Privacy Impact Assessment
for the

Forensic Services Division System

DHS/USSS/PIA-017

May 9, 2017

Contact Point
Kelli A. Lewis
Forensic Services Division
U.S. Secret Service (USSS)
(202) 406-5274

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

Abstract

The United States Secret Service (USSS or Secret Service) Forensic Services Division System (FSDS) provides the Forensic Services Division (FSD) organization with a suite of tools that facilitate its support of the USSS mission. FSDS tools provide authorized users with resource and case tracking functionalities, an automated handwriting recognition capability, and the ability to capture finger and palm prints. The Secret Service is conducting this Privacy Impact Assessment (PIA) because FSDS collects personally identifiable information (PII) on members of the public.

Overview

The goal of Forensic Services Division (FSD) is to provide timely and accurate forensic examinations of latent print and questioned document evidence, to assist with training and consultation, and to meet visual communications requirements in support of the mission of the United States Secret Service (USSS or Secret Service). The tools that comprise the Forensic Services Division System (FSDS) are the Forensic Services System, Forensic Information System for Handwriting, and Live-Scan. FSDS collects information regarding members of the public, USSS employees, contractors supporting USSS, and employees of other federal agencies. The description of each tool is listed below in greater detail.

- Forensic Services System (FSS) - FSS is composed of the FSD Vault – Case Tracking database. The FSD Vault is a case tracking database that uses Microsoft Access to enter, search, and retrieve cases submitted to FSD for forensic examinations or other examinations submitted in support of the dual investigative and protective mission of the USSS. The entry screen allows personnel to enter tracking information for all evidence that enters the FSD Vault from USSS offices and outside agencies. This system is used primarily by FSD employees, but potentially other USSS employees, who have a valid need to access its resources to perform work-related tasks.
- Forensic Information System for Handwriting (FISH) - The FISH system is an automated archive handwriting recognition system used to search new letters containing threats to USSS protectees or protected facilities/events against previously submitted material. FISH is used by FSD to identify individuals or groups that may pose a risk to USSS protectees or protected facilities/events.
- Live-Scan - The Live-Scan system electronically captures fingerprints and palm prints without using black fingerprint ink. The Live-Scan technology provides a clean, digitized scan of fingerprints and palm prints as well as a collection of biographic information and mug shot images that will be electronically transmitted to the FBI's Next Generation Identification (FBI-NGI) national database for an automated search against over

60,000,000 criminal fingerprint records.[1] The FBI-NGI database is a collection of criminal, applicant, and military fingerprints and palm print records submitted for employment purposes and in conjunction with criminal investigations. Information pertaining to USSS law enforcement officers who carry concealed firearms is also collected by this application for accountability purposes. The Secret Service Live-Scan Program (SSLSP) is an enterprise-wide initiative with 125 Live-Scan booking stations deployed to Secret Service offices throughout the contiguous United States and Alaska, Hawaii, and Puerto Rico, for use in employment and criminal checks. The current Live-Scan booking stations include a single unit consisting of a cabinet, monitor, scanner, computer, keyboard, mouse, signature pad, Uninterruptible Power Supply (UPS/Surge Protector), photo printer, and a printer for fingerprints and palm prints.

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?

The Secret Service is authorized to collect information maintained in FSDS pursuant to 18 U.S.C. § 1029(d), 1030(d), 3056, and 3056A; 5 U.S.C. § 1104 and 9101; Executive Order 9397 (as amended); and 5 C.F.R. Chapter 1, Subchapter B, Parts 731, 732 and 736. Supporting authority includes Pub. L. 92-544 (Title II) and Pub. L. 107-56 (Title II). Supplemental regulatory authority includes 28 CFR 0.85, Part 20, and 50.12.

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

The DHS/USSS-001 Criminal Investigation Information[2], DHS/USSS-003 Non-Criminal Investigation Information[3], and DHS/USSS-004 Protection Information[4] system of records notices (SORN) applies to the collection, use, maintenance, and dissemination of PII by FSDS.

---

[1] *See* Next Generation Identification (NGI) Privacy Impact Analysis, *available at* https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/next-generation-identification-ngi-retention-and-searching-of-noncriminal-justice-fingerprint-submissions.

