Privacy Impact Assessment
for the

287(g) Program Database

December 28, 2009

Contact Point
William Riley
Office of State and Local Coordination
U.S. Immigration and Customs Enforcement
(202) 732-5050

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

Abstract

The U.S. Immigration and Customs Enforcement (ICE) Office of State and Local Coordination maintains a database for the 287(g) Program, under which ICE delegates Federal immigration enforcement authorities to state and local law enforcement agencies. The database is used to track the progress of delegation agreements between ICE and state and local law enforcement agencies and the vetting and training of individual state and local law enforcement officers who are candidates for 287(g) authority. ICE is conducting this Privacy Impact Assessment (PIA) because the 287(g) Program database collects, uses, and maintains personally identifiable information (PII).

Overview

The ICE Office of State and Local Coordination (OSLC) maintains the 287(g) Program database in support of the ICE 287(g) Program. The 287(g) Program operates under the authority of section 287(g) of the Immigration and Nationality Act (INA), which authorizes ICE to delegate Federal immigration enforcement authorities to state and local law enforcement agencies. Under the Program, ICE enters into agreements with state and local law enforcement agencies to delegate to the agencies' law enforcement officers the authority to enforce certain federal immigration laws. Law enforcement officers who receive this delegated authority may by question and detain individuals for potential removal from the United States based on their immigration status.

OSLC created the database to track the progress of written agreements between ICE and state and local law enforcement agencies (LEAs). LEAs that are interested in participating in the 287(g) Program contact ICE to request 287(g) authority. Once ICE determines that it would be beneficial and appropriate to delegate 287(g) authority to the LEA, ICE negotiates a written agreement with the LEA delegating the 287(g) authority and defining the LEA's responsibilities regarding the use of the authority and its handling of information pertaining to suspected violations of Federal law.

Once 287(g) authority is granted to a state or local law enforcement agency, the database is used to track the vetting and training of individual state and local law enforcement officers who are candidates for 287(g) authority. The LEA nominates specific law enforcement officers as candidates to receive the 287(g) authority. The candidates complete and submit to ICE OSLC a Federal background check form (which collects extensive biographic, educational, employment, criminal and civil action, and mental health information). The LEA also completes and submits a 287(g) Candidate Questionnaire for each nominated candidate (which collects information about the candidate's eligibility, suitability, authority, and previous misconduct and/or criminal history). OSLC forwards the hard copy of the candidate's background check form and 287(g) Candidate Questionnaire to the ICE Office of Professional Responsibility (OPR), which vets the candidates to determine their suitability to serve as a 287(g) officer. ICE OPR notifies the OSLC which candidates have a criminal history and which candidates were successfully vetted.

All 287(g) candidates will undergo the same vetting process as ICE personnel. The vetting process is covered under the Department of Homeland Security Personnel Security Management System of Records (DHS/ALL-023 SORN, 74 FR 3084).

Once the candidates have been successfully vetted, they receive training from ICE personnel on the Federal laws and regulations they will be authorized to enforce and their appropriate implementation. The candidate's performance during training is assessed to ensure they can effectively and appropriately use the 287(g) authority. Once a candidate is successfully vetted and successfully completes training, the candidate is officially delegated the 287(g) authority and receives an ICE law enforcement credential.

Information Maintained in the Database

The 287(g) database contains official contact information for each candidate, biographical and identifying information about each candidate, and rosters of training classes (itemized in Section 1.1). It also contains the outcome of the vetting process, whether the candidate has a criminal history, and whether the individual passed the required 287(g) training. The 287(g) database may also contain details about the candidate's criminal history such as the charges filed against the individual, the outcome of the case, and any relevant mitigating factors.

The 287(g) database also maintains various categories of non-personal information such as agreements between OSLC and LEAs, arrest statistics for the LEAs (extracted from ICE's Enforcement Integrated Database (EID) but not associated with specific 287(g) officers), and communications between OSLC Program Managers and the LEAs.

The 287(g) database is also capable of producing several reports that document, for example, the status of various 287(g) agreements and the performance of various LEAs (such as the number of criminal aliens identified and removed as a result of the 287(g) Program). The only reports that include personal information are the lists of candidates nominated by each LEA and the list of candidates assigned to a particular training session. The reports do not include sensitive information such as the candidate's Social Security number (SSN), date of birth, or criminal history.

