Privacy Impact Assessment
for the

Field Support System

(FSS)

DHS/USSS/PIA-014(a)

May 8, 2017

Contact Point
Michael Breslin
Deputy Assistant Director
Office of Investigation
U.S. Secret Service
(202) 406-5729

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) uses the Field Support System (FSS) to support both investigative and protective functions of field operations. FSS is a combination of toolsets residing on a secure network in order to provide users with virtual environments that are used to further USSS operational activities, such as the investigation of financial crimes, cyber-crimes, and potential threats toward individuals and events under Secret Service protection. This Privacy Impact Assessment (PIA) is being updated to reflect the following changes to the operational environment: the removal of the SafeCraker and Cyber Shield toolsets; and the addition of Customer Proprietary Network Information (CPNI) and eInformation Network (eIN).

In addition, the FSS was part of the Criminal Investigative Division Suite (CIDS) System but is currently undergoing its own security authorization under the USSS Criminal Investigative Technology (CIT) Program.

Overview

Managed by the Office of Investigations, Field Support System (FSS) is a system that supports the Criminal Investigation Technology (CIT) Program and field personnel by providing access to certain information to further the dual mission of the United States Secret Service (Secret Service or USSS). FSS resides on the Secret Service network and is supported and maintained at the Rowley Training Center (RTC).

FSS is a system specifically designed to host unique "operations-oriented" missions within a virtual environment based on specific requirements. Authorized personnel access the FSS environment using Federal Information Processing (FIPS) -approved encryption[1] when appropriate and are authenticated into designated authorized environments. This access allows field personnel to operate in a secure environment that is customizable to meet most mission requirement needs.

FSS provides a unified, secure, and autonomous hosting environment in which the Secret Service can deploy mission-required capabilities deemed inappropriate for traditional secure networks due to access, connectivity, or security constraints. Operations of this nature include those that possess one or more of the following requirements:

- Operations connected to government or non-government systems that are not wholly owned and operated by the Secret Service.

[1] *See* DHS 4300A Sensitive System Handbook 5.5.1 Encryption, *available at* https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_4300a_policy_v8.pdf.

- Operations that communicate in a manner that is prohibited on most Secret Service networks (*e.g.*, operations that require content delivery over encrypted mobile broadband).
- Operations providing a common operating environment to other federal, state, local or international law enforcement partners or designee providing real time material support to the Secret Service.
- Operations that collect or produce an inherently dangerous artifact that must be handled with extreme caution (*e.g.*, malware collection, forensics operations).

As a General Support System (GSS), FSS is UNCLASSIFIED/LAW ENFORCEMENT SENSITIVE and is uniquely and purposely designed to exist outside of the perimeter of the USSS enterprise architecture. FSS contains tools and technical field operations that are mission-essential/critical.

As part of the FSS business flow, it is divided into the following categories: Criminal Services, Investigative Services, and Protective Services. Each category collects personally identifiable information (PII).

- The Criminal Services category contains information about suspects, such as names, addresses, phone numbers, Social Security numbers (SSN), and dates of birth (DOB).
- The Investigative Services category contains information used to support court orders or warrants, conduct video surveillance, make audio recordings, and collect Internet Protocol (IP) addresses, mobile phone numbers, and email addresses.
- The Protective Services category contains the names and contact information of law enforcement officers and other officials, as well as USSS field office partners involved in protective operations.

FSS now includes three tool sets that previously fell under separate system boundaries - CPNI, eIN, and Intercept Platform - to meet mission requirements. The SafeCraker and Cyber Shield toolsets have been decommissioned due to their outdated functionality and lack of supportability.

Reason for the PIA Update

The FSS PIA is being updated to reflect the removal of the SafeCraker and Cyber Shield toolsets from the operational environment, and the addition of CPNI and eIN. The SafeCraker and Cyber Shield toolsets are obsolete, and the toolsets are no longer capable of meeting operational needs and requirements due to their lack of capability, performance, and supportability.

