Privacy Impact Assessment Update
for the

Federal Protective Service Dispatch and Incident Record Management Systems

DHS/NPPD/PIA-010(b)

March 25, 2014

Contact Point
Eric L. Patterson
Director, Federal Protective Service
National Protection and Programs Directorate
(202) 732-8000

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS), National Protection and Programs Directorate (NPPD), Federal Protective Service (FPS) owns and operates a suite of systems, collectively referred to as the Dispatch and Incident Record Management Systems. These systems track the daily activities of FPS officers and perform case management for the incidents that occur in and around the federal facilities that FPS secures. This update to the PIA provides additional transparency into how FPS uses its case management data, to include using U.S. Customs and Border Protection's TECS system as an investigative case management tool and incorporating limited FPS case management data into the DHS Pattern Information Collaboration Sharing System (DPICS2).

Overview

The Federal Protective Service (FPS) is an operational component of the Department of Homeland Security (DHS), National Protection and Programs Directorate (NPPD) whose 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-disciplinary police force. FPS carries out a variety of responsibilities in support of this mission, such as providing contract enforcement support for special events and conducting investigations into criminal activity, including threats against employees, visitors, or federal property.

FPS owns and operates a suite of systems used to support nationwide incident reporting whereby federal employees, contractors, and visitors may report suspicious activity, security-related matters, and alleged violations of law related to the protection of federal facilities. This suite of systems is collectively referred to as the FPS Dispatch and Incident Record Management Systems. The original PIA, published in September 2009, outlines the three main systems FPS uses to track the daily activities of its officers and to perform case management for the incidents that occur in and around the federal facilities that FPS secures. In March 2012, an update to the PIA added a fourth system to the suite of systems and covered the transition from a paper-based system to an electronic system for retaining information FPS officers collect during field interviews.

The full suite of systems in the FPS Dispatch and Incident Record Management Systems includes the following:

1. FPS Dispatch Operations Log – an application that creates a continuous, chronological log of reports of daily activities.
2. Web Record Management System (WebRMS) – the nationwide incident reporting system, which serves as a central repository for all case management data.

3. Dictaphone Police Recorder – a system allowing FPS Protective Security Officers, without direct access to WebRMS, to record information telephonically.

4. Field Interview Report database – an electronic database of data captured from field interviews conducted during the course of a preliminary investigation.

This update to the PIA provides further transparency into how data is used as part of the investigative case management process and how data is shared in order to enhance coordination of incident response and appropriately respond to threats and criminal activity occurring in or around federal facilities. Specifically, this update addresses two additional systems that FPS uses to manage or share its case management data, which are owned and operated by other components of DHS. These two systems are detailed below:

(1) TECS, a modified version of the former Treasury Enforcement Communications System, principally owned and managed by U.S. Customs and Border Protection (CBP),[1] as an investigative case management tool; and

(2) DPICS2, a system owned and managed by U.S. Immigration and Customs Enforcement (ICE), whose purpose is to facilitate sharing with internal and external law enforcement partners.[2] FPS exports limited case information from WebRMS into DPICS2.

The scope of this PIA Update is limited to FPS and its use of TECS and DPICS2. DHS has published separate PIAs to cover other uses of the TECS and DPICS2 systems.

Investigative Case Management via TECS

Every day FPS protects the homeland by managing risk and ensuring continuity for one of the most crucial elements of our national critical infrastructure –our nation's federal facilities and their occupants. FPS ensures federal building protection by detecting, disrupting, and investigating threats using law enforcement authorities. FPS uses a system owned and managed by CBP, known as the TECS system, as its primary investigative case management system.

FPS is one of several users of TECS and uses the TECS Case Management (CM) module to maintain investigative activities around federal buildings, relevant to criminal investigations. FPS uses TECS CM to manage criminal investigations of alleged violations of law and to have access to investigative records/data entered by FPS law enforcement personnel during the course of an investigation. Additionally, CM is the method FPS employs for criminal investigation

[1] *See* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing, December 22, 2010, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs.pdf. See DHS/CBP-011 - U.S. Customs and Border Protection TECS, December 19, 2008, 73 FR 77778.

