Privacy Impact Assessment
for the

Federal Protective Service Dispatch and Incident Record Management Systems

September 16, 2009

Contact Point
Gary Schenkel
Director, Federal Protective Service
U.S. Immigration and Customs Enforcement
(202) 732-8000

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

Abstract

This Privacy Impact Assessment (PIA) describes U.S. Immigration and Customs Enforcement's Federal Protective Service (FPS) Dispatch Operations Log, Web Record Management System, and Dictaphone Police Report Recorder, collectively referred to as the FPS Dispatch and Incident Record Management Systems. FPS uses these systems to track the daily activities of its officers and to perform case management for the offenses and incidents that occur in and around the Federal facilities that FPS secures. ICE is conducting this PIA because these systems collect personally identifying information (PII) about members of the public.

Overview

FPS owns and operates three systems that support the communication and reporting of daily activities, incidents, and offenses in and around Federal buildings and facilities protected by FPS: (1) the Dispatch Operations Log, (2) Web Record Management System (WebRMS), and (3) the Dictaphone Police Report Recorder. FPS is an operational component within U.S. Immigration and Customs Enforcement (ICE) that provides law enforcement and security services to more than 8,800 Federal facilities nationwide. The FPS mission is to render Federal properties safe and secure for Federal employees, officials, and visitors in a professional and cost effective manner by deploying a highly trained and multi-disciplined police force.

FPS carries out a variety of responsibilities in support of this mission, such as providing contract security guard services, crime prevention seminars, facility security surveys, operational and law enforcement support for special events, and conducting investigations into suspected criminal activity, including threats against employees, visitors or Federal property. To perform these activities, FPS employs Security Officers (i.e., contract guards), FPS Officers, and Criminal Investigators. The FPS Officers manage and supervise the Security Officers who primarily staff the security check points of the Federal facilities. The Criminal Investigators investigate serious crimes committed in and around Federal facilities.

Nationwide FPS field operations are coordinated through centralized command and control facilities called MegaCenters, which report to FPS Headquarters in Washington, D.C. FPS operates four MegaCenters that service the eleven regional FPS offices around the United States. Each MegaCenter has its own General Support System, which consists of a mission specific application network, an office automation network, a radio network and a video network. The General Support System allows the MegaCenters to provide regional alarm monitoring, dispatching, and criminal investigations reporting for the Federal facilities in their assigned areas.

While on duty, FPS Officers and Security Officers use hand-held radios or telephones to report a range of daily activities to MegaCenter Dispatchers in real time. As the information is received from the officers, the Dispatchers enter it into the MegaCenter's Dispatch Operations Log (DOL), an application that creates a continuous, chronological log for the facilities in its region. Typical DOL entries include reports of officers coming on or going off duty, reports of an individual officer's location at a given time,

and all offenses and incidents reported during a shift. Incidents include occurrences such as an alarm activation at a facility, reports of lost property, and injuries occurring on the premises. Offenses include civil and criminal violations of law against employees, visitors, and Federal property, such as theft, threats, assault and vandalism.

The DOL entries contain any PII reported by officers in the field to the MegaCenter relevant to the reported event or occurrence. For example, a DOL entry about a slip and fall on Federal property may contain the name of the injured individual and whether he or she was transported to the hospital. DOL entries about offenses may include personal information about witnesses, victims and suspects. Each DOL resides on the respective MegaCenter's General Support System and is not linked to any system outside of the MegaCenter.

When FPS Officers and Security Officers report an event that is an incident or offense, they are also required to create a separate report in the FPS nationwide incident/offense reporting system known as WebRMS. To do so, they request a WebRMS case control number (CCN) from the MegaCenter Dispatchers at the time they report the offense/incident for recording into DOL. The Dispatcher creates the WebRMS case record for that particular offense/incident, obtains the DOL-generated CCN, and provides the CCN to the reporting officer in the field. The officers are then responsible for completing a more detailed report of the incident/offense in WebRMS. WebRMS has specific data fields that must be completed as well as a narrative field in which the officers can provide general information and a description of what occurred. FPS Officers complete the report by logging into WebRMS. FPS Security Officers do not have WebRMS accounts and cannot enter their reports directly into the system, so they complete them telephonically using the MegaCenter's Dictaphone Police Report Recorder (DRR). Using the CCN provided by the Dispatcher, the FPS Security Officers follow prompts over the telephone and dictate their report into DRR, which records the information. Later, MegaCenter personnel retrieve and transcribe the dictated reports and manually enter the information into the appropriate WebRMS record. FPS supervisors review all WebRMS records for accuracy, situational awareness and follow-up, if necessary.