Typical Transaction

After having signed a 287(g) agreement with ICE, the local LEA identifies candidates among their officers for 287(g) delegation, and sends hard copies of the required background check forms and 287(g) Candidate Questionnaire to the OSLC. OSLC creates records in the 287(g) database for each candidate, and enters their names, basic contact information, SSNs, and dates of birth. OSLC sends the hard copies of their federal background check forms and 287(g) Candidate Questionnaire to ICE OPR, which performs background checks on the individuals. OPR will notify OSLC by email if the candidates have criminal histories, and provide details of the arrests or convictions, which OSLC will note in the candidate record in the 287(g) database. OSLC will also note in the candidate records whether the candidates have passed their background checks, once OSLC is notified by OPR. Once the individual candidates have successfully passed the background check and completed the required training, their status is set to "active" in the 287(g) database.

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?

The database collects and maintains information about state and local law enforcement officers that have been nominated to serve as 287(g) officers by state and local LEAs that participate in the 287(g) Program. This includes current and former 287(g) officers, and pending and unsuccessful candidates for 287(g) status. The 287(g) database contains the candidate's name, official contact information, state/local badge number, ICE-issued credential badge number, SSN, and date of birth. The 287(g) database contains a field that reflects the status and result of the background check process ("active" for candidates who have been successfully vetted; "inactive" for candidates who were either not judged suitable for 287(g) authority or who have not yet completed the vetting process). The 287(g) database also contains a field that reflects the result of the training process ("passed" for candidates who successfully complete training; "failed" for candidates who did not successfully complete training; and "withdraw" for candidates who withdrew prior to completing the training).

The database contains a field indicating whether or not the candidate has a criminal history ("positive" for individuals with a criminal history; "negative" for individuals with no criminal history; or blank for individuals who have not yet been vetted) as well as a free text field for additional comments. The comment field may contain a reference to the case numbers of any associated criminal conduct, a brief description of the charges alleged, a brief summary of the outcome of the criminal proceedings against the candidate, and other details such as mitigating factors. Candidates also submit information on a form to OSLC (including name, address, SSN, and bank account information) to allow for the electronic transfer of funds to the candidate's bank account for purposes of payment of travel reimbursements. None of this financial information is entered into the 287(g) database and it is retained only in the candidate's paper file.

The 287(g) database also contains official contact information for LEA points of contact and ICE Field Office points of contact (e.g., a responsible Special Agent in Charge or Field Office Director), rosters of training classes, as well as non-personal information described in the overview.

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

The names of 287(g) candidates are provided by LEAs who are participating in the 287(g) Program. The candidates themselves complete and submit the Standard Form 85P, "Questionnaire for Public Trust Positions," which provides extensive biographic, educational, employment, criminal and civil action, and mental health information. Of all of the information in the SF-85P, however, only the candidate's SSN, date of birth, and official contact information are stored in the database. The LEAs complete and submit a 287(g) Candidate Questionnaire on each candidate, which provides documentation

of eligibility, suitability, misconduct and criminal history issues that the LEA is aware of. None of the information on the 287(g) Candidate Questionnaire is stored in the database. ICE OPR provides information on the results of the vetting process, including whether the individual has a criminal history, details about the alleged criminal offense, and the result of the vetting process. ICE training managers provide information on the results of the 287(g) training process.

The system also includes arrest statistics for each state and local agency participating in the 287(g) Program which are obtained from ICE's EID system. This information is not associated with any particular 287(g) officer, but rather is associated only with a specific participating LEA.

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

The database directly supports the ICE's need to operate the 287(g) Program, specifically to negotiate and track agreements with LEAs to participate in the program; to track the results of 287(g) agreements in the form of arrests made; and to identify, train, vet, and delegate authority to 287(g) officers. Using the database, ICE can quickly compile a list of candidates assigned to a particular training session, or determine whether a particular candidate has been successfully vetted. This improves the consistency, efficiency, and effectiveness of ICE's 287(g) Program.

Arrest statistics from the ICE EID system are needed to track law enforcement activities of participating LEAs. For example, OSLC is frequently asked to report statistical trends and analysis on the implementation of the 287(g) Program. In particular, reports are required on the law enforcement activities (encounters, apprehensions, deportations, etc.) performed by specific LEAs. Without the original contact information on the LEA and its respective officers, the Program has no way of accurately capturing activity levels with regard to the execution of 287(g) delegation of authority.