[2] DPICS2 was formerly known as the ICE Pattern Analysis and Information Collection (ICEPIC) system. DPICS2 is covered by the privacy documentation published for ICEPIC, including the DHS/ICE/PIA-004 ICEPIC PIA, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_icepic.pdf, and subsequent updates, and the DHS/ICE-002 ICEPIC System of Records Notice (SORN), August 18, 2008, 73 FR 48226. In the future, ICE will be updating the ICEPIC PIA and SORN to reflect the change of the system name to DPICS2.

record keeping (similar to records maintained in WebRMS) allowing for Special Agents (SA) and Supervisory Special Agents (SSA) to perform their investigation/management activities in the course of carrying out their official duties. The Dispatch and Incident Record Management Systems PIA[3] lays out the preliminary investigative process whereby a Protective Security Officer (i.e., contract guard) or a sworn FPS law enforcement officer (Inspector or Criminal Investigator) documents information pertaining to incidents in the WebRMS system.

Based upon FPS Criminal Investigative Standards and Electronic Case Management policy, an FPS Criminal Investigator may conduct a full investigation in which case the Criminal Investigator documents the investigative process using TECS. TECS is not linked to WebRMS. At FPS, only Criminal Investigators have access to TECS, and relevant information is entered into TECS manually. Examples of the types of records that FPS documents in TECS include suspected violations of law, arrests, judicial actions (to include information pertaining to presenting the case to the relevant judicial jurisdiction for prosecution), and conviction information in connection with serious crimes[4] occurring in or around federal properties or facilities.

During the course of a typical investigation, FPS collects personally identifiable information (PII) directly from the reporting persons, victims, witnesses, and suspects who voluntarily provide it. This information may be supplemented by further information from government law enforcement systems and commercial information systems. When PII is collected from commercial information systems, FPS checks its accuracy against information from government law enforcement information systems and information voluntarily supplied by the individual, provided that individual is interviewed by an FPS Criminal Investigator.

As a user of TECS, FPS has control over how its data is used, but does not control retention of the data in the TECS database. The approved retention for records in TECS is 75 years.[5] However, the National Archives and Records Administration (NARA) approved retention for FPS's criminal investigative records is 20 years. Use of TECS over time could result in FPS information being retained for longer than the approved retention time. FPS is working to identify a long-term case management solution to this retention problem. In the meantime, FPS addresses this by maintaining only limited information in TECS. TECS is primarily used for its search capabilities; the majority of FPS's investigative files is managed in paper form and retained for 20 years consistent with the FPS SORN. When records in TECS are

[3] *See* DHS/NPPD/PIA-010 Federal Protective Service Dispatch Incident Records Management Systems, *available at* http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/FPS_WebRMS_PIA.pdf.
[4] Serious crimes are those that are considered to be Part 1 offenses under the Department of Justice Federal Bureau of Investigation's (FBI) Uniformed Crime Reporting Program. *See* FBI, UNIFORM CRIME REPORT, CRIME IN THE UNITED STATES, 2009, *available at* http://www2.fbi.gov/ucr/cius2009/about/offense_definitions.html. Serious crimes can also be any criminal offense classified as a felony under the laws of the United States, any state or any foreign country where the crime occurred.
[5] *See* DHS/CBP-011 - U.S. Customs and Border Protection TECS, December 19, 2008, 73 FR 77778.

due to be either destroyed or archived, based on the factors outlined in the retention schedule, FPS must make a request to have those records deleted (or archived) from TECS.

Within TECS, FPS does not share its criminal investigative records with other DHS components or TECS users. Authorized TECS users, both inside FPS and outside of the agency, are able to perform subject-based queries of records and identify other records that are associated with the subject (or individual). The search could be based on several parameters such as name, date of birth, social security number, or other personal identifiers (e.g., driver's license number, passport number). Based on the inputted parameters, TECS returns possible matches, and the user reviews those results in order to validate the findings or to determine if the records indicate a positive match to the individual that was queried as part of the criminal investigation.

When an authorized TECS user from an outside agency conducts a query that returns possible matches to FPS records, the query result does not allow the user access to the full record. For example, if a user queries a subject of a previous FPS investigation that resulted in an arrest, the response to the TECS query reflects that an arrest record exists that belongs to FPS. If the agency is interested in obtaining further information pertaining to the arrest (based on the subject record in TECS), the agency must make direct contact with FPS to initiate a law enforcement-to-law enforcement request based on official need.