[2] *See* DHS/USSS-001 Criminal Investigation Information SORN, 76 FR 49497 (August 10, 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-08-10/html/2011-20226.htm.

[3] *See* DHS/USSS-003 Non-Criminal Investigation Information System SORN, 76 FR 66937 (October 28, 2011), *available at* https://www.gpo.gov/fdsys/pkg/FR-2011-10-28/html/2011-27882.htm.

[4] *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.

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

No. The Authority to Operate for FSDS is pending completion of this PIA.

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

Several legacy schedules which apply to FSDS components have been reviewed and approved by NARA. They include N1-087-10-001 (Live-Scan) and N1-087-06-002 (Forensic Information System for Handwriting). N1-87-92-002 also covers several general categories of USSS investigative records.

In addition, a new Department of Homeland Security (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 that may change some of the retention periods, once approved and issued.

In general, the Secret Service retains the information no longer than is useful or appropriate for carrying out the information dissemination, collaboration, or investigation purposes for which it was originally collected. Information collected that becomes part of a case is retained in FSDS for a period that corresponds to the specific case disposition assigned.

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.

The information collected in FSDS is not covered by the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

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

FSDS maintains PII and biographical information for employment and criminal subjects when USSS requires such information to perform its protective and investigative responsibilities. FSDS maintains the following information:

- FSD Vault – Case Tracking Database collects names, case numbers, and case names.
- FISH contains handwritten threatening letters. FISH software links letters together based on handwriting characteristics, thereby consolidating cases for the USSS Protective Intelligence and Assessment Division. The system stores case information such as case number and case name, as well as a suspect name if there is one assigned to the case. The majority of the threatening letters in FISH are of unknown authorship.
- Live-Scan provides a clean, digitized scan of fingerprints, palm prints, and mug shot images. Biographic information may include names, date of birth, addresses, Social Security number (SSN), telephone numbers, e-mail addresses, biometric identifiers, gender, race, and unique identifying numbers. USSS Live-Scan transactions are submitted to FBI-NGI through a secure VPN connection established through U.S. Department of Justice's (DOJ) Joint Automated Booking System (JABS) and Civil Applicant System (CAS). Both connections provide a secure link for transmitting electronic fingerprint and biometric data to the FBI-NGI for search.

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

FSDS collects information regarding members of the public, USSS employees, contractors supporting USSS, and employees of other federal agencies. USSS collects information from law enforcement agencies, to include the USSS, in the course of performing investigative and protective investigations, and in the case of information pertaining to USSS employees and applicants, from law enforcement authorities in support of background investigations. USSS collects information pertaining to USSS law enforcement officers who carry concealed firearms from internal agency records. The Live-Scan system of FSDS collects information directly from the individual (*e.g.*, fingerprint, mug shot, biographic details) while the FSD Vault and FISH systems input information generated by investigative processes.

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

The FSDS system does not use information from commercial or other publicly available data.

2.4 Discuss how accuracy of the data is ensured.

Information is checked for accuracy during the criminal investigative and the adjudication processes, including when possible, the collection of information directly from subject individuals. When collecting information directly from a subject, employee, or employment applicant, the

individual verifies the accuracy of the data input. FSD employees input data into the FSDS based on the information provided by the submitting USSS or outside agency personnel. This information is confirmed at various steps in the FSD process, which may include the FSD Vault personnel, the case examiner, and finally, it is verified by a second qualified case examiner.

Systems are also set up for function testing to ensure the performance of the system is current and accurate. FISH is calibrated each day when a case search is performed using a known case number to ensure the return of expected results. Live-Scan booking station computers contain built-in quality control features to ensure only quality prints are entered into the system.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that inaccurate data may be maintained within the system because FSDS relies heavily on information from other government law enforcement databases, and is generally not the original source of collection.

Mitigation: This risk is partially mitigated. USSS will not take any action unless the information received has been reviewed by USSS employees engaged in protective and investigative activities who have been trained in the interpretation of the information and are familiar with the environment from which the information was collected and used.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

The information collected and maintained within FSDS is used in support of the accomplishment of the Secret Service's dual investigative and protective mission. USSS uses the information collected during investigations to track evidence; identify individuals or groups that may pose a risk to USSS protectees or protected facilities/events; and identify individuals under investigation based upon criminal allegations or in conjunction with employment background investigations.

