Privacy Impact Assessment (PIA) Update
for the

Federal Protective Service Dispatch and Incident Record Management Systems

DHS/NPPD/FPS/PIA-010(c)

July 14, 2017

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

Reviewing Official
Jonathan R. Cantor
Acting 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) is updating the Dispatch and Incident Record Management Systems (DIRMS) Privacy Impact Assessment (PIA). This PIA update reflects the removal of the Treasury Enforcement Communications System (TECS), Field Interview Report (FIR) system, and FPS's sharing of case management data into the DHS Pattern Information Collaboration Sharing System (DPICS). This PIA update also documents the addition of the new Law Enforcement Information Management System (LEIMS).

Overview

The Federal Protection Service (FPS) is an operational component within the National Protection and Programs Directorate (NPPD) that provides law enforcement and security services to approximately 9,000 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. This support is provided 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. This suite of systems is referred to in the PIA as the FPS Dispatch and Incident Record Management Systems (DIRMS). These systems are used by federal employees and contractors to document and report suspicious activities, security-related matters, and alleged violations of law related to the protection of federal facilities. In addition, visitors may report suspicious activity and alleged violations of law related to the protection of federal facilities to FPS officers. The original PIA, published in September 2009[1], outlines the three primary applications FPS uses to track such activities of its officers and to perform case management for incidents that occur:

- Dispatch Operations Log (DOL)
- Web Records Management System (WebRMS)
- Dictaphone Police Report Recorder

In March 2012, an update to the DIRMS PIA[2] added FPS's use of the Field Interview Report (FIR) system to collect and analyze information from field interviews, contacts, and stops at

[1] *See* DHS/NPPD/PIA-010 Federal Protective Service Dispatch Incident Records Management Systems, *available at* www.dhs.gov/privacy.
[2] *See* DHS/NPPD/PIA-010(a) Federal Protective Service Dispatch Incident Records Management Systems, *available at* www.dhs.gov/privacy.

protected federal facilities around the country that have been identified as a significant vulnerability. However, the FIR system never met the operational needs of FPS and is not currently used.

In 2014 the Treasury Enforcement Communications System (TECS)[3], which is owned by U.S. Customs and Border Protection (CBP), and DHS Pattern Information Collaboration Sharing System (DPICS)[4], which is owned by U.S. Immigration and Customs Enforcement (ICE) were added to the DIRMS inventory as systems FPS shares data. However, DPICS is no longer used by FPS and this functionality is covered by the WebRMS application. Likewise, FPS's use of TECS was phased out in February 2017. This functionality for FPS will be replaced by the new FPS Law Enforcement Information Management System (LEIMS). LEIMS is expected to be operational in August 2017. The information currently in TECS will remain in the system and with CBP until the system is decommissioned. FPS will not migrate information from TECS to LEIMS. This system will facilitate additional case processing activities.

The current full suite of systems in the FPS DIRMS includes the following:

1. DOL – An application that creates a continuous, chronological log of reports of daily activities.
2. WebRMS – The nationwide incident reporting system, which serves as a central repository for all case management data. **Note:** The use of WebRMS by FPS will be phased out and this functionality will be provided by LEIMS. WebRMS will continue to operate for a period of time once LEIMS is operational for continuity purposes until WebRMS can be decommissioned. At this time, the exact decommission date is unknown but estimated to be within 6 to 12 months after LEIMS is in production.
3. LEIMS (new) – Allows FPS investigators and inspectors to document specific details and the outcome of all case activities. LEIMS is currently in development and is expected to be operational in August 2017.
4. Dictaphone Police Recorder – A system that allows FPS Protective Security Officers without direct access to WebRMS to record information telephonically. **Note:** The Dictaphone Police Recorder will eventually be replaced by a new Voice Over IP phone system called Phone and Voice Recording System. At that time, FPS will update this PIA.

[3] *See* DHS/CBP/PIA-021 TECS System: Platform, *available at* www.dhs.gov/privacy.
[4] *See* DHS/ICE/PIA-004 ICE Pattern Analysis and Information Collection (ICEPIC), *available at* www.dhs.gov/privacy. After the publication of this PIA, the system name was changed from ICEPIC to DPICS. DPICS has since been decommissioned.

Reason for the PIA Update

The reason for this PIA Update is to document the addition of LEIMS to the case management process. This update also documents the removal of TECS, FIR, and sharing case management information through DPICS.

The addition of LEIMS does not add any new privacy risks that have not been addressed in previous versions of this PIA.

