Privacy Impact Assessment Update
for the

Federal Protective Service Dispatch and Incident Record Management Systems

DHS/NPPD/PIA-010(a)

March 13, 2012

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

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

Abstract

This Privacy Impact Assessment (PIA) updates the National Protection and Programs Directorate's Federal Protective Service Dispatch and Incident Record Management Systems to add the Field Interview Report (FIR) system to its suite of record management systems and to include administrative changes to the existing PIA. FPS will use the FIR system to collect and analyze information from field interviews, contacts, and stops at protected federal facilities around the country that have been identified as a significant vulnerability. NPPD is conducting this PIA because this new management reporting system will collect Personally Identifying Information (PII) about members of the public.

Introduction

FPS is an operational component within the National Protection and Programs Directorate (NPPD) that was previously held within U.S. Immigration and Customs Enforcement (ICE) and 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 by deploying a highly trained and multi-disciplinary police force.

To support the communication and reporting of daily activities, incidents, and offenses in and around federal buildings and facilities, FPS owns and operates a suite of systems collectively referred to as the FPS Dispatch and Incident Record Management Systems. The original PIA, published in September 2009, outlines how 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. This PIA updates the Federal Protective Service Dispatch and Incident Record Management Systems to incorporate the Field Interview Report into the system.

FPS officers regularly conduct field interviews, which are interviews of members of the general public, agency employees and/or agency contractors. FPS conducts field interviews during the course of preliminary investigations and in doing so, captures personal information from individuals when reasonable suspicion exists under the Terry Doctrine or on a voluntary basis when a consensual contact is made. FPS officers catalog this information and analyze it to determine if recurrence or patterns contribute to the preliminary investigation or indicate a requirement for further investigation. FPS officers have been conducting field interviews since the agency's inception and have been using a paper-based system for collecting the data. As part of this update, FPS will electronically retain information collected from field interviews in the FIR database.

Similar to the information documented in the original PIA, the types of information FPS collects during field interviews and maintains in the FIR database will vary depending on the type of incident or offense. FPS may collect information on individuals such as suspects, victims, witnesses, participants, employees, building occupants, and visitors. At a minimum, FPS will collect the individual's name and general contact information.

FPS may also collect contextual information about the individual in relation to the particular incident or offense, some of which may be sensitive. For example, an FPS officer may describe the specific indicators that contributed to reasonable suspicion for initiating a contact.

By transitioning from the paper-based system to the electronic FIR database, FPS can use the information collected from field interviews to reduce vulnerabilities at protected federal facilities around the country by identifying patterns of similar activity. For example, using FIR an FPS officer could identify that the same person or vehicle was involved in at investigation at two or more protected facilities or in multiple cities. The creation of a basic data system that would give officers near real-time feedback ("hits" or "alerts") regarding people or vehicles entered into the database would allow collection of the needed information and facilitate identification of threats to protected properties. Such rapid feedback would encourage officers to collect the requisite information to identify threats to protected properties. The data maintained in FIR will only include data that is lawfully obtained during legally permissible encounters with citizens in or around federal facilities during the course of daily business.

Reason for the PIA Update

This PIA updates the FPS Dispatch and Incident Record Management Systems to add FIR to its suite of record management systems. The PIA also includes an administrative change to reflect that FPS is now an organizational component of NPPD.

Privacy Impact Analysis

The System and the Information Collected and Stored within the System

Collectively, the FPS Dispatch and Incident Management Systems are used to track the daily activities of FPS officers and to perform case management for the offenses and incidents that occur in and around the federal facilities that FPS secures. Specifically, FIR will collect information about individuals and/or vehicles that are subjects of FPS field interviews, which are contacts or stops made in connection with preliminary investigations. Contacts can occur for a variety of reasons. In particular, FPS officers may make contact with people who display an unusual interest in security countermeasures and protective procedures, minor infractions that do not result in an arrest or suspicious activity. These individuals are typically persons believed to be involved in or related to a particular incident or offense, such as suspects and participants.

The exact information collected about these individuals varies, depending on the type of incident or offense that occurred. However, at minimum, FPS collects basic identifying information such as name and contact information. Where relevant, FPS may collect other information such as: full name, aliases, sex, race, appearance (e.g. hair or eye color), distinguishing characteristics, residence address, phone number, date of birth, height, weight, social security or alien number, driver's license number, vehicle plate number, vehicle description, and passport number. FPS may also collect contextual information about the individual in relation to the particular incident or offense, some of which may be sensitive. For

example, an FPS officer may describe the specific indicators that contributed to reasonable suspicion for initiating a contact.

The scope of information collected will not change as part of this update. This update reflects a transition from a paper-based system to retaining this information in the electronic FIR database.

Uses of the System and the Information

FPS will use FIR to identify significant vulnerabilities and threats to federal facilities that FPS secures. FIR will provide near real-time feedback ("hits" or "alerts") relating to people or vehicles entered into the FIR database. FPS officers and command staff will use information in the FIR database during an event, incident or offense to help make decisions regarding the dispatch of additional resources to a particular location or to decide the nature of any follow up investigation required.

