Privacy Impact Assessment
for the

Field Support System

(FSS)

DHS/USSS/PIA-014

October 18, 2013

Contact Point

U.S. Secret Service
Office of Investigations (INV)
Criminal Investigative Division (CID)
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) uses the Field Support System (FSS) for ongoing investigations into criminal activity. FSS is a combination of three programs which detect criminal activity and collect evidence in ongoing investigative cases ranging from financial crimes, cyber-crimes, and potential threats toward individuals and events under Secret Service protection. This Privacy Impact Assessment (PIA) is being conducted because the FSS collects personally identifiable information (PII).

Overview

FSS is a separate but supported subsystem of the Criminal Investigation Division Suites (CIDS). FSS is managed by the Office of Investigations and supports field personnel by providing access to certain electronic communications and evidence necessary to further criminal investigations. FSS resides on internal and external networks of the Secret Service. The programs on FSS are as follows:

- SafeCraker: During the course of an investigation, the Secret Service may in some circumstances lawfully confiscate and review electronic media from subjects or suspects pursuant to a court order and/or warrant. When the media is encrypted and/or password protected, SafeCraker allows Secret Service personnel to recover the encrypted files. SafeCraker runs a program that unlocks the device by running a series of numbers until the right combination is found. SafeCraker also unlocks email accounts. SafeCraker harnesses the combined idle processing power of the central processing units of authorized computers across secure Secret Service networks and other trusted networks. SafeCraker sends a lock to these computers, along with a block of combination variations. Once a computer exhausts the block, SafeCraker sends another block until the encryption is broken and the device is unlocked. The password is obtained once the encryption is unlocked. The password is then used to open the container that stores the data.
- Intercept Platform: During the course of an investigation the 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:
    1) Telephone information from both hardline and mobile wireless, domestically and internationally. This includes subscriber information of both the initiator and receiver, the locations of the parties, and the voice conversations.
    2) 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.
    3) Video surveillance of people, places and things.

- Cyber Shield: Cyber Shield is used to detect criminal activity on the Internet and identify subjects/suspects. Cyber Shield provides a way to investigate certain electronic discussions, transactions, and other activities on the Internet that could 1) pose a threat to individuals and events under Secret Service protection; 2) utilize schemes to exploit vulnerabilities within computer networks; 3) harm individual consumers; or 4) damage the economy of the United States. Users consent to monitoring when accessing Cyber Shield sites, consistent with 18 U.S.C. § 2511(2)(c) - Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

Investigative and Protection information is solicited and obtained under the authority of the Federal Records Act (44 U.S.C. § 3101) and implementing regulations (Title 36, Code of Federal Regulations, chapter XII). Information is collected in conjunction with the following types of criminal investigations: financial, counterfeit, and cyber-crimes. Such investigations are authorized by 18 U.S.C. §§ 3056 - Powers, Authorities, and Duties of United States Secret Service; 1029 - Fraud and Related Activity in Connection with Access Devices; 1030 - Fraud and Related Activity in Connection with Computers; 3121 – General prohibition on pen register and trap and trace device use; and 2510-2522 -- the Wire and Electronic Communications Interception and Interception of Oral Communications and Title III of the Omnibus Crime Control and Safe Streets Act of 1968 as amended by the electronic Communications Privacy Act (ECPA) (Pub. L. 99-508; 10/21/86).

1.2 What Privacy Act Systems of Records Notice(s) (SORN(s)) apply to the information?

The DHS/USSS-001 Criminal Investigation Information System SORN, 76 FR 49497 (August 10, 2011), and DHS/USSS – 004 Protection Information System SORN, 73 FR 77733 (December 19, 2008), provide notice regarding the collection of PII and the routine uses associated with the collection of the PII.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

FSS is a separate but supported subsystem of the CIDS. The certification and accreditation for CIDS was completed on August 22, 2012, and expires on August 22, 2015. The Certification & Accreditation of Intercept Platform and Cyber Shield is pending approval of this PIA. SafeCraker is covered by its respective Authority to Operate (ATO) which was granted on August 22, 2012.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

A records retention schedule is currently being developed to be submitted for approval to NARA.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

This information is not covered by the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

SafeCraker: The following information is obtained once the encryption is unlocked by SafeCraker:

- Username;
- Password;
- IP address;
- Browser history;
- Photos;
- Contacts;
- Voicemails;
- Text messages;
- Email messages;
- Video files;
- Audio files;
- Personal calendars;
- Word processing documents;
- Spreadsheets;
- Applications;
- Call logs;
- Deleted files;
- Cached pages;
- Cookie data; and
- Instant messenger chat and client logs.

