICE agents and other federal agents for ELSUR checks.

3.2 How long is information retained?

ICE proposes to retain information in the ELSUR system for fifty (50) years from the date of the court order authorizing the intercept of oral, wire, or electronic communications or 50 years after closure of the related case file, whichever is later. ICE proposes to retain paper copies of ICE's electronic surveillance requests and Title III court orders for the same 50 year period.

ICE proposes that requests for ELSUR checks be destroyed once the ELSUR check is completed. All hard copy "Request for Indices Checks for Prior Applications of ELSUR Activity" forms will be shredded. Any requests received electronically will be deleted after the request is completed.

ICE proposes to retain ELSUR Title III Reports in hard copy for five (5) years from the date returned to the requesting investigative agent, after which time ICE will shred them. Once the ELSUR Title III Report is run and printed by the user, the system automatically deletes it from its cache.

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

No. ICE is preparing a retention schedule for the records described above for NARA approval.

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 privacy risk that information will be retained for longer than is needed to accomplish the purpose for which the information was originally collected.

Mitigation: The information in ELSUR is retained for the timeframes outlined in Question 3.2 to ensure application information is available to ICE to facilitate ELSUR checks in accordance with Title III. This retention period is consistent with law enforcement system retention schedules generally and appropriate in length given ICE's law enforcement mission.

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?

ICE shares ELSUR data upon request with U.S. Secret Service (USSS) agents that submit an ELSUR check request during the preparation of their own Title III electronic surveillance request. Within DHS, only USSS agents and ICE agents have the authority to request Title III authorization to conduct a court authorized intercept. ICE shares ELSUR information in the form of an ELSUR Title III Report or no-match result with the USSS to fulfill the statutory requirement to report all previous requests for electronic surveillance to the court.

4.2 How is the information transmitted or disclosed?

ICE shares the ELSUR Title III Report or a no-match result with the USSS by fax or email. ICE shares this information with the USSS electronic surveillance unit, which then notifies the requesting USSS agent either verbally or via email.

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

Privacy Risk: A risk is presented that information may be shared with DHS components without a need to know.

Mitigation: The risks posed by the sharing of this information are mitigated because ICE will only share ELSUR information with the USSS's electronic surveillance unit for USSS agents who are seeking the information to comply with federal law in connection with a Title III request. These agents have a need to know this information so that they can include it in their affidavits as required by Title III.

Section 5.0 External Sharing and Disclosure

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

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

ICE is required to share the results of ELSUR checks with other federal investigative agencies to support those agencies' preparation of their own Title III requests. ICE routinely shares information in the form of ELSUR Title III Reports with other federal agencies that have the authority to seek Title III orders in support of criminal investigations, such as the FBI and DEA. ICE discloses ELSUR information only as necessary to allow those agencies to fulfill their statutory requirement to report to the court all previous requests for electronic surveillance requests and orders on the same target(s).

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.

Yes. The sharing described above is compatible with the original purpose for collection, which is to maintain a searchable index of all electronic surveillance requests and orders in support of ICE criminal

investigations. All external sharing falls within the scope of published routine uses in the DHS/ICE-009 External Investigations SORN (75 FR 404, January 5, 2010). In addition, the disclosure of ELSUR information to other federal investigative agencies is required under Title III.

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

ICE shares the ELSUR Title III Report, or a no-match result, with other federal investigative agencies by fax or an encrypted email. Typically ICE shares this information with the requesting agency's own electronic surveillance unit, who then notifies the requesting agent either verbally or via email.

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 privacy risk that ELSUR information may be shared with agencies outside of DHS that do not have a need to know.

Mitigation: Information in ELSUR is shared only with federal law enforcement agencies that have the authority to seek Title III orders and a need for the results of ICE's ELSUR checks in order to meet Title III requirements. The process ICE and other agencies have established for conducting ELSUR checks ensures that agencies who do not have a mission to investigate criminal activity will not be able to access this information.

Section 6.0 Notice

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

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

No. The individuals that are the subjects of ICE's electronic surveillance requests are not notified of the application or the court's decision prior to the intercept of oral, wire and electronic communications (if approved). The court order and/or the application remain under seal until unsealed as determined by the issuing judge. The effectiveness of the electronic surveillance as a tool in criminal investigations typically depends on the target remaining unaware of the agency's investigative interest in him or her, and of the Title III application/order. Individuals who are aware of the agency's investigative interest and ability to intercept their communications are likely to change their behavior to avoid detection. For example, if an individual that was the subject of a criminal investigation became aware that ICE had obtained a Title III order authorizing the interception of his cell phone communications, he would likely stop using that phone to conduct any illegal activities.