Customer Proprietary Network Information (CPNI):

The CPNI Reporting website serves as a mechanism for telecommunications carriers to report to law enforcement a breach of customer proprietary network information (CPNI). The Federal Communications Commission requires telecommunication carriers report CPNI data breaches electronically to the USSS and Federal Bureau of Investigation (FBI) through a "central reporting facility," in accordance with 47 C.F.R. 64.2011.[2] The CPNI reporting website fulfills that function.

CPNI is the data collected by telecommunications corporations about a consumer's telephone calls.[3] It includes the time, date, duration, and destination number of each call; the type of network to which a consumer subscribes; and any other information that appears on the consumer's telephone bill. If a carrier submits a report of CPNI breach to the CPNI Reporting website, the carrier is asked to provide the name, telephone number, and email address of a contact person for that carrier. The website does not ask for or require a personal (non-business) telephone number or email address. In addition, the website specifically advises individuals against including any CPNI data in their reports. USSS uses CPNI to determine if the data breach meets investigative thresholds to warrant an investigation.

The information collected from the carrier is simultaneously sent to the appropriate division of the USSS and the FBI. The information collected consists of the name of the contact person submitting the CPNI report for the telecommunications carrier, job title, work telephone number, work email address, business address, branch address, and incident location. CPNI does not include subscriber information, i.e., it does not include subscriber name, SSN, address. Once an investigation is started by either the USSS or the FBI, each agency may share resulting information with the other.

eInformation Network (eIN):

The eIN is comprised of multiple web, database, and application servers. The eIN allows trusted users to search the websites and databases for information related to financial crimes. It provides authorized USSS personnel, law enforcement agencies, and financial institutions with a centralized repository of data on counterfeit checks, notes, documents, skimming, fictitious instruments, and bank/credit card fraud and loss information against which information can be cross-referenced to determine if further investigation is warranted.

Due to the closing of a Secret Service datacenter, the cost of support and maintenance of both CPNI and eIN are being absorbed into the FSS infrastructure. They are closely coupled and

[2] *See* 47 C.F.R. 64.2011, *available at* https://www.gpo.gov/fdsys/pkg/CFR-2010-title47-vol3/pdf/CFR-2010-title47-vol3-sec64-2011.pdf.
[3] A statutory definition of CPNI can be found at 47 U.S.C. § 222 (h)(1), *available at* https://www.gpo.gov/fdsys/pkg/USCODE-2009-title47/pdf/USCODE-2009-title47-chap5-subchapII-partI-sec222.pdf.

functionally aligned with other toolsets within FSS, allowing Secret Service to provide direct oversight, support, and maintenance at a significant cost savings to the Government.

Intercept Platform

During the course of an investigation, USSS may have a court order or warrant to conduct electronic surveillance or real-time audio interception. Intercept Platform permits USSS personnel to intercept and locate wireless transmissions. Intercept Platform provides a way to preserve PII and collect video images through real-time monitoring. Intercept Platform provides the capability to collect and analyze the following:

- Telephone information from both hardline and cell site simulators,[4] domestically and internationally; including the subscriber information of both the initiator and receiver, as well as the locations of the parties and the voice conversations.
- Internet packets in transit from one host to another, along with the header information and the route of transit. These packets contain payload data such as email messages, chats, documents, and pictures.
- Video surveillance of people, places, and things.

Privacy Impact Analysis

Authorities and Other Requirements

There are no changes in the specific legal authorities and/or agreements that permit and define the collection of information in FSS, other than the CPNI Reporting website citation, 47 C.F.R. 2011, which augments the prior USSS authority to investigate data breaches set forth in 18 U.S.C. § 1030.[5]

Characterization of the Information

FSS collects and retains the following PII:

CPNI:

- Telecommunications carrier;
- Job title;
- Telephone number;

[4] *See* DHS Policy Directive 047-02: Department Policy Regarding the Use of Cell-Site Simulator Technology (October 19, 2015), *available at* https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf.

[5] *See* 18 U.S.C. § 1030, *available at* https://www.gpo.gov/fdsys/pkg/USCODE-2010-title18/pdf/USCODE-2010-title18-partI-chap47-sec1030.pdf.