Information Sharing via DPICS2 and the LEIS Service

FPS provides law enforcement and security services to approximately 9,000 federal facilities nationwide, which are widely dispersed and reside within the jurisdiction of many other law enforcement agencies. At times, FPS may need to share data with other law enforcement entities, such as other DHS components or state and local law enforcement entities, to effectively coordinate incident response and appropriately respond to threats and criminal activity occurring in or around federal facilities. Allowing external partners to access limited subsets of FPS data can be a vital part of solving crime, protecting facilities, and saving resources by reducing time necessary to complete tasks.

To enhance coordination with law enforcement agencies, FPS uses DPICS2, a system managed by ICE and fully described in ICE's DPICS2 PIA.[6] DPICS2 was created to assist DHS law enforcement and homeland security personnel in identifying suspect identities in support of the homeland security mission. The information processed by DPICS2 is a compilation of information from existing DHS investigative and apprehension records systems, as well as immigration benefits and alien admission records systems.

FPS uses the Law Enforcement Information Sharing (LEIS) Service to share data from WebRMS with external partners, resulting in an increased capability to mitigate risks to federal

[6] *See* DHS/ICE/PIA-004 ICE Pattern Analysis and Information Collection (ICEPIC) (now known as DPICS2), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_icepic.pdf

facilities. DHS personnel are able to query the data in DPICS2 for search purposes. Law enforcement partners outside DHS query certain data in DPICS2, including the FPS data, via an external interface called the LEIS Service.[7] This process allows for greater collaboration with law enforcement stakeholders through the use of innovative technology.

To promote privacy protection and to limit data sharing, FPS limits the amount of data made available through DPICS2 and the LEIS Service by carefully scoping the inclusion of WebRMS records to those that are relevant and necessary to meeting FPS's information sharing needs. First, FPS limits the records available in DPICS2 to the last five years of WebRMS data.

FPS further limits sharing of WebRMS data by including only records that are classified according to certain pre-approved activity codes. These activity codes correspond to the incident type. For example, an activity code for aggravated assault could be used to retrieve WebRMS records of incidents involving aggravated assault. Only records classified by activity codes that are pre-approved by the DHS Privacy Office for inclusion in DPICS2 are made available. This ensures that only data associated with incidents that are appropriate for sharing are made available to DPICS2 users and to external users through the LEIS Service. Internal DHS users of DPICS2 are able to view the full FPS record in response to queries. However, when an external agency queries DPICS2 via the LEIS Service, the search results are limited to the following data fields from WebRMS:

- date of record;
- record number;
- location of event (building number & address);
- activity code;
- description of activity code; and
- name of the individual who was subject of the agency's search.

Receipt of this limited information notifies the agency of the existence of an FPS case file relating to the individual. The agency must then contact FPS to request additional information in which case information is provided in accordance with existing procedures and as permitted by the Privacy Act System of Records covering FPS's data, Law Enforcement Authority in Support of the Protection of Property Owned or Occupied by the Federal Government, DHS/ALL-025.[8]

[7] *See* DHS/ICE/PIA-004(a) ICEPIC PIA update describing the operation of the Law Enforcement Information Sharing Service, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_icepic-4a.pdf.
[8] *See* DHS/ALL-025 - Department of Homeland Security Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security, February 3, 2010, 75 FR 5614.

Privacy Risks and Mitigation

The above described use of TECS and DPICS[2] poses four main privacy risks.

The first risk stems from inconsistencies between FPS's published Dispatch and Incident Records Management PIA and how information is actually managed and shared. The result is that individuals may not be provided adequate notice, or may not be fully aware of how their information is used. This risk is mitigated by the update to this PIA, which provides further transparency into how FPS uses its incident management data and discusses two additional systems that FPS uses to manage and share data.

Second, with the use of two systems that are managed by other DHS components with other authorized users, FPS's information could be shared beyond that which is necessary to support of FPS's specific mission. As a result, the information could be misused. This risk is mitigated as follows: while other TECS users are able to query records in the TECS system, the results of the query provide limited information that are determined by the FPS Criminal Investigator to be necessary during the record's creation. TECS authorized users can only query TECS records for official business. Returned results may include information about a subject of a criminal investigation, such as name, date of birth, and other identifying information, that would be needed to confirm a positive match.