Per Title III, ICE is required to notify the subject of the electronic surveillance no later than ninety (90) days after denial of the Title III request or the termination of the electronic surveillance (or extensions thereof as approved by the issuing judge), unless notification is postponed by the issuing judge (e.g., due to an ongoing investigation or current court proceeding).[6]

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

No. In all cases, because of the criminal law enforcement purpose for which the information is collected, opportunities for the individual to decline to provide information are nonexistent. Title III intercepts are nonconsensual by statute.

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

No. Because of the criminal law enforcement purpose for which the information is collected, opportunities for the individual to decline to provide information are nonexistent. Title III intercepts are non-consensual by statute.

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 individuals may be unaware that their information is collected and processed by ELSUR.

Mitigation: The risk is mitigated by the publication of this PIA and the External Investigations SORN. In most cases, notice is not given due to the law enforcement nature of the collections. Additional notice or the opportunity to consent to use of the information would compromise the underlying law enforcement purpose of the system and may put the success of pending criminal investigations at risk. Additionally, notice of the Title III request and/or approved court order is required by law to be provided to the subject of the electronic surveillance no later than ninety (90) days after denial of the Title III request or the termination of the electronic surveillance (or extensions thereof as approved by the issuing judge), unless notification is postponed by the issuing judge (e.g., due to an ongoing investigation or current court proceeding).

Section 7.0 Access, Redress and Correction

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

[6] *See* 18 U.S.C. § 2518(8)(d).

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

Individuals may request access to records about them in ELSUR 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 ELSUR could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension.

In addition to the procedures above, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the ICE FOIA Office. Please contact the ICE FOIA Office at (866) 633-1182 or see the ICE FOIA Office's website for additional information (http://www.ice.gov/foia). If an individual believes more than on 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, SW, Building 410, STOP-0550, Washington, DC 20528.

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

If individuals obtain access to the information in ELSUR 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 this system of records, or seeking to contest its content, may submit a request in writing to the ICE FOIA Office. Please contact the ICE FOIA Office at (866) 633-1182 or see the ICE FOIA Office's website for additional information (http://www.ice.gov/foia). If an individual believes more than on 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, SW, Building 410, STOP-0550, Washington, DC 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 re-dress available to individuals and how those risks are mitigated.

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

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

Section 8.0 Technical Access and Security

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

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

Access to the ELSUR system will be limited to authorized personnel assigned to the ICE TechOps Unit with a need to know as determined by the Unit Chief, and whose job duties include the input or searching of ELSUR information. The TechOps Unit Chief will be responsible for approval of all requests for ELSUR user accounts. Access to the system is restricted using an authentication process including the use of usernames and passwords.

User roles govern the rights and permissions granted to each user. Menu options vary depending on the user role. The table below lists the classes of users who interact with the system.

User Role	Description
User	Query and view ELSUR records and generate reports.
Record Keeper	Query and view ELSUR records, enter and modify data, and generate reports.

User Role	Description
Administrator	Query and view all ELSUR records, enter and modify data. Delete records and add, modify, or delete users from the system. Assign and re-set passwords.

8.2 Will Department contractors have access to the system?

Yes, ICE contractors who have undergone a background check and signed the DHS Rules of Behavior may be assigned to run ELSUR checks, enter information into the system, perform system maintenance operations, and conduct IT development work on the system.

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

All ICE personnel and contractors complete annual mandatory privacy and security training, specifically the Culture of Privacy Awareness Training and the Information Assurance Awareness Training. Additionally, informal ELSUR application training is provided to users on the job, which includes guidance on appropriate uses of the system as well as issues relating to data accuracy.

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

The Certification and Accreditation is expected to be completed by February 2011.

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

ELSUR will use database-level auditing to capture information associated with any viewing, insertion, updating, or deletion of records in the dataset, and the user that performed the activity. The ELSUR application-specific audit trail provides adequately detailed information to facilitate reconstruction of events if a compromise or malfunction occurs. The audit trail is protected from actions such as unauthorized access, modification, and destruction that would negate its forensic value. TechOps reviews audit trails when there is an indication of system misuse to ensure users are accessing and updating records according to their job function and responsibilities.

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

ICE also has a process in place for investigating and responding to suspicious activities on the system. That process includes automated tools to assist the administrators in their monitoring, analysis, and reporting. The process is consistently followed. Information suggesting misuse of the system is

referred to the appropriate office and any individuals suspected of misuse are subject to investigation, disciplinary action, or removal in accordance with ICE policy.

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: The privacy risks to this system are primarily the risks of unauthorized system access or use and inadequate system security.

Mitigation: Both risks have been mitigated by following DHS and government-wide security protocols that establish controls appropriate for this type of sensitive data. As described above and elsewhere in this PIA, those controls include user access controls, auditing, intrusion detection software, and user training.

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?

ELSUR is an information technology system that supports ICE's compliance with statutory requirements imposed by Title III.

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

ELSUR is in the development phase of the system lifecycle.

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

No.

Responsible Officials

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

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security