WebRMS incident/offense reports are updated if there is an investigation or additional information about the incident/offense is received. All reports are ultimately either closed or referred for investigation to FPS Criminal Investigators or local law enforcement authorities. WebRMS and DRR do not reside on the MegaCenters' General Support Systems, and they are not linked to any systems outside of FPS.

If the Social Security number (SSN) is collected from an individual (SSNs are always collected if there is an arrest), it is used to identify the individual and to perform record checks in Federal government law enforcement information systems such as the National Crime Information Center (NCIC).

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?

These systems collect information about individuals who are the subject of routine reporting by FPS Officers and Security Officers concerning incidents and offenses in Federal facilities protected by FPS. These individuals are typically persons believed to be involved in or related to a particular incident or offense, such as suspects, victims, witnesses, participants, employees, and building occupants and visitors. The type of information collected about these individuals varies depending on the type of incident or offense that occurred, but basic identifying information (such as name and contact information) is usually collected at a minimum. Where relevant, other information may also be collected such as citizenship, sex, age, race, weight, eye color, hair color, scars, marks, tattoos, employer, NCIC number, driver's license number, aliases, and Social Security number.

If the Social Security number is collected from an individual (SSNs are always collected if there is an arrest), it is used to identify the individual and to perform record checks in Federal government law enforcement information systems such as NCIC.

Contextual information about the individual in relationship to the particular incident or offense may also be collected, some of which may be sensitive. For example, for persons injured in a slip and fall, the systems may record the type of injury suffered (e.g., broken leg) and the details of the event itself. For criminal activity, the systems may reflect the relationship of the individual to the crime (e.g., victim, witness, suspect), the nature and details of the crime (e.g., assault), and any personal property that was damaged or stolen.

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

The reporting FPS Officer or Security Officer typically collects information directly from the individuals involved in the incident or offense. Information may also be collected from Federal, state, or local police officers who also respond to or assist with the incident or offense. If an investigation of an offense is initiated, the FPS Officer may perform a query in the FBI's NCIC and enter the NCIC record number for the individual and associated information into the WebRMS records.

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

The information is being collected to serve as an official record of FPS field activities, and reports of incidents and offenses in Federal buildings protected by FPS. Information in DOL is collected

in real-time from the responding officer to make a record of the daily events that occur in or around Federal facilities secured by FPS, and to allow for the dispatching of additional resources as needed to respond to incidents or offenses. The specific information collected is necessary to provide an adequate record of FPS activities, which may be relied upon later to perform an investigation or to recreate the circumstances of a particular event. This information may also be used to document the appropriateness of FPS activities in the event of an inquiry or investigation. The information is also used to generate statistical reports for facility, regional, and nationwide incidents and offenses at FPS-protected facilities.

1.4 How is the information collected?

FPS Officers and Security Officers radio or telephone the MegaCenter Dispatcher to report daily activity data for entry into DOL.

Information about incidents and offenses is usually collected during interviews by the FPS responding officer(s) directly from the individuals involved, e.g., victims, suspects and witnesses. FPS Officers enter their incident and offense reports directly into WebRMS. FPS Security Officers use a telephone to access the DRR, where they log in by typing a user ID and password into the phone keypad. The DRR prompts the Security Officer to dictate specific information for the incident or offense report and records his or her oral responses. The officer's oral report is retrieved by FPS Dispatchers at the MegaCenter and transcribed into the WebRMS record.

1.5 How will the information be checked for accuracy?

The information collected may be verified by the inspection of identification or other documents, or during any subsequent investigation which may take place. Information may also be verified through information maintained by other law enforcement agencies (e.g., NCIC results) in the event of an associated investigation of the offense or incident. FPS supervisors review all submitted reports for accuracy, situational awareness and follow-up if necessary.

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

The authority to collect this information is 40 U.S.C. § 1315, "Law Enforcement Authority of Secretary of Homeland Security for Protection of Public Property."