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.

Cyber Shield:

- Username;
- Password;
- IP address from account registration;
- Stolen debit/credit card information;
- Stolen bank account information;
- Stolen personal identification numbers;
- False identity documents; and
- Content of web forums.

2.2 What are the sources of the information and how is the information collected for the project?

SafeCraker: The PII is collected from lawfully obtained electronic devices (computers, servers, thumb drives, cell phones, etc.) of individuals under criminal investigation. The information is gained based on a court order and/or warrant using computer forensics to reveal usernames and passwords. Once the agent gains access to the content of the electronic media, the content is analyzed and collected as evidence in a criminal case.

Intercept Platform: The 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 using court order and/or warrant.

Cyber Shield: The PII is collected consensually from users who enter it onto a server that is managed, hosted and monitored by the USSS. Cyber Shield provides users with unified communications services such as email, instant messaging, and video sharing.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No.

2.4 Discuss how accuracy of the data is ensured.

In the instances when a court order and/or warrant is issued for the collection of PII, a validation check is conducted pre-collection, during-collection, and post-collection. Before collection, a pre-check is initiated to make sure the collection tools are configured in accordance with the court order, consent document or memorandum of understanding. When collection begins, another check is conducted to validate that the collection is properly obtaining the authorized information. USSS personnel frequently re-check the validity of the process during collection. If, at any time, the collection process deviates from the initial authorized protocols, the collection process is immediately terminated, an analysis is conducted

on the cause, and a re-initiated collection is conducted. At the conclusion of the collection process, another check is conducted to validate the collected information.

Cyber Shield collects data entered by the users themselves, helping to assure the data entered is accurate. Intercept Platform collects real-time audio and video of activities occurring in places where agents have lawful access. Intercept Platform records only what is occurring in real-time. There is no editing feature to alter the recorded activities.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that more PII may be collected than is necessary to accomplish the purpose for which the information was originally collected.

Mitigation: The risk is mitigated because data is most often collected by Secret Service agents trained in collecting from various sources only that PII which is necessary and appropriate for investigative purposes, whether that information is obtained from individuals or entities. PII is collected to ensure the user: 1) remains identifiable during their interactions with the agency; 2) is not erroneously identified as, or linked to, another individual; and 3) may be further investigated (if warranted). USSS only uses the data to detect and respond to activities that indicate a reasonable suspicion of unlawful activities or to support law enforcement investigations and prosecutions to the extent that they contain information relevant to a criminal or suspected criminal activity. All other PII is deleted.

Privacy Risk: There is a privacy risk that PII pertaining to individuals who are not targets of Secret Service investigations may be collected.

Mitigation: FSSS collects information using carefully defined parameters, specifically tailored to identify relevant information for official purposes, while also minimizing false positives (i.e., mis-hits or information unrelated to the Secret Service's missions). All information collected at the direction of the Secret Service that is not needed to carry out the Agency's missions is discarded.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

SafeCraker: Once the encryption is unlocked, the password is obtained. The SafeCraker toolset uses the password to open the container that stores the data and access the content of encrypted and/or password protected files. The PII obtained from the decrypted files may be used for purposes of prosecution or other law enforcement.

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/suspects. PII obtained from the use of the Intercept Platform toolset is used to obtain situational awareness of network vulnerabilities, threats, malicious network activities, and patterns of criminal activity. PII is also used for purposes of prosecution or other law enforcement.

Cyber Shield: The Cyber Shield toolset uses the PII to identify suspect identities and to track criminal activity. If stolen PII is discovered on the website, Cyber Shield may use the PII to identify victims. The PII may also be used to chart an investigative strategy to track, disrupt and dismantle criminal networks. Analyses of the communications protocols may provide intelligence and investigative leads on criminal targets, including those known to the USSS and new targets for investigation. Additionally, Cyber Shield identifies ongoing and planned criminal schemes, allowing the USSS to disrupt these criminal operations and prevent further crimes. The USSS may disseminate recovered PII to applicable public and private sector organizations to assist in the identification and prevention of crime and the protection of the true owner of the PII when appropriate.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

3.3 Are there other components with assigned roles and responsibilities within the system?

No. There are no other components with assigned roles and responsibilities within the system.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: The privacy risk associated with the uses of the PII is the potential that the information could inaccurately identify lawful behavior as suspicious and form the basis of an investigation.