The query results also identify FPS as the owner of the record. To obtain further information, the user must make an official request as a law enforcement entity. Information, such as the Criminal Investigator's reports of investigation, is restricted and accessible only to authorized FPS personnel. All TECS users must undergo a background investigation (BI) prior to being granted access.

In addition to this threshold criterion for access, CBP (TECS System owner) also employs several layers of training, review, and access control. All users are required to read and comply with the TECS security requirements, as well as take and pass the TECS Security and Privacy Awareness course annually in order to establish and retain TECS access. Supervisory review is required to ensure that only authorized records are entered and the information is accurate.

Extensive audit logs are maintained showing who has accessed records and what changes, if any, were made to the records. Lastly, access to TECS is controlled by both the physical location and mission responsibilities of the user. For example, FPS records can be restricted from view from other TECS users based on physical location or mission responsibility of the TECS user. FPS relies and adheres to the "Third Agency Rule" with respect to the dissemination of Subject Records that are owned by another agency. Simply, this means that information accessed and viewed through TECS cannot be disclosed outside of TECS and others who use TECS by the accessing agency without specific approval of the agency or entity which owns (i.e., first collected and submitted) the data being accessed.

FPS uses DPICS2 and the LEIS Service primarily to enhance information sharing; however, measures are in place to ensure that such sharing is very limited in scope. First, FPS only includes records in DPICS2 that pertain to certain activities that are pre-approved by the DHS Privacy Office for inclusion in DPICS2. Further, the results of external users' queries are limited to a small subset of information, just enough to confirm a positive match. External users must contact FPS for additional information upon confirmation of a match or a hit.

A third risk is that by maintaining incident data in two different systems, WebRMS and TECS, there could be inconsistencies between the two. This risk is mitigated through FPS policy, which requires FPS supervisors to review and approve information that is entered in WebRMS. If the offense entered into WebRMS will be subsequently entered into TECS as part of a criminal investigation, FPS criminal investigative supervisors will conduct a further review of the information contained in WebRMS for completeness and accuracy as well as review and approve the information entered into TECS.

The fourth risk identified is related to retention. With the use of two outside systems, there is a risk that the retention periods for records in each system may be incompatible with FPS's retention period of 20 years, as allowed by the FPS Law Enforcement SORN.[9] For example, records in TECS are maintained for 75 years, in accordance with CBP's SORN.[10] As a user of TECS, FPS has control over how its data is used, but does not control retention of the data in the TECS database. Use of TECS over time could result in FPS information being retained for longer than the approved retention time. FPS is working to identify a long-term case management solution to address this issue. Additionally, FPS retains minimal information in TECS. TECS is primarily used for its search capabilities; however, the bulk of FPS's investigative files is managed in paper form and retained for 20 years consistent with the FPS SORN.

For those records that FPS maintains in DPICS2 and shares through the LEIS Service, only the last five years of data from WebRMS (the nationwide incident reporting system, which serves as a central repository for all case management data) are made available, and the data is only retained for a period of ten years and then archived for five years. This very limited retention helps reduce the risks of misuse or inappropriate sharing of records, and closely aligns with FPS's own retention period.

Reason for the PIA Update

This PIA is being updated because the existing Dispatch and Incident Record Management Systems PIA does not address FPS's use of TECS as an investigative case

[9] *See* DHS/ALL-025 - Department of Homeland Security Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security, February 3, 2010, 75 FR 5614.
[10] *See* DHS/CBP-011 - U.S. Customs and Border Protection TECS, December 19, 2008, 73 FR 77778.

management tool or fully describe how FPS shares its incident management data with external law enforcement partners. In addition to ad-hoc sharing of information, FPS shares limited information with external partners through DPICS2 to enhance coordination with stakeholders and increase FPS's ability to mitigate risks to federal facilities, as well as to coordinate incident response to threats and criminal activity occurring in or around federal facilities.