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.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk that information maintained within FSDS could be used for a purpose inconsistent with that of its original collection, or beyond the scope of the user's mission.

Mitigation: This risk is mitigated through Secret Service's implementation of strict access controls within the system, which is housed on a closed network, as well as the adherence to stringent information management processes. Access to FSDS is only provided to USSS personnel who have a valid need to know the information in order to perform work-related tasks. This ensures that each user has access to only the data for which he/she has a need to know in order to perform his/her protective or investigative responsibilities. Additionally, system and privacy-specific training is provided to Secret Service employees engaged in protective and/or criminal investigation activities to ensure that all individuals with access to data maintained within FSDS are aware of the proper methods for handling information.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

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

The SORNs identified in section 2.1 provide notice regarding the collection of information and the routine uses associated with data maintained within FSDS. Notice to individuals prior to collection of information related to potential criminal activity may not be feasible in that it could

impede law enforcement investigations. Regarding civil matters such as employment checks, notice is provided on the application documents. The final rules for the applicable system of records officially exempt the system from portions of the Privacy Act.

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

Due to the law enforcement nature of this information collection, individuals do not have the right to consent to particular uses of the information in FSDS such as criminal submissions. Persons who are subjects of civil (applicant) checks are aware that their fingerprints have been collected since such persons either voluntarily contribute their fingerprints or consent to being fingerprinted by the processing agency.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not be provided with notice that their information has been collected by the Secret Service and stored in FSDS.

Mitigation: This risk cannot be fully mitigated. In addition to the SORNs cited in section 1.2, which identify the data collected and maintained by this system, as well as the routine uses of that information, this PIA serves as public notice of the existence of FSDS. Beyond this, it is not feasible to provide notice to individuals prior to the collection of information as such notice could impede law enforcement investigations, and would undermine the purpose of FSDS.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

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

Information that becomes part of an investigative case file will be retained for a period that corresponds with the relevant N1-087-89-002 and N1-087-92-002 retention schedules. However, cases maintained due to judicial notice, or those cases involving crimes which have no statute of limitations (*e.g.*, homicides) may be retained indefinitely. Information that is collected but does not become part of an investigative case file, per existing retention schedules established and/or approved by the National Archives and Record Administration, are destroyed/deleted when no longer needed for administrative, legal, or audit purposes.

Information that is derived or received from another law enforcement agency may have specialized retention requirements established by the origination agency, and are subject to the

retention schedules outlined in the SORNs associated with the system from which the information originated.

Currently, the Live-Scan system schedule, N1-087-10-001, describes the controlling FBI protocol: records are retained either until the statute of limitations has been reached for all criminal violations, or after 75 years, whichever is later. Criminal identification records are updated when the FBI records indicate that the individual has reached 99 years of age; civil identification records are deleted when the FBI records indicate the individual has reached 75 years of age. Images may be removed at an early date, provided there is a request by the submitting agency or as a result of a court order specifically stating that the images be removed.

A new DHS Enterprise Schedule designed to standardize retention of investigative records across the Department and its Components is currently pending review by NARA that may change some of the retention periods, once approved and issued.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that information will be retained in FSDS for longer than is required or needed to support the accomplishment of USSS's investigative or protective missions.

Mitigation: This risk is mitigated through the provision of proper records retention training to all system users, as well as through periodic audits of the system. The information in FSDS will be retained for the timeframes outlined in Section 5.1 consistent with general law enforcement system retention schedules and as necessary to complete the Secret Service's mission. The retention period for this system will support the effective enforcement of laws by USSS investigative personnel by ensuring that information pertaining to individuals who are encountered can be identified and linked. Closed cases can contain information that may be relevant to a new or existing/ongoing case, and need to be readily searchable and accessible for the designated period of time.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

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.

FSDS information may be shared with other federal, state, and local law enforcement, and

other domestic or foreign government units, who, by their jurisdictional responsibilities, have a need-to-know to aid in investigative processes. FSDS reports information to external law enforcement partners as part of normal operations when the external agency submits evidence for forensic examination; for example, latent print and/or questioned documents analysis). The FSDS management oversees information sharing in routine operations.

