Privacy Impact Assessment Update
for the

Field Investigative Reporting System
(FIRS)

DHS/USSS/PIA-009(a)
November 18, 2016

Contact Point
Gregory James
U.S. Secret Service
Office of Investigations (INV)
Criminal Investigative Division
Department of Homeland Security
(202) 406-9330

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The United States Secret Service (Secret Service or USSS) is updating the Privacy Impact Assessment (PIA) for the Criminal Investigative Division's Field Investigative Reporting System (FIRS), which is a suite of several tools and applications that facilitates the reporting of law enforcement activities that fall within the Secret Service's jurisdiction. The Secret Service is conducting this Privacy Impact Assessment (PIA) to document changes in system functionality, the renaming of Wireless Tracking Reporting (WTR), and the removal of the Comprehensive Incident Database on Targeted Violence (CID-TV) from the FIRS suite of applications.

Overview

FIRS is an internal USSS web-based suite of capabilities designed to support USSS law enforcement and staff personnel through the digitization and categorization of case information, threat assessments, and crime patterns; creation of standard operating procedures; and capture of lessons learned. Each of the interconnected capabilities of the FIRS system is reachable via links on the FIRS home page. In order to access the system, an authorized user enters his or her username and password on the FIRS home page, which is authenticated against the Active Directory. Once authenticated, the user is granted access to various capabilities and applications within FIRS based on his or her role. All user roles, including the ability to read, write, or modify information, are predefined based on an individual's need to know and the requirements of his or her particular position, and require the approval of the FIRS Information System Owner (ISO). Once approved, the FIRS Administrator assigns applicable roles to each user. The database that retains FIRS information is maintained under the Application Provision System (APS)[1], and is encrypted-at-rest.

Information entered into FIRS is related to new or existing cases and investigations of crimes that fall within the Secret Service's jurisdiction, including counterfeiting and electronic crimes. The data entered into FIRS consists of the personally identifiable information (PII), including names, dates of birth, aliases, and Social Security numbers (SSN), related to the subjects of criminal investigations and to USSS employees. PII maintained within FIRS falls into one the following categories: Criminal Services, Investigative Services, and Protective Services.

- The Criminal Services category contains information such as case numbers that are linked to a name(s) involved in criminal or informant-related investigations, polygraph results, cybercrime information, forensic reports, seized evidence, and

[1] The Application Provisioning System (APS) is a three tiered software design/architecture focused on ingesting, processing, and analyzing raw data that is collected from various USSS investigative and protective data sources.

warrant information.

- The Investigative Services category contains information used to investigate new or existing cases, such as case numbers, banking/credit card information related to electronic crimes, seized evidence, forged checks or bonds that have signatures, information pertaining to informants such as arrests records, images from cameras, and wiretap recordings.
- The Protective Services category contains basic special agent information such as: training; agent assignment tracking; and trip details, such as lodging, trip location, and financial reimbursements.

Reason for the PIA Update

DHS is updating the FIRS PIA to reflect changes to the operational environment, including the removal of the Comprehensive Incident Database on Targeted Violence (CID-TV) tool, the update of Flipbook, and the renaming of Wireless Tracking Reporting (WTR).

During the development of CID-TV, a tool used in the research of past incidents of targeted violence directed toward public officials, public figures, and prominent facilities, structures, and events, USSS intended to migrate its functionality into FIRS. However, due to funding and system development issues, that integration never occurred. Therefore, coverage for the CID-TV system is no longer provided under the FIRS PIA. USSS will be documenting CID-TV in a separate PIA.

The Flipbook application, used to facilitate the collection of data to conduct analysis of risk associated with protectee protection, is undergoing a redesign, with an anticipated testing and release date in late 2017. Flipbook was originally coded using a framework called Richfaces 3.x, which reached its End of Life support (EOL) in June 2016. USSS is in the process of upgrading all of its primary tools to a more current and supported framework called Primefaces 5.x. The new framework will allow USSS to standardize its application development process across the board, provide the same “look and feel” for all of its applications, and provide enhanced capabilities to the developers and users. The move to this new framework does not impact the level of PII collected in any way.