Privacy Impact Analysis

Authorities and Other Requirements

The following are the specific legal authorities that permit and define the collection of information by the Federal Protective Service for maintenance for the purposes described in this PIA Update:

- Section 1706 of the Homeland Security Act of 2002, codified at 40 U.S.C. § 1315, Law Enforcement Authority of Secretary of Homeland Security for Protection of Public Property.
- Office of the Attorney General, Guidelines for the Exercise of Law Enforcement Authorities by Officers and Agents of the Department of Homeland Security under 40 U.S.C. § 1315, dated March 1, 2005.
- DHS Delegation 17007, Delegation for Administration of the Federal Protective Service, dated December 18, 2009.
- NPPD Delegation 17007.001, Delegation to the Director for the Federal Protective Service, dated December 24, 2009.
- 41 C.F.R. § 102-74.15 requires occupants of facilities under the custody and control of Federal agencies to promptly report all crimes and suspicious circumstances occurring on federally-controlled property first to the regional FPS.
- 41 C.F.R. § 102-85.35 requires FPS to provide general law enforcement for General Services Administration-controlled property.

Additionally, FPS's activities, as described in this PIA are covered under the DHS SORN for Law Enforcement Authority in Support of the Protection of Property Owned or Occupied by the Federal Government.

Characterization of the Information

This update does not change the characterization of the data that FPS collects as part of its Dispatch and Incident Record Management Systems.

Uses of the Information

The uses of FPS's incident management data have not changed with this update. Rather, this update provides greater transparency into the system FPS uses during the criminal investigative process. Specifically, FPS uses the TECS CM module to document and manage information during the process of a criminal investigation. FPS SAs and SSAs access TECS to record their investigation/management activities in the course of carrying out their official duties. That information may be used to support the law enforcement mission of FPS, DHS, and other federal, state, local and international law enforcement agencies with law enforcement, intelligence, and counterterrorism responsibilities. FPS collects PII because that information is necessary for potential judicial action in a court of law, to sufficiently identify an individual to the exclusion of others before filing charges, etc.

FPS creates records on individuals in TECS only if there is an investigative interest in the individual or the individual is connected to an ongoing criminal investigation (i.e., suspect). FPS does not create records on the victims or witnesses within TECS. If information is collected on victims or witnesses through investigative reports, that information is restricted, can only be viewed by FPS Criminal Investigators, and is not searchable within TECS.

Authorized TECS users, both inside FPS and outside of the agency, are able to perform subject-based queries of records and identify other records that are associated with the subject (or individual). The search could be based on several parameters such as name, date of birth, social security number, or other personal identifiers (e.g., driver's license number, passport number). Based on the inputted parameters, TECS returns possible matches, and the user reviews those results in order to validate the findings or to determine if the records indicate a positive match to the individual that was queried as part of the criminal investigation.

When FPS conducts searches of TECS, FPS Criminal Investigators review possible matches and make a determination as to whether or not the possible match is the same individual as the query. When an authorized TECS user from an outside agency conducts a query that returns possible matches to FPS records, the query result does not allow the user access to the full record. For example, if a user queries a subject of a previous FPS investigation that resulted in an arrest, the response to the TECS query reflects that an arrest record exists that belongs to FPS. If the agency is interested in obtaining further information pertaining to the arrest (based on the subject record in TECS), the agency must make direct contact with FPS to initiate a law enforcement-to-law enforcement request based on official need.

Additionally, FPS exports limited incident data from WebRMS in ICE's DPICS[2] system in order to share data with other DHS law enforcement and homeland security personnel, and with external law enforcement partners through the LEIS Service. This sharing serves to improve coordination with external stakeholders and augment FPS's risk management capabilities.

Notice

As described in the Dispatch and Incident Record Management Systems PIA, FPS collects most information directly from individuals. There may be occasional instances where DIRMS maintains information about individuals that is not collected directly from them. For example, a witness or victim may provide information about a suspect. However, individuals generally have notice of what information is being collected and why. There is a slight risk that individuals may not be fully aware of how their information is used. That risk is mitigated by publishing this PIA Update and through publication of the SORN.

Data Retention by the project

There is no change in the retention of data in the WebRMS database or any of the systems that collectively make up FPS's Dispatch and Incident Record Management Systems. With this update, however, limited WebRMS data is also retained in ICE's DPICS^2 system for the purpose of facilitating external sharing with internal and external law enforcement partners. This data is retained in DPICS^2 for a period of ten years and then archived for five years. After the five year period, the information is destroyed unless it becomes relevant to law enforcement activity, at which point the retention schedule is reset.