1.4 How is the information collected?

ICE collects candidate information using the SF-85P (OMB Control Number 3206-0191) and the 287(g) Candidate Questionnaire (currently undergoing PRA approval), which is completed by individual candidates from state and local LEAs that participate in the 287(g) Program. ICE may collect additional information from 287(g) candidates for the purpose of completing the vetting and suitability determination. The SF-85P and the 287(g) Candidate Questionnaire are mailed to OSLC along with two completed fingerprint cards (FD-254).

All 287(g) officer arrests and other activity data is extracted from ICE's IIDS Data Mart, which is populated with data from EID. This data is extracted from EID using a script that automatically de-identifies the performance of individual officers, while maintaining the performance of each participating state or local LEA. This data is then formatted into an MS Excel document, and imported into the 287(g) database. This process involves no manual data entry.

1.5 How will the information be checked for accuracy?

Biographic information about the 287(g) candidates is obtained either directly from the candidate or their employer (the LEA), and is therefore deemed to be highly reliable. Other information in the system, such as details regarding the candidate's criminal history and the result of the vetting, is obtained from other sources including federal databases such as the FBI's Integrated Automated Fingerprint Identification System (IAFIS), which provides a fingerprint-based criminal history records check. Individuals have the opportunity to request their own IAFIS criminal history record and to seek corrections if the criminal history information is inaccurate.

Arrest data extracted from EID is presumed to be correct because it is the official ICE system in which arrests by ICE personnel and 287(g) officers are documented. Arresting agents and officers enter information about arrestees directly into the EID application and use biometric-based record checks to verify identity information.

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

The Immigration and Nationality Act (INA) provides legal authority for the entire 287(g) Program within the OSLC. Section 287(g) (effective September 30, 1996) was added through the Illegal Immigration Reform and Immigrant Responsibility Act (IIRAIRA).

In order to capture required data from the LEAs and the respective 287(g) officers, the OSLC enters into a legally binding Memorandum of Agreement (MOA) with each LEA. The MOA is signed by the Assistant Secretary of ICE as well as the LEA authority.

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: The 287(g) database could present a risk of the over-collection of PII.

Mitigation: ICE collects only a limited amount of information about 287(g) candidates necessary to track, vet, and train them. All PII collected is necessary to the purpose of ensuring the candidates are suitable for a delegation of authority, to manage information about 287(g) officers, and to provide training to candidates. The limited scope of information collected and maintained ensures that the risk of over-collection is mitigated.

Privacy Risk: The collection and maintenance of the SSN presents an increased risk of identity theft if that information is compromised.

Mitigation: The 287(g) database limits access to candidate and officer SSNs to only those database users who have a need for that information in the course of their 287(g) Program job responsibilities. Because the sole purpose for including the SSN in the database is to enroll candidates in 287(g) training courses (for which the SSN is required), access to the SSN is limited to those users who

have a training manager user role. This technological control mitigates the risk that unauthorized persons can access the SSN for improper uses.

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.

Originally developed as a temporary data repository for the 287(g) Program, the database evolved into the primary source of information for the Program and its staff members. Use of the PII maintained in the database is limited to ICE internal purposes only and the data is not used by any groups external to ICE.

The PII in the system is only used for the purpose of administering the 287(g) Program. For example, class rosters are maintained to track who is enrolled in each training session. Candidate SSNs and dates of birth are maintained for identification purposes. Candidate SSNs are also used to facilitate the candidate's enrollment in law enforcement training courses at the DHS Federal Law Enforcement Training Center (FLETC), which requires the SSN for enrollment. Candidate dates of birth are used by ICE to book passenger air reservations to FLETC, which now require date of birth under the Secure Flight program.

The 287(g) database uses other non-personal information for a variety of purposes, including the tracking of the progress of negotiations for each 287(g) agreement; the calculation of arrest statistics for each participating LEA; and the recording of notes of communications between ICE and the LEAs on various matters pertaining to the 287(g) Program. The database also provides OSLC management and ICE executives with statistical reports such as the arrest statistics, numbers of 287(g) officers trained, and 287(g) agreement status.

Internal to the OSLC, the database reports are used to analyze process times for 287(g) agreements, status of 287(g) officers in the vetting process prior to training and several other ad hoc requirements such as a comparison between fiscal years of 287(g) officers trained in a specific region.