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

There is a risk that the information collected may not be accurate or timely because it is not always collected directly from the individual to whom it pertains. For example, information about the person accused of committing a criminal act could be provided by victims and witnesses. As with all law enforcement activities or investigations, there is also the risk that individuals may misrepresent

information about themselves or others in an effort to frustrate law enforcement investigations or for other reasons. To mitigate these risks, FPS investigations and other enforcement activities seek to collect and compare sufficient relevant information to ensure that any information relied upon to take actions that may affect individuals is accurate and complete to the greatest extent possible. In addition, FPS follows written standard investigatory procedures and appropriately documents the sources of its information so that the credibility and reliability of the source can be considered when evaluating the information provided.

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 the information in DOL to allow regional FPS command staff to stay apprised of activities in their areas of responsibility. This information may also be used by FPS command staff during an event, incident or offense to help dispatch additional resources to a particular location.

ICE uses the information in DRR and WebRMS to identify the alleged suspects, victims, witnesses or other persons pertinent to an incident or offense, and to describe details of the incident/offense itself. This information is used to perform necessary follow-up actions such as an investigation, to track the rate of incidents and offenses at Federal facilities, and to inform FPS staffing and security decisions. Reports from WebRMS are also used to provide FPS, ICE, and DHS Headquarters staff with information about incidents/offenses occurring nationally in or around Federal buildings.

If the Social Security number is collected (SSNs are always collected if there is an arrest), it is used to identify the individual and to perform record checks in Federal government law enforcement information systems such as NCIC. The NCIC Number is recorded to reflect that a record was found in response to an NCIC query.

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

Several standard management reports are programmed into WebRMS that provide Headquarters FPS, ICE, and DHS staff with statistical information about offenses or incidents occurring nationally in or around Federal buildings.

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

The systems described in this PIA do 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.

Information security awareness and privacy training courses are required for all FPS employees and contractors who have access to ICE systems and use these applications. In addition, the DHS Rules of Behavior govern the actions of individual system users that utilize government IT systems within the agency. Users are required to sign and acknowledge the Rules of Behavior before access is granted to these FPS systems.

Audits and security monitoring are performed to ensure the security of these FPS systems. The workstations, servers and other computing equipment that support DOL and WebRMS are contained in areas that have appropriate physical access controls. Physical access to the FPS data centers is controlled by a badge proximity reader. Physical access to WebRMS workstations are protected by Federal security officers and proximity badge readers. Access controls are layered with access permitted only to the area the employee or contractor is authorized to enter.

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 described in Question 1.1 above is retained in the WebRMS and DOL application databases.

3.2 How long is information retained?

The data in DOL will be retained for seven (7) years. ICE will retain the oral recordings in DRR until the recording is deleted by a MegaCenter Dispatcher upon retrieval and transcription, usually within 12 hours. The data in WebRMS will be retained for 25 years after the date of the incident or offense, or after the completion of any associated law enforcement action and/or judicial proceedings, whichever is later.

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

No. ICE is in the process of drafting a record retention schedule for the information described in this PIA.

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

The risk associated with the data retention is unauthorized or malicious access or retaining longer than is necessary. The information in DOL, DRR, and WebRMS is retained for a period of time appropriate for their respective purposes. For example, the DRR data is retained for a very limited period of time because it is a temporary record that is created only to allow its transcription to a more formal recordkeeping system. WebRMS maintains data for an appropriate length of time given its law enforcement purpose, and the retention period of 25 year is consistent with retention periods for other law enforcement systems. The DOL data is maintained for a shorter period (seven years) because the offense/incident data is also recorded in WebRMS.

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?

The information is not shared with other parts of DHS except on an ad hoc basis with other DHS law enforcement organizations for law enforcement investigatory, evidentiary, or prosecutorial purposes, or for civil proceedings.

4.2 How is the information transmitted or disclosed?

When information is shared, it is shared in the form of paper printouts only. Paper reports are delivered in a secure manner consistent with the handling of any law enforcement sensitive material.

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.

The privacy risks are that the information will be lost, stolen or compromised. However, information is not generally shared internally with other DHS components, except as needed to facilitate law enforcement investigatory, evidentiary, or prosecutorial purposes. In those instances, information is shared via hard copy printouts that are hand delivered to and signed for by authorized personnel, or registered mail, thereby reducing the privacy risks associated with transmitting sensitive personal information.

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?

The information is not shared outside of DHS except on an ad hoc basis with other non-DHS law enforcement organizations for law enforcement investigatory, evidentiary, or prosecutorial purposes, or for civil proceedings. Recipient agencies can include the U.S. Department of Justice, the Federal Bureau of Investigation, and State and local law enforcement agencies.