There is a risk that records may be retained longer than permissible under the relevant retention schedule. This risk is mitigated by the retention schedule. FPS maintains investigative case management records in TECS according to CBP's retention period for TECS records, which is 75 years.[11] The NARA approved retention for FPS's criminal investigative records is 20 years. Use of TECS over time could result in FPS information being retained for longer than the approved retention time. FPS is working to identify a long-term case management solution to this retention problem. In the meantime, FPS addresses this by maintaining only limited information in TECS. TECS is primarily used for its search capabilities; the majority of FPS's investigative files is managed in paper form and retained for 20 years consistent with the FPS SORN. When records in TECS are due to be either destroyed or archived, based on the factors outlined in the retention schedule, FPS must make a request to have those records deleted (or archived) from TECS.

Information Sharing

FPS shares information in TECS for law enforcement investigatory, evidentiary, or prosecutorial purposes, or in connection with specific civil proceedings. Records in TECS may be shared with other authorized users of TECS pursuant to TECS User profiles, a Memorandum of Understanding (MOU), or other user agreement.

FPS may share information on a "need to know" basis with other federal, state, local, tribal, and foreign law enforcement, with law enforcement agencies in response to a specific

[11] *See* DHS/CBP-011 - U.S. Customs and Border Protection TECS, December 19, 2008, 73 FR 77778.

request, when the agency has demonstrated a justifiable need for that information. These requests must be made from the head of the requesting agency (or its designee), and be made on official agency letterhead. FPS follows an internal approval process to ensure the appropriateness of the disclosure before making any release of records. Upon receipt of a request, FPS reviews the request to ensure it is a valid request that allows FPS to share the information with another law enforcement or public safety agency. An FPS Criminal Investigator evaluates and fulfills the request, and an FPS Branch Chief performs a review and must provide approval before records may be released externally.

FPS uses DPICS2 to enhance its ability to share information with DHS law enforcement and homeland security personnel and external law enforcement partners to promote the FPS mission to manage risks to federal facilities. FPS makes more limited information from WebRMS available to external law enforcement partners through the LEIS Service, which is used by external law enforcement agencies that ICE has approved to use the system via a signed Memorandum of Understanding.

There is a risk that more information than necessary to accomplish the FPS mission could be shared. FPS mitigates this risk in two ways. First, FPS limits the records made available against which to query only to WebRMS records from the last five years and classified by certain activity codes that correspond to certain incident types (e.g., aggravated assault) that have been pre-approved by the DHS Privacy Office for inclusion in DPICS2. Secondly, for external users who query the data through the LEIS Service, the search results are limited to the following data fields from WebRMS:

- date of record;
- record number;
- location of event (building number & address);
- activity code;
- description of activity code; and
- name of the individual who was subject of the agency's search.

In order for an external user to obtain additional information pertaining to a match, the agency must contact FPS to request access. FPS then determines whether additional sharing is appropriate, as permitted by the Privacy Act System of Records covering FPS's data.

Redress

There is no change to the access, redress, or correction procedures or related privacy risks.

Auditing and Accountability

Both TECS and DPICS2 are owned and managed by CBP and ICE, respectively. Both systems use a multi-layered approach for auditing and accountability that includes usage oversight, recurring user training, information technology safeguards, access control protocols, and audit trails. Authorized FPS users are subject to the user access and training requirements and for following all applicable terms of use and rules of behavior for the TECS and DPICS2 systems. Further details can be found in the PIAs covering these systems.

Additionally, the system owners are responsible for approving any new users to their systems who would, in turn, potentially have access to FPS data. For example, as the system owner for TECS, CBP must provide authorization for an outside entity's access to TECS through the issuance of a MOU. The MOU specifies the general terms and conditions that govern the use of the functionality or data, including privacy-related limitations on use and the types of information in TECS to which the agency is being granted access, depending upon their mission needs. CBP also uses Interconnection Security Agreements (ISA) to cover any interface implemented between CBP and the outside entity. The ISA specifies the data elements, format, and interface type to include the operational considerations of the interface.

Responsible Official

Eric L. Patterson
Director, Federal Protective Service
National Protection and Programs Directorate
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security