Mitigation: All Secret Service agents are trained to act upon only that PII which is both credible and necessary in the furtherance of the agency's protective and investigative missions. Access to the PII is limited only to those Secret Service employees who need access to effectively perform their jobs. All Secret Service employees and contractors are trained on the appropriate use of PII.

This risk is also mitigated by users reviewing PII against the court order or warrant if applicable. To the extent FSS collects information describing the exercise of an individual's First Amendment rights, it must be relevant to an authorized Secret Service law enforcement activity and, as such, permitted by the Privacy Act. To the extent such information is not relevant to a Secret Service law enforcement activity; it is deleted as noted in Section 5.1.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

The DHS/USSS-001 Criminal Investigation Information System SORN, 76 FR 49497, (August

10, 2011), and DHS/USSS – 004 Protection Information System SORN, 73 FR 77733 (December 19, 2008), 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.

All users accessing Cyber Shield must agree to Terms of Service at registration (and on each successive login), which include monitoring of activity by Cyber Shield. The Terms of Service are the result of collaboration with the Department of Justice, Computer Crimes and Intellectual Property Section, but do not state that Cyber Shield is managed by a U.S. Government agency. When a user accepts the Terms of Service, which are displayed on the login screen, they agree to rules of online behavior and are informed that using the service indicates consent to have their Cyber Shield communications monitored. As a result, the monitoring is consensual, pursuant to 18 U.S.C. § 2511(2)(c) - Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Individuals provide their information voluntarily. Prior to registration, and at each login, Cyber Shield users are provided a Terms of Service agreement that includes the user's consent to monitoring. If the user's media is obtained by USSS, users are asked to complete Standard Form 1922, Consent to Search. User information may also be obtained through other lawful means (e.g., search warrant) that do not require consent. Under some circumstances, individuals cannot decline to provide information (e.g., court order, search warrant). Information obtained during the course of an investigation is maintained in accordance with law enforcement retention rules and policies. Information collected and maintained on individuals is subject to the Privacy Act and the Freedom of Information Act.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: In cases where consent is not requested, there is a risk that subjects of an investigation may not know that information about them is being collected and maintained.

Mitigation: The DHS/USSS-001 Criminal Investigation Information System SORN, 76 FR 49497 (August 10, 2011), and DHS/USSS – 004 Protection Information System SORN, 73 FR 77733 (December 19, 2008), provide general notice of the purpose of collection, redress procedures, and the routine uses associated with the collection of the information.

This PIA provides similar notice to the general public as to the collection and use of information for this purpose. Advanced notice of the collection of information to investigative targets or others involved in the investigation generally is not provided as it would compromise ongoing law enforcement investigations.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

FSS stores and retains PII. The Secret Service retains the information no longer than is useful or appropriate for carrying out the investigation for which it was originally collected. Information which is

collected that becomes part of an investigative case file will be retained corresponding to the specific case type (e.g., 30 years for judicial criminal cases; 20 years for judicial protective intelligence records; 10 years for non-judicial criminal cases; 5 years for non-criminal cases, including but not limited to protective intelligence case records). Case files involving crimes which have no statute of limitations (e.g., murder) may be retained indefinitely. Information which is derived or received from another law enforcement agency may have specialized retention requirements based upon conditions established by the originating agency. (For example, any case file containing Protected Internal Revenue Service Information has a minimum 8-year retention period.)

Information which is collected that does not become part of an investigative case file is subject to existing retention schedules established and/or approved by the National Archives and Records Administration (NARA); USSS-held data is destroyed/deleted when no longer needed for administrative, legal, or audit purposes

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: Data may inadvertently be stored for a period longer or shorter than that which is required or necessary.