Though the function of the WTR application remains the same, it was renamed Mobile Wireless Reporting (MWR). The change was designed to alleviate concerns that wireless devices were consistently being tracked or monitored. MWR continues to provide USSS personnel with the ability to capture data for the wireless phone tracking of targets, including missions carried out to support broader Secret Service investigations.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

There are no changes in the specific legal authorities and agreements that permit and define the collection of information in FIRS.

Characterization of the Information

FIRS collects the following information in the Criminal, Investigative, and/or the Protective Services categories:

- Full Name (Collected/Retained)
- Addresses (Collected/Retained)
- Phone Numbers (Collected/Retained)
- Email Addresses (Collected/Retained)

Criminal and Investigative Services only:

- Alias/A/K/A (Collected/Retained)
- SSN/ Tax Identification Number (TIN) (Collected/Retained)
- Date Of Birth (DOB) (Collected/Retained)
- Physical Descriptions/ Identifiers (Height, Weight, Sex, etc.) (Collected/Retained)
- Vehicle Descriptions (Make, Model, License Plate) (Collected/Retained)
- Physical Characteristics/Identifying Marks & Disfigurements (Collected/Retained)

The information in the system is collected directly from individuals as part of an investigation or indirectly through the investigation of individuals. With the removal of CID-TV

from the FIRS system, information is no longer collected from commercial sources or publicly available data.

Investigators check the information for accuracy during the course of the investigation process, and again when the information is entered into FIRS. Additional checks are conducted by Field Office supervisors, Field Office administrative personnel, and the Criminal Investigative Division. Automated checks are embedded into the tools to ensure accuracy of the data.

Uses of the Information

There are no changes in the uses of the information.

Data Retention by the Project

There are no changes to the data retention schedule for this system. The Secret Service continues to retain the information no longer than is useful or appropriate for carrying out the information dissemination, collection, or investigation purposes for which it was originally collected. Information that is collected and becomes part of an investigative case file will be retained for a period that corresponds to the specific case type developed (e.g., 30 years for judicial criminal cases, 10 years for non-judicial criminal cases, and 5 years for non-criminal cases). Case files involving crimes that have no statute of limitations (e.g., murder) may be retained indefinitely. Information that is derived or received from another law enforcement agency may have specialized retention requirements based upon equities established by the originating agency. Relevant retention schedule numbers are: N1-087-89-002 and N1-087-92-002. Also there is a pending DHS Enterprise Schedule for the Investigative Retention Schedules being approved by National Archives and Records Administration which will change some of the retention periods..

Information collected that does not become part of an investigative case file, per existing retention schedules established and approved by the National Archives and Record Administration (NARA), may be destroyed/deleted when no longer needed for administrative, legal, or audit purposes. Understanding that the time frames associated with such purposes can vary widely (e.g., a backup of a database that is overwritten on a nightly basis, versus a litigation-related preservation order that may remain in effect indefinitely), it is not practical to assign a specific retention period to this type of data

Privacy Risk: There is a risk that information will be kept in FIRS for longer than necessary.

Mitigation: This risk is partially mitigated. USSS provides records retention training to all system users and periodically audits the system. The information in FIRS will be retained for the

timeframes outlined in Section 5.1 consistent with general law enforcement system retention schedules and necessary to complete the Secret Service's mission

Information Sharing

Information maintained in FIRS may be shared outside of DHS with other federal, state, local, and foreign agencies for law enforcement purposes on a case-by-case basis. Any information shared from FIRS to external law enforcement entities would occur under existing agreements. Such sharing will take place only after USSS determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions in accordance with the purposes and routine uses specified in the Secret Service's DHS/USSS-001 Criminal Investigation Information System System of Record Notice (SORN), 76 FR 49497[2], in support of the Secret Service mission.