- Work email address;
- Business address;
- Branch address; and
- Incident location.

eIN:

- Full name;
- Date of Birth;
- Gender;
- Country of birth;
- Email address;
- SSN or Passport Number and Country;
- City and state of residence/visit location;
- Job function;
- Weapon carrier status;
- Driver's license number;
- State criminal ID number;
- Alien number; and
- Other identifying number or Arrest record.

Intercept Platform:

- Telephone Number;
- Address;
- Internet Protocol (IP);
- Video Feeds such as images of subjects/suspects, activities, and other visual information;
- Live and recorded audio;
- Live and recorded images;
- Text messages;
- Phone Conversations; and

- Location of wireless transmission.

The information maintained in FSS is checked for accuracy by investigators and system audit controls during the course of the investigative process (for the Criminal and Investigative Services categories) and again when the information is entered into FSS. Operational Administrators (OA) and the FSS Administrator (FSSA) conduct additional checks for accuracy. USSS also ensures accuracy though automated checks embedded into the tools.

The sources of the information are as follows:

CPNI: Information is collected directly from individual employees of the carrier submitting the CPNI Report.

eIN: The eIN allows trusted users to search for information related to U.S. counterfeit currency in which the source of information comes directly from the U.S. Secret Service's internal databases and information related to credit card issuers comes directly from Visa, MasterCard, American Express, and Discover.

Intercept Platform: PII is collected from traditional voice communications systems (telephonic, wireless, etc.); live and recorded audio; live and recorded images; and IP based data networks such as the Internet. The information is obtained pursuant to a court order or warrant.

Uses of the Information

CPNI: USSS uses CPNI to determine if the reported data breaches meet the investigative threshold to warrant a full investigation.

eIN: The eIN is comprised of multiple web, database, and application servers that are used to provide a solution to facilitate the sharing and receiving of information to and from USSS business partners (i.e., federal, state, and local law enforcement entities, banking institutions, and other sources within the public and private sector). The eIN allows trusted users to search for information related to U.S. counterfeit currency. Users can submit a request form to forward U.S. counterfeit currency to the Secret Service for detection or retention. Additionally, users can search and obtain security points of contact relating to credit card issuers.

Intercept Platform: The Intercept Platform toolset is used to detect and respond to illegal activities in real time. The toolset intercepts oral, wire, and electronic communications such as phone conversations and emails. It is used to reveal the location of the subject. The images from the video feeds are used to identify subjects or suspects. USSS uses PII obtained from the Intercept Platform toolset to obtain situational awareness of network vulnerabilities, threats, malicious network activities, and patterns of criminal activity. USSS also uses Intercept Platform PII for purposes of prosecution or other law enforcement.

Notice

Notice remains unchanged with this update. The DHS/USSS-001 Criminal Investigation Information System System of Records Notice (SORN), 76 FR 49497,[6] (August 10, 2011), and DHS/USSS-004 Protection Information System SORN, 73 FR 77733 (December 19, 2008),[7] provide notice regarding the collection of information and the routine uses associated with the collection of the information. Notice to individuals prior to collection of information could impede law enforcement investigations.

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 case). 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[8] and N1-087-92-002.[9] However, a new DHS Enterprise Schedule designed to standardize retention of investigative records across the Department and its Components is currently pending review by the National Archives and Records Administration (NARA) that may change some of the retention periods, once approved and issued.

Information collected that does not become part of an investigative case file, per existing retention schedules established and approved by NARA, may be destroyed or 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. However, it should be understood that the Secret Service has no interest in preserving such information any

---

[6] *See* DHS/USSS-001 Criminal Investigation Information, 76 FR 49497 (August 10, 2011), *available at* https://www.gpo.gov/fdsys/pkg/FR-2011-08-10/html/2011-20226.htm.
[7] *See* DHS/USSS-004 Protection Information System, 76 FR 66940 (October 28, 2011), *available at* https://www.gpo.gov/fdsys/pkg/FR-2011-10-28/html/2011-27883.htm.
[8] *See* N1-087-89-002, *available at* https://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0087/n1-087-89-002_sf115.pdf.
[9] *See* N1-087-92-002, *available at* https://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0087/n1-087-92-002_sf115.pdf.

longer than is absolutely necessary.