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.

External sharing is consistent with original collection of information, specifically the reporting of incidents and offenses so that they may be further investigated or prosecuted. The SORN that covers this information is the Law Enforcement Authority in Support of the Protection of Property Owned or Occupied by the Federal Government[1] DHS/ALL-025 (74 FR 3088, Jan. 16, 2009), which has routine uses allowing FPS to share the information for law enforcement and criminal and civil litigation purposes.

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

The information is shared only through hard copy printouts. The information is transmitted by secure means only, such as hand delivery with signature by the receiving agency employee, or by facsimile or registered mail.

[1] For additional information regarding the Law Enforcement Authority in Support of the Protection of Property Owned or Occupied by the Federal Government (DHS/ALL-025, 74 FR 3088, January 16, 2009) visit www.dhs.gov/privacy.

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

The external sharing of information described above is consistent with the law enforcement and security purposes for which the information was collected. ICE has appropriate measures in place to secure the information during transit and to validate the information's accuracy before ICE takes any action that is adverse to an individual. ICE shares ICE-generated law enforcement reports only with law enforcement organizations that have demonstrated a need-to-know the information in the course of their official duties. DHS-mandated security and privacy training also mitigate the risk that FPS users will share or handle sensitive information improperly.

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?

The publication of this PIA and the Law Enforcement Authority in Support of the Protection of Property Owned or Occupied by the Federal Government SORN (DHS/ALL-025, January 16, 2008, 74 FR 3088) provide general public notice of the collection of this information. Individuals are also generally aware when being interviewed by an FPS officer that their information is being collected by FPS for the purpose of documenting and/or investigating an incident or offense. Formal written notice is not provided to individuals at the point of collection of this information because of the law enforcement context in which it is collected. In some instances, providing notice to individuals whose information is being collected would interfere with FPS's ability to carry out its law enforcement mission by potentially frustrating the confidential nature of its investigations, methods, or sources. Notice is provided to the individual when the information is collected directly from the individual during or after arrest through the reading of Miranda rights. When information is obtained through witnesses, no specific form of notice is provided.

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

The information individuals provide to FPS during an incident or offense is generally provided on a voluntary basis. However, individuals suspected to have committed a crime or offense may be required to provide information pertaining to their identity. Individuals may decline to provide further information by exercising their Fifth Amendment rights against self-incrimination under the U.S. Constitution.

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

Depending on the nature of the investigation, FPS officers may ask persons if they wish to consent to particular uses of the information they provide – for example, individuals who request to provide information to FPS confidentially will be advised the extent to which their identity may be protected under applicable laws. Generally, however, because these FPS systems are used for law enforcement purposes, the opportunity to consent to use of the information is not provided as it would compromise the underlying law enforcement purpose of the system and may put pending investigations at risk.

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.

Since most of the information contained in these FPS systems is collected directly from the individual, they have actual notice concerning what information is being collected and why. Furthermore, the risk that individuals may not be aware that their information may be contained within these systems is mitigated by the public notice provided through this PIA and the applicable SORN.

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 these FPS systems by following the procedures outlined in the Law Enforcement Authority in Support of the Protection of Property Owned or Occupied by the Federal Government SORN (DHS/ALL-025, January 16, 2008, 74 FR 3088). 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 these systems 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.

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the component's FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "contacts." If an individual believes

more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0550, Washington, D.C. 20528.

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

If individuals obtain access to the information in these FPS systems pursuant to the procedures outlined in the Law Enforcement Authority in Support of the Protection of Property Owned or Occupied by the Federal Government 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 Law Enforcement Authority in Support of the Protection of Property Owned or Occupied by the Federal Government 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.

Individuals seeking to contest the systems' content may submit a request in writing to the component's FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "contacts." If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0550, Washington, D.C. 20528.

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

The procedure for submitting a request to correct information is outlined in the Law Enforcement Authority in Support of the Protection of Property Owned or Occupied by the Federal Government 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?

If an individual is not satisfied with the response to an access or correction request, he or she can appeal to the appropriate authority provided for in the FOIA process. The individual will be informed how to file an appeal if and when a request is denied.