Mitigation: This risk is mitigated by providing proper records retention training to all system users and periodically auditing the system. The information in FSS 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.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Yes, any information maintained in FSS may be shared in accordance with the purposes and routine uses specified in the Secret Service's System of Records Notices DHS/USSS-001 (Criminal Investigative Information System, 76 FR 49497 and DHS/USSS – 004 Protection Information System SORN, 73 F.R. 77733 in support of the Secret Service investigative mission. For example, investigation information may be routinely shared with the Department of Justice for purposes of prosecution or other law enforcement. Identified information that becomes part of an investigative or criminal case file may be shared on a need-to-know basis with federal, state, and local law enforcement agencies, other foreign and domestic government units, or private entities in accordance with the routine uses outlined in the applicable SORNs.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Any information maintained in FSS may be shared in accordance with the purposes and routine uses specified in the Secret Service's DHS/USSS-001 Criminal Investigative Information System SORN, 76 FR 49497 (August 10, 2011) in support of the Secret Service investigative mission, and DHS/USSS –

004 Protection Information System SORN, 73 FR 77733 (December 19, 2008), in support of the Secret Service's protective mission. 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 purposes of the original collection, as determined on a case-by-case basis.

6.3 Does the project place limitations on re-dissemination?

Yes. When users log on to FSS, they are advised that information obtained from the system should be shared only with those individuals or entities that have an official need to know as part of their official responsibilities and steps should be taken to ensure that the PII contained therein is appropriately safeguarded.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Agency policy requires that users of the system document the dissemination of information obtained from the system in their memorandum of record on the matter.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: To the extent that information may be released pursuant to any routine uses, the privacy risk identified is the disclosure of PII to an unauthorized recipient.

Mitigation: To mitigate this risk, disclosure may be made only by authorized Secret Service employees engaged in criminal investigative activities who are trained on the use of FSS. Authorized Secret Service FSS users may only share the data pursuant to routine uses specified in the Secret Service's DHS/USSS-001 Criminal Investigative Information System SORN, 76 FR 49497 (August 10, 2011), in support of the Secret Service investigative mission, and DHS/USSS – 004 Protection Information System SORN, 73 FR 77733 (December 19, 2008), in support of the Secret Service protective mission.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Access requests should be directed to Communications Center, FOIA/PA Officer, 245 Murray Lane, S.W., Building T-5, Washington, D.C. 20223 and will be considered on a case-by-case basis.

However, as noted in DHS/USSS-001 Criminal Investigative Information System SORN, 76 FR 49497 (August 10, 2011), and DHS/USSS – 004 Protection Information System SORN, 73 FR 77733 (December 19, 2008), the system of records is exempt from the Privacy Act's access and amendment provisions; therefore, record access and amendment may not be available in all cases.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The procedures are the same as those outlined in Question 7.1.

7.3 How does the project notify individuals about the procedures for correcting their information?

The mechanism for requesting correction of information contained in any Secret Service criminal investigation information system and Secret Service protective intelligence information is specified, respectively, in the DHS/USSS-001 Criminal Investigation Information System SORN, 76 FR 49497 (August 10, 2011), and DHS/USSS – 004 Protection Information System SORN, 73 FR 77733 (December 19, 2008), published in the Federal Register. The Secretary of Homeland Security has exempted these systems from the notification, access, and amendment procedures of the Privacy Act because they are law enforcement systems.

However, DHS/USSS will consider individual requests to determine whether or not information may be released. Thus, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the USSS FOIA Officer, 245 Murray Drive SW., Building T-5, Washington, DC 20223.

7.4 Privacy Impact Analysis: Related to Redress

Redress may be available by making a written request to the Secret Service Freedom of Information Officer as described above; however, providing individual access and/or correction of the records may be limited for law enforcement reasons as expressly permitted in the Privacy Act and the DHS/USSS-001 Criminal Investigative Information System SORN, 76 FR 49497 (August 10, 2011) and DHS/USSS – 004 Protection Information System SORN, 73 FR 77733 (December 19, 2008).

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

The system is audited regularly to ensure appropriate use and access to PII. There are also technical safeguards such as the use of client software which is installed on work stations and requires a valid approved user identification and password.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All Secret Service employees and contractors are required to receive annual privacy and security training to ensure their understanding of proper handling and securing of PII. Also, DHS has published the *Handbook for Safeguarding Sensitive PII*, providing employees and contractors additional guidance.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

DHS physical and information security policies dictate who may access Secret Service computers and filing systems. Specifically, DHS Management Directive 4300A outlines information technology procedures for granting access to Secret Service computers. Access to the information is strictly limited by access controls to those who require it for completion of their official duties.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Project review, new sharing agreements, and MOUs are reviewed by subject matter experts, program managers, and appropriate directorate officials. Information sharing occurs in the post-collection phase, after information has already been downloaded.

Responsible Officials

Edward Lowery
Special Agent in Charge
Criminal Investigative Division
U.S. 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