Privacy Risk: There is a privacy risk that information will be kept in FSS 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 FSS will be retained for the timeframes outlined in this section consistent with general law enforcement system retention schedules and as necessary to complete the Secret Service's mission.

Information Sharing

Information maintained in FSS may be shared outside of DHS with other federal, state, local, and foreign agencies for law enforcement purposes on a case-by-case basis pursuant to the routine uses specified in the applicable SORNs. Such sharing will take place only after Secret Service 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 SORN, 76 FR 49497[10] and DHS/USSS-004 Protection Information System SORN, 76 FR 66940[11] in support of the Secret Service mission.

Information maintained in FSS is shared with recipients in accordance with the routine uses listed in the DHS/USSS-001 Criminal Investigation Information System SORN and DHS/USSS-004 Protection 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 through training, users are instructed to record any disclosure of information outside of DHS by noting the disclosure. USSS policy requires that specified users of FSS document the dissemination of information obtained from FSS in their memorandum of record. Additionally, FSS includes a disclosure reminder to help ensure that the necessary documentation occurs.

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 physical security controls that protect PII against unauthorized disclosure. Disclosure may be

[10] *See* DHS/USSS-001 Criminal Investigation Information, 76 FR 49497 (August 10, 2011), *available at* https://www.gpo.gov/fdsys/pkg/FR-2011-08-10/html/2011-20226.htm.
[11] *See* DHS/USSS-004 Protection Information System, 76 FR 66940 (October 28, 2011), *available at* https://www.gpo.gov/fdsys/pkg/FR-2011-10-28/html/2011-27883.htm.

made by authorized Secret Service employees engaged in criminal investigation, non-criminal investigation, and protective activities who are trained in the use of FSS. Authorized Secret Service users of FSS may only share the data with recipients who have a need-to-know, as outlined in the Routine Use portion of the DHS/USSS-001 Criminal Investigation Information System SORN and DHS/USSS-004 Protection Information System SORN.

Redress

Redress may be available by making a written request to the Secret Service Freedom of Information Act (FOIA) Officer. However, as noted in DHS/USSS-001 Criminal Investigative Information System SORN, 76 FR 49497, and DHS/USSS-004 Protection Information System SORN, 73 FR 77733, the system of records is exempt from the Privacy Act's (PA) access and amendment provisions; therefore, record access and amendment may not be available in all instances, for all individuals, and determinations may be made on a case-by-case basis. Requests should be directed to Communications Center, FOIA/PA Officer, 245 Murray Lane, S.W., Building T-5, Washington, D.C. 20223.

Auditing and Accountability

All necessary measures are in place to ensure that the information stored within FSS is used in accordance with the stated practices in this PIA update. FSS is audited 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 Tool Administrators (TA), OA, or FSSA review and approve the roles and access levels of all users.

A prospective FSS user requests an account through the completion and submission of a request to the TA, OA, and/or FSSA. The TA, OA, and/or FSSA determines the prospective user's roles and accessibility options for the system prior to the account being created. The TA, OA, and/or FSSA approves or rejects a request, depending upon whether the appropriate criteria for role creation are met. The TA, OA, and/or FSSA are able to view, assign, add, and delete roles for specific user accounts, though any changes to user accounts must be approved by the system owner.

All USSS employees are required to receive annual privacy and security training to ensure their understanding of proper methods for handling and securing of PII. Department of Homeland Security (DHS) has published the "Handbook for Safeguarding Sensitive PII," providing employees and with contractors additional guidance. Additionally, system administration training is provided by the FSS Information System Owner, and 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 require it for the completion of their official duties. It is not anticipated that FSS 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 Officials

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

Latita Payne
Privacy Office
United States Secret Service
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

_____

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