To provide FPS officers with "hits" or "alerts," FIR will have the capability to match data fields to determine patterns of activity. Of the data fields collected, only the name, aliases, social security or alien number, state of issue of the driver's license, vehicle plate state, or vehicle make will be used for the initial matching capability. In the case of a positive match against the vehicle make, the vehicle model, year, and color will also be matched. The other data fields are used only to distinguish positive matches from false positives.

The information FPS maintains in the FIR database will serve as an official record of FPS field interviews conducted in and around federal buildings protected by FPS. FIR will collect information in real-time as the officer conducting the field interview creates a record of the interview. The specific information collected is necessary to provide an adequate record of FPS activities, which may be relied upon later to initiate an investigation. This information may also be used to document the appropriateness of FPS activities, in the event of an inquiry or investigation, and to identify recurrent activity that may not merit further investigation. The information is also used to generate statistical reports for facility, regional, and nationwide incidents and offenses at FPS-protected facilities.

If the individual voluntarily elects to provide a Social Security number, FPS will use that information to identify the individual and to perform record checks in federal government law enforcement information systems, such as the National Crime Information Center (NCIC.) The NCIC Number is recorded to reflect that a record was found in response to an NCIC query.

Several standard management reports will be programmed into the FIR database that will provide FPS Headquarters and appropriate DHS leadership with statistical information about offenses or incidents occurring nationally in or around federal buildings. Information may also be shared outside of DHS 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.

Privacy Risk: While the scope of information collected has not changed, there is a risk that "hits" or "alerts" generated through the FIR matching capability will result in false positives.

Mitigation: To mitigate this risk, the FIR database will have primary and secondary matching capabilities. In the case of an initial match, additional fields are matched to help reduce false positives. FPS officers will review the information before taking action. FPS officers are also required to complete annual and refresher training, as well as sign and acknowledge Rules of Behavior before access is granted to the system.

Privacy Risk: There is a privacy risk of inappropriate use of information in the system.

Mitigation: Several measures help to prevent inappropriate use of information in the system. Contact with citizens that generate this information and reports are governed by constitutional law, and all FPS officers receive in-depth training on this topic, both initially and during annual refresher training. Penalties are established for misuse. System operating structure will not permit user-generated queries, except at the headquarters level where analysts are carefully supervised in their daily activities. All queries at the field level are performed automatically when a user enters new data. This will prevent a field level user from searching the data unless a field interview has been completed and entered into the system relating to the information.

Privacy Risk: There is a privacy risk of inappropriate access to the FIR system.

Mitigation: Access to the system is password protected and administered to assure access is granted only to those with a need to use the system and covered by existing privacy protection policies, as with the other law enforcement sensitive databases utilized by this agency. In addition, all employees are required to successfully complete annual training on computer security and privacy protection.

Retention

FPS is in the process of drafting a retention schedule to cover all FPS Dispatch and Incident Management Systems records. The FIR database has a retention period of 25 years after the date of the interview or after the completion of any associated law enforcement action and/or judicial proceedings, whichever is later.

Internal Sharing and Disclosure

The FIR database will not connect, receive or share PII with any other internal DHS system. However, if FPS deems there to be a pattern of activity that requires further investigation, information may enter that information into the primary case management system for FPS. If at that time it is determined that the information meets the criteria of the DHS ISE-SAR program,[1] FPS will enter that information into the FBI's e-Guardian system to confirm whether a Suspicious Activity Report (SAR) is required.

Additionally, several standard management reports will be programmed into the FIR database that will provide FPS Headquarters and appropriate DHS leadership with statistical information about offenses or incidents occurring nationally in or around federal buildings. Internal sharing is consistent with the original collection of information. The information is

[1] *See* http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-dhswide-sar-update-20101117.pdf

shared internal to DHS and its components in accordance with the Privacy Act only as needed to facilitate law enforcement investigatory, evidentiary, or prosecutorial purposes.

External Sharing and Disclosure

The information FPS collects through field interviews 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. Recipients may 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 or Occupied by the Federal Government DHS/ALL-025 (February 3, 2010, 75 FR 5614), which has routine uses allowing FPS to share the information for law enforcement, criminal investigations, and civil litigation.

Notice

As indicated in the previously-published PIA, the publication of the PIA and the Law Enforcement Authority in Support of the Protection of Property Owned or Occupied by the Federal Government SORN (DHS/ALL-025, February 3, 2010, 75 FR 5614) 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. When information is obtained through witnesses, no specific form of notice is provided.

Individual Access, Redress, and Correction

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

Technical Access and Security

Access to the FIR system is password protected and administered to assure access is granted only to those with a need to use the system and covered by existing privacy protection policies, as with the other law enforcement sensitive databases utilized by this agency. All employees are required to successfully complete annual training on computer security and privacy protection.

Technology

The existing technology associated with the FPS Dispatch and Incident Records Management System has not changed with this update and the attendant privacy risks continue to be mitigated as previously described.

Responsible Official

Eric Patterson
Federal Protective Service
Department of Homeland Security

Approval Signature

[Original signed copy on file with the DHS Privacy Office]

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security