Privacy Impact Assessment

for the

Federal Protective Service Dispatch and Incident Record Management Systems

DHS Reference No. DHS/FPS/PIA-001(d)

July 30, 2020

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS), Federal Protective Service (FPS) owns and operates a suite of systems, collectively referred to the Dispatch and Incident Record Management Systems (DIRMS). 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. FPS is updating this Privacy Impact Assessment (PIA) to reflect general changes to the system infrastructure and the upgrade of the Dictaphone Police Recorder to the NICE Voice Recorder.

Overview

FPS is an operational component within the DHS Management Directorate 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 DIRMS, a suite of systems, to support nationwide incident reporting. 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. FPS uses several applications to track such activities and to perform case management for incidents that occur:

- Dispatch Operations Log (DOL) - An application that creates a continuous, chronological log of reports of daily activities.
- Web Records Management System (WebRMS) - The nationwide incident reporting system, which serves as a central repository for all case management data.[1]

[1] 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 as a read-only system for continuity purposes. Once LEIMS is operational, WebRMS will be decommissioned.

- Law Enforcement Information Management System (LEIMS) - Allows FPS investigators and inspectors to document specific details and the outcome of all case activities.
- Dictaphone Police Report Recorder - A system that allows FPS personnel without direct access to WebRMS to record information telephonically.

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 regional FPS offices around the United States. The four MegaCenter locations are all a part of one General Support System network which consists of mission specific applications, a radio system, and a video network. The General Support System allows the MegaCenters to provide the infrastructure to support the applications above.

Reason for the PIA Update

This PIA is being updated to document the change from the Dictaphone Police Recorder to the NICE Voice Recorder. While the two applications perform the same function of recording and storing phone calls received by the MegaCenters, the old system uses antiquated hardware and software which is no longer supported. In order to comply with DHS security requirements, the Dictaphone Police Report Recorder was removed from the MegaCenters and replaced with the NICE Voice Recorder, allowing for recording of all radio and telephone transmissions between Dispatchers and FPS Field Officers and play-back recordings for event reconciliation, records retrieval and quality assurance.

This PIA also documents the infrastructure change of the MegaCenters. In 2019, the four individual MegaCenters in Philadelphia, PA; Denver, CO; Battle Creek, MI; and Suitland, MD; were replaced by a single MegaCenter General Support System network that spans the four locations. The MegaCenter General Support System performs the same business/mission functions as the individual MegaCenters did.

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 2017.

FPS' 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 Notice (SORN).[2] The General Information Technology Access Account Records System (GITAARS) SORN also provides coverage for the collection of information needed to provision access to DIRMS.[3]

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 and around 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;
- Address;
- Race;
- Sex;
- Height;
- Weight;
- Build;
- Posture;

[2] *See* 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 Fed. Reg. 27274 (June 14, 2017), *available at* https://www.dhs.gov/system-records-notices-sorns.
[3] *See* DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 Fed. Reg. 70792 (November 27, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.

- Eye color;
- Hair color;
- Nationality;
- Scars/Marks/Tattoos;
- Phone numbers;
- Email addresses;
- Driver's license number;
- Employer;
- Photograph;
- Writing hand;
- National Crime Information Center (NCIC) number;
- Vehicle information;
- FPS Officer Badge Number;
- FPS Officer Name;
- Physical Security Officer (PSO) Name; and
- PSO last four digits of SSN.

The photos collected 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 Federal Bureau of Investigation's (FBI) National Crime Information Center.[4]

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

[4] 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. *See* U.S. DEPARTMENT OF JUSTICE, FEDERAL BUREAU OF INVESTIGATION, NATIONAL CRIME INFORMATION CENTER (NCIC), https://www.fbi.gov/services/cjis/ncic (last visited July 28, 2020).

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 due to changes documented in this PIA.

Uses of the Information

The use of FPS' incident management data have not changed with this update. 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.

The NICE Voice Recorder is used to record all telephone transmissions, such as those between Dispatchers and FPS Field Officers. These recordings are saved and allow for play-back for event reconciliation, records retrieval, and quality assurance.

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. LEIMS maintains personally identifiable information from DHS and FPS employees and contractors, as well as members of the public involved in FPS operations, investigations, and other activities.

Notice

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 because the individuals interact directly with the FPS PSO.

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. FPS continues to work with DHS Headquarters to propose a records retention schedule. FPS intends to request National Archives and Records Administration (NARA) approval to retain the data 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 the 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.

Privacy Risk: There is a risk that information will be retained for longer than is required or needed in DIRMS.

Mitigation: The risk is not mitigated yet. Once a NARA-approved records schedule is determined and approved, FPS will follow that schedule.

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 FBI, 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*.[5] 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.

[5] *See supra* note 3.

Auditing and Accountability

There have not been any changes since the last PIA update regarding auditing and accountability. Access to DIRMS applications 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 used by this agency. All employees are required to successfully complete annual training on computer security and privacy protection. Auditing capabilities are enabled on the Windows and Linux server operating systems.

Responsible Officials

Eric L. Patterson
Director, Federal Protective Service
U.S. Department of Homeland Security
(202) 732-8000

Approval Signature

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

_____

Dena Kozanas
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717