Privacy Impact Analysis

Authorities and Other Requirements

There have been no changes in the specific legal authorities that permit and define the collection of information by FPS for maintenance since the last PIA update in 2014.

FPS's activities, as described in this PIA, are covered under the Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security System of Records (SORN).[5]

Characterization of the Information

These systems collect information about individuals who are the subject of routine reporting by FPS 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. The list below is a comprehensive list of the of data elements collected by DIRMS:

- Name;
- Alias;
- Social Security number (SSN);
- Alien Registration Number (A-Number);
- Date of birth;
- Age;

[5] DHS/ALL-025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security System of Records, 82 FR 27274 (June 14, 2017).

- Address;
- Race;
- Sex;
- Height;
- Weight;
- Build;
- Posture;
- Eye color;
- Hair color;
- Nationality;
- Scars/Marks/Tattoos;
- Phone numbers;
- Email addresses;
- Driver's license number;
- Employer;
- Photograph;
- Hand writing exemplars;
- National Crime Information Center (NCIC) number; and
- Vehicle information.

The addition of LEIMS will allow investigating officers to attach hand writing exemplars and photographs to their case files. These photos may contain images of victims, suspects, or other areas of interests to aid in the investigation.

If the 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 FBI's National Crime Information Center[6].

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

[6] The National Crime Information Center (NCIC) is an electronic clearinghouse of crime data used by criminal justice agencies nationwide. It helps criminal justice professionals apprehend fugitives, locate missing persons, recover stolen property, and identify terrorists. Further information is available at https://www.fbi.gov/services/cjis/ncic.

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. There are no new privacy risks associated with the characterization of the information under DIRMS.

Uses of the Information

The use of FPS's incident management data have not changed with this update. Rather, this update provides greater transparency into FPS's use of LEIMS once it becomes operational in summer of 2017. FPS 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.

LEIMS provides a platform for FPS inspectors and investigators to capture and process records of their law enforcement activities. Records maintained within the system are associated with incident response, criminal case investigation, and physical security activities, security assessments, and inspections. As with other DIRMS, LEIMS will maintain personally identifiable information (PII) from DHS and FPS employees and contractors, as well as members of the public involved in FPS operations, investigations, and other activities.

Notice

As with other DIRMS, LEIMS collects most information directly from individuals via officer interviews. There may be occasional instances when 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.

Data Retention by the project

There is no change in the retention of data in any of the systems that collectively make up FPS' DIRMS.

NPPD will work with DHS Headquarters (HQ) to propose a records retention schedule. NPPD intends to request National Archives and Records Administration (NARA) approval to retain for 20 years from the end of the fiscal year in which the case was closed. Cases deemed significant pursuant to criteria detailed in the proposed records schedule because of historical interest will be retained permanently. This retention schedule is consistent with the proposed DHS

Enterprise Schedule for Investigative Records. After 20 year period, the information would be destroyed or, if deemed necessary, retained further under a reset retention schedule. All records will be treated as permanent until a records retention schedule is approved by NARA.

Information Sharing

Information sharing has not changed for the applications listed in this PIA update, therefore no new privacy risks were identified. 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. External sharing is consistent with the original collection of information; specifically, FPS shares 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, Occupied, or Secured by the Department of Homeland Security*[7]. Routine uses G, I, and J of this SORN allow FPS to share the information for law enforcement, criminal investigations, and civil litigation. Routine use G allows for disclosure to appropriate federal, state, tribal, local, international, or foreign law enforcement agencies. Routine use I allows for disclosure to a court, magistrate, or administrative tribunal in the course of presenting evidence. Routine use J allows for disclosure to third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate to the proper performance of the official duties of the officer making the disclosure. FPS collects this information to support law enforcement and security operations within the FPS jurisdiction.

Redress

There are no changes to the individual access, redress, and correction processes associated with this PIA update. Therefore, no new privacy risk associated with access, redress, and correction were identified.

Auditing and Accountability

There have not been any changes since the last PIA update. Access to DIRMS are password-protected and administered to assure access is granted only to those with a need to use the system and covered by existing privacy policies, as with the other law enforcement sensitive databases utilized by this agency. All employees are required to successfully complete annual

[7] DHS/ALL-025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security System of Records, 82 FR 27274 (June 14, 2017).

training on computer security and privacy protection. Auditing capabilities are enabled on the server Operating System.

Responsible Official

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

Approval Signature

Original, signed copy on filed with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security