For example, investigation information may be routinely shared with the Department of Justice's Drug Enforcement Agency's International Organized Crime Intelligence and Operations Center (DOJ DEA IOC2) for purposes of prosecution or other law enforcement purposes. To the extent that information may be released pursuant to any routine uses, such release may be made only if it is compatible with the purpose of the original collection, as determined on a case-by-case basis.

Information maintained in FIRS is shared with recipients listed in the DHS/USSS-001 Criminal Investigation Information System SORN who have a need-to-know in the performance of their official duties. Security warnings requiring that the information be kept in law enforcement channels are orally reinforced during telephone calls. Additionally, the USSS routinely marks its investigative documents as "law enforcement sensitive (LES) - not for further dissemination without permission."

By policy and user training, users are instructed to record any disclosure of information outside of DHS by noting the disclosure. FIRS includes a disclosure reminder. USSS policy requires that users of FIRS document the dissemination of information obtained from FIRS in their memorandum of record.

Privacy Risk: There is a risk that information will be shared inappropriately by an external agency, beyond those individuals and entities that have a need to know.

Mitigation: This risk is mitigated through the integration of administrative, technical, and

[2] *See* DHS/USSS-001 Criminal Investigation Information System (Dec. 19, 2008), *available at* https://www.regulations.gov/document?D=DHS-2008-0163-0001

physical security controls that protect PII against unauthorized disclosure. Disclosure may only be made by authorized Secret Service employees engaged in criminal investigation activities who are trained in the use of FIRS. Authorized Secret Service users of FIRS may only share the data with recipients who have a need-to-know, as outlined in the Routine Use portion of the SORN.

Redress

Access, redress, and correction have not changed with this update.

Auditing and Accountability

All necessary measures are in place to ensure that the information stored within FIRS is used in accordance with the stated practices in this PIA update. USSS audits FIRS regularly to ensure appropriate use and access to information across the various tools that comprise it. There are also technical safeguards, such as the requirement that users have a valid approved user identification and password, as well as process safeguards, such as the requirement that the FIRS ISO review and approve the roles and access levels of all users.

A prospective FIRS user requests an account through the completion and submission of the system request form to the Account Manager. The FIRS ISO determines the prospective user's roles and accessibility options for the system prior to the account being created. The ISO approves or rejects the request, depending upon whether the appropriate criteria for role creation are met. If the ISO approves the role request for the user, the ISO sends an email to the FIRS Administrator to set up the FIRS account for the user. If the FIRS ISO denies the request, an email stating the denial will be sent to the prospective user and the FIRS ISO will obtain additional information about the necessity of the access role. Upon the ISO's final approval, the FIRS Administrator grants the appropriate role to the user. Following this, the FIRS Administrator sends an email back to the user notifying him/her that the request was approved and that account set up was completed. The FIRS Administrator is able to view, assign, add, and delete roles for specific user accounts, though any changes to user accounts must be approved by the FIRS ISO.

All USSS employees are required to receive annual privacy and security training to ensure their understanding of proper handling and securing of PII. DHS has published the "Handbook for Safeguarding Sensitive PII," providing employees and contractors with additional guidance. System administration training is provided by the FIRS Information System Owner. In addition, Privileged User Training is provided by the USSS Chief Information Security Officer through the intranet.

DHS physical and information security policies dictate who may access USSS computers

and filing systems. Specifically, DHS Management Directive 4300A outlines information technology procedures for granting access to USSS computers. Access to the information is strictly limited by access controls to those who required it for completion of their official duties. It is not anticipated that FIRS will be utilized by other DHS components or external entities. Such a change would trigger an update to this PIA.

All information sharing agreements, MOUs, and new uses of information are reviewed by the USSS Privacy Office, Office of Chief Counsel, and the respective program offices.

Responsible Official

Deputy Assistant Director
Office of Investigations
United States Secret Service
Department of Homeland Security

Approval Signature

_____

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