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

Individuals can request access to information about them through the FOIA process and may also request that their information be corrected. The law enforcement nature of the information contained in

DOL and WebRMS is such that the ability of individuals to access or correct their information may be limited. However, outcomes are not predetermined and each request for access or correction is individually evaluated.

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?

Each FPS user must be approved by their direct supervisor and the system owner to access the systems. A request form is completed and forwarded to the system owner. Once approved, the system administrators create a userID and temporary password for a user. In addition, the user is assigned a role, which governs the user's access rights as described in the paragraph below.

Access to these systems is predetermined by the individual's job title. FPS Officers have access to WebRMS, but can only edit a limited number of fields. The MegaCenter Dispatchers also have access to WebRMS and can enter data into the remaining WebRMS fields. Only the FPS MegaCenter Dispatchers and FPS command staff have access to DOL, and Dispatchers also have access to DRR to retrieve recorded reports. FPS Security Officers have access to the DRR but do not have direct access to either WebRMS or DOL.

8.2 Will Department contractors have access to the system?

Yes. DHS contractors serving as Dispatchers in the MegaCenters may have access to these systems. In addition, DHS contractors who serve as FPS Security Officers have access to the DRR. The contractors are trained and cleared based upon the same standards as DHS employees.

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. Each government employee and contractor must be read and accept the DHS rules of behavior before being allowed access.

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

Yes. Certification and Accreditation is complete for these systems and each system received an Authority to Operate (ATO): FPS's four MegaCenter GSS systems (on which the DOL application resides) received ATO on October 10, 2007, and WebRMS received its ATO on May 31, 2007.

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

The safeguards and auditing measures described below are essentially the same for the MegaCenters GSS and WebRMS. All technical safeguards comply with DHS Information Technology security standards set forth in DHS Directive 4300A.

Safeguards include technical controls such as Identification and Authentication. Technical controls provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. Each user is authenticated before access is permitted. Each user must be approved and have a properly adjudicated background investigation prior to being granted access. The system administrator creates a userID and temporary password for a user and assigns a role approved by the system owner, which governs the user's access rights. Users are required to change the password the first time they access the system, and every 90 days thereafter. UserIDs are unique to an individual and group userIDs are not permitted. A user has up to three attempts to logon. After the third unsuccessful attempt, the application automatically locks out the userID until the password administrator unlocks and resets it.

Individual accountability is tracked through the association of a userID with the actions the user performs in the MegaCenter application. The application does not permit a user to bypass the user authentication requirements.

Logical Access Controls are built into the hardware and software features. Only authorized users have access to or within the GSS or WebRMS application and are restricted to particular transactions and functions using the concept of "least privilege" whereby users are only granted access to that which they need to perform their duties. User accounts are linked to the appropriate access control list (ACL) once the request for access has been approved. Access is restricted by the ACL to the lowest level needed for the users to do their jobs. Access rights are strictly controlled by application roles and MegaCenter GSS controls.

Audit trails assist in ensuring user accountability. MegaCenter audit trails have been implemented using application audit tables in the MegaCenter database. Audit trails include transaction history, recording the identity of individuals (userID) who view, edit or delete records, and the date timestamp of the transaction. They also track successful and unsuccessful logon attempts and successful and unsuccessful attempts to access modules within the GSS and WebRMS applications.

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?

The system presents a risk that individuals who are not authorized may gain access to the data. This risk is mitigated through the use of access controls such as the MegaCenter GSS and WebRMS access control list. Access to the data is also restricted to the lowest level needed for users to perform their job function. In addition, security logs are monitored regularly to detect any instance of unauthorized transaction attempts. Additional security controls are in place such as an audit trail of invalid login attempts, SSL encryption between server and client Web browsers, and SHA-1 hashing on passwords that are stored in the database.

User activity is individually tracked through the association of a user with their userID and password. Audit trails within the application and database create a transaction history, recording the identity of individuals (userID) who edit or delete documents as well as the date of the action. Users who are found to violate the rules of behavior are subject to disciplinary action and/or revocation of access privileges to these and other sensitive data systems.

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 General Support System consist of a mission specific application network, an office automation network, a radio network and a video network, with DOL as the main sub-system/application containing information about the general public. WebRMS is an application designed to capture law enforcement incident and offense information.

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

GSS and WebRMS are in the Operation/Maintenance phase of the system lifecycle. Maintenance to the system is performed periodically and tracked by the Change Management process.

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

This system does not employ technology that may raise privacy concerns.

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