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

The database does not include any analytical tools. The database produces basic reports that show the performance of specific LEAs (but not specific officers). The database also produces reports on the status of requests for 287(g) authority and the status of 287(g) agreements.

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.

For both the tracking and reporting functions of the 287(g) database, appropriate training is given prior to access by users. Separate training material has been prepared for regular system users, training managers, program managers and the administrator. Each set is prepared based upon the access available to each user and their role in the 287(g) database. In addition, all database users complete mandatory ICE annual privacy and security training, which stresses the importance of appropriate and authorized use of personal data in government systems. Individuals who are found to have accessed or used the 287(g) database data in an unauthorized manner will be disciplined in accordance with ICE policy.

Also, users of the 287(g) database are assigned access roles that are pre-designated by their position and their supervisor. This ensures that users are only granted access to that information they need to perform their function. The system administrator is able to access and change all fields in the database, but the OSLC only allows three administrators to exist at any given time. These controls ensure that information is handled in accordance with the above-described uses.

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 data stored in the 287(g) database will be retained. This data includes everything noted in Question 1.1 as well as search queries written to pull reports, the reports themselves, and any correspondence documented between ICE and the LEA partners participating in the 287(g) Program.

3.2 How long is information retained?

ICE proposes to retain the records of 287(g) Officers in the database for five (5) years once the records are changed to "inactive" status. Other electronic records in the database and associated paper records, such as search queries, reports, and correspondence and agreements between ICE and the LEA partners, are also retained for five (5) years.

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

No. ICE has drafted a proposed records retention schedule for the 287(g) Program that contains the retention periods proposed in Question 3.2.

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 287(g) Program has decided to maintain records in the database for the limited duration of five years once the records are changed to "inactive" status. This preserves records for a sufficient time in case they are necessary after an officer becomes inactive, but also ensures that they don't persist in a way that unnecessarily increases the risk of their misuse or disclosure. The 287(g) Program uses a variety of technical controls to protect data while it is maintained in the system, as described in Section 8.

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?

There is no sharing within DHS of personal information stored in the 287(g) database.

4.2 How is the information transmitted or disclosed?

There is no sharing within DHS of personal information stored in the 287(g) database.

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.

No privacy risks have been identified as the personal information stored in the database is not shared within DHS.

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?

Personal information from the 287(g) database is not shared with any external organizations. However, OSLC does acknowledge that a judicial order can certainly be placed on data within the database and ICE would disclose information as necessary to support any investigations or litigation that may involve information in the database.

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.

PII from the 287(g) database is not shared with any external organizations. The DHS Personnel Security Management System of Records Notice (SORN) DHS/ALL-023 (74 FR 3084, January 16, 2008) and the DHS General Training Records SORN DHS/ALL-003 (73 FR 71656, November 25, 2008) cover the PII collected and maintained in the database. These SORNs are being republished to clarify the nature of the information they maintain relating to the 287(g) Program.

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

PII from the 287(g) database is not shared with any external organizations.

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

No privacy risks have been identified as the information is not disclosed outside of DHS.

Section 6.0 Notice

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

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

Yes. The SF-85P form completed by the officer candidates includes a Privacy Act Statement that provides notice of the collection of the information for the purpose of conducting vetting. This PIA also provides public notice of the collection of information, as do the SORNs referenced in Question 5.2 above.

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

A 287(g) candidate can decline to provide their information at any point in this process. However, if they decline, they cannot be properly vetted or trained and ICE will not delegate authority to them as a 287(g) officer. Refusal to complete the required forms results in non-participation by that officer in the 287(g) Program.

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. Individuals do not have the option to provide for particular uses of their information. ICE will use their information for the purposes described in this PIA and the DHS Personnel Security Management and DHS General Training Records SORNs.

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: There is a risk that individuals are not aware of the existence of the 287(g) database and the data it maintains.

Mitigation: Individual candidates for the 287(g) Program submit the SF-85P, which includes relevant privacy notice to individuals regarding the data they provide. Further, this PIA serves as public notice of the existence of the 287(g) database.

Section 7.0 Access, Redress and Correction

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

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

Individuals may request access to records about them in the 287(g) database by following the procedures outlined in the DHS Personnel Security Management SORN and the DHS General Training Records SORN.

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:

ICE FOIA Officer
800 North Capitol Street, N.W.
5th Floor, Suite 585
Washington, D.C. 20528

Individuals may also submit requests by fax at 202-732-0310 or by email at ice-foia@dhs.gov. Please see the ICE FOIA Office's website for additional information (http://www.ice.gov/foia/index.htm). 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 the 287(g) database pursuant to the procedures outlined in the DHS Personnel Security Management SORN and the DHS General Training Records 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 DHS Personnel Security Management SORN and the DHS General Training Records SORN.

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:

ICE FOIA Officer
800 North Capitol Street, N.W.
5th Floor, Suite 585
Washington, D.C. 20528

Individuals may also submit requests by fax at 202-732-0310 or by email at ice-foia@dhs.gov. Please see the ICE FOIA Office's website for additional information (http://www.ice.gov/foia/index.htm). 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 DHS Personnel Security Management SORN and the DHS General Training Records 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 are risks of a lack of access to information and inability to seek redress and correction.

Mitigation: 287(g) candidates may access and correct information about themselves by contacting the 287(g) Program through their 287(g) contact or through the FOIA process. These procedures are adequate to address the individual's right to access and correct their records.

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?

The OSLC Program Manager must approve requests for ICE personnel to become users of the database. Once approved, the database Administrator creates a profile based on the anticipated role of the user. Once the profile is created, the Administrator conducts training with the user, leaving also a training slide presentation with snapshots and high-level guidance regarding reports and queries available. After the user successfully completes the required training, the user's account is activated and he or she can then begin using the system. Only ICE personnel are permitted to have user access to the database.

The following describes user roles and privileges for the 287(g) database:

- OSLC User – Read-only access to the database. OSLC users cannot edit information contained in the database and cannot view or edit SSNs in the database.
- Training Manager – Same privileges as the OSLC user, except the Training Manager also has privileges to view and update SSNs in the system.

- Program Manager – Read/write access on the entire database, except cannot view or edit SSNs. Limited reporting capabilities.
- Administrator – Read/write/delete/add access to the entire database including SSNs.

8.2 Will Department contractors have access to the system?

ICE contractors have access to the 287(g) database. Their main role is to run reports and extract data from the database, providing statistics to the OSLC Section Chiefs and Program Managers. Secondary to this function is the maintenance of the database. OSLC contractor support is responsible for making any changes to the data tables, report designs and any other enhancements required by the OSLC management. These personnel undergo an extensive clearance process before being granted physical access to the facility as well as login information for the ICE Network. Also, the OSLC Contracting Officer's Technical Representative assigned to this contract gives prior written approval for any personnel coming on board. Contractors are tasked with any enhancements to the system as well as the technical, design, and administrative documentation required to maintain the system within ICE OCIO guidelines.

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 and training on Securely Handling ICE Sensitive but Unclassified (SBU)/For Official Use Only (FOUO) Information. The 287(g) database training includes the high level of sensitivity regarding the PII, its handling, use, and penalties. In addition, all ICE employees must read and sign a Rules of Behavior agreement when logging on to the ICE Network, which governs user activity and includes guidelines for the protection of sensitive information.

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

The 287(g) database certification is expected to be completed by July, 2010.

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

The 287(g) database captures information associated with viewing, inserting, updating, or deleting of records in the dataset, and the user that performed the activity. The 287(g) database's audit trail provides adequately detailed information to facilitate reconstruction of events if compromise or malfunction occurs. The audit trail is protected from actions such as unauthorized access, modification and destruction that would negate its forensic value. OSLC will review audit trails when there is indication of system misuse.

The 287(g) database restricts access to all privileged functions and security-relevant information to explicitly authorized personnel. The system enforces the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks. Users without a specific need to see SSNs stored in the 287(g) database cannot view or edit that information.

The 287(g) database sits on the OSLC Shared Drive on a protected folder within the ICE Network. ICE has a process in place for investigating and responding to suspicious activities on its network. That process includes automated tools to assist the administrators in their monitoring, analysis, and reporting. The process is consistently followed. The database runs within the DHS network and is protected by DHS network firewalls.

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, 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?

The 287(g) database is an operational project. It is in use on a daily basis within the OSLC and assists the OSLC management with tracking and reporting.

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

The 287(g) database is in the Operations and Maintenance stage of the ICE System Development Life Cycle (Enterprise Architecture, OCIO).

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