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

Information maintained in FSDS may be shared outside of DHS with other federal, state, local, and foreign agencies for law enforcement purposes on a case-by-case basis to conduct criminal law enforcement investigations and other enforcement activities, to uphold and enforce the law, and to ensure public safety. This external sharing is compatible with the original law enforcement collection in support of the dual mission of the USSS and is consistent with the routine uses contained in the DHS/USSS-001 Criminal Investigation System SORN, DHS/USSS-003 Non-Criminal Investigation Information System SORN, and DHS/USSS-004 Protection Information System SORN. Information is shared pursuant to Memoranda of Understanding (MOU) or through sharing between USSS personnel and other agency personnel, including those law enforcement officials assigned to a joint investigation or with prosecuting agencies. FSDS data will be shared if doing so will further law enforcement efforts conducted by USSS or its law enforcement counterparts, and provided that disclosure is consistent with applicable law and agency policies.

6.3 Does the project place limitations on re-dissemination?

Yes. The information is shared by USSS only upon verification of need-to-know and in conjunction with warnings regarding improper re-dissemination. External law enforcement agencies may have further requirements on re-dissemination of the information received from FSDS systems.

Additionally, the USSS routinely marks sensitive investigative documents as “law enforcement sensitive (LES) – not for further dissemination without permission.”

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

By policy and through training, users are instructed to record any disclosure of information outside of DHS by noting the disclosure. Any disclosure of PII would be referenced in a forensic report or listed in correspondence on official Secret Service letterhead in response to a forensic examination from a law enforcement agency. Correspondence and forensic reports containing PII are maintained in the FSD evidence vault or official correspondence files and are maintained in accordance with applicable USSS records retention policies.

Additionally, all FSDS systems require the use of audit logs which record transactions sent and received from external agencies and departments.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that sensitive information, including PII may be improperly disclosed, used, or further disseminated by the agencies with which USSS shares information.

Mitigation: This risk is mitigated through the limiting of disclosure of information by authorized USSS employees engaged in law enforcement activities who are trained on FSDS systems. Authorized USSS users may only share the data pursuant to routine uses specified in the DHS/USSS-001 Criminal Investigation Information SORN, the DHS/USSS-003 Non-Criminal Investigation Information SORN, and DHS/USSS-004 Protection Information SORN. The Secret Service may share information from FSDS with other federal, state, local, and foreign agencies for law enforcement purposes, and all sharing will be determined on a case-by-case basis. Lastly, USSS includes with any shared information warnings regarding improper re-dissemination, and employs audit logs to record the sharing of all information shared with external agencies and departments.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

Individuals seeking access to any record containing information maintained within FSDS, or seeking to contest the accuracy of its content, may submit a Privacy Act (PA) request to the USSS. Individuals, regardless of citizenship or legal status, may also request access to their records under FOIA. Access requests will be directed to the Secret Service's Freedom of Information Act

(FOIA) Officer, Communications Center (FOIA/PA), 245 Murray Lane, Building T-5, Washington, D.C. 20223. Requests will be processed under both FOIA and PA as appropriate to provide the Requestor with all information that is releasable. Given the nature of the information in FSDS (sensitive law enforcement information), all or some of the requested information may be exempt from correction pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. However, such requests will be considered on a case-by-case basis consistent with law enforcement necessity.

Notwithstanding the applicable exemptions, USSS reviews all such requests on a case-by-case basis. If compliance with a request would not interfere with, or adversely affect the accomplishment of the Secret Service's protective and investigatory mission, information contained within this system may be released or amended. Instructions for filing a FOIA or PA request are available at http://www.dhs.gov/foia.

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 within FSDS are outlined in the SORNs associated with this system, as outlined in section 1.2. Further notice is provided through this PIA.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a privacy risk that an individual may have limited access to his or her information, or the ability to correct that information.

Mitigation: This risk cannot be fully mitigated. Individuals can request access to information about themselves under the FOIA and Privacy Act, and may also request that their information be corrected. The nature of FSDS and the information it collects and maintains is such that the ability of individuals to access or correct their information may be limited through the implementation of exemptions. The redress and access measures offered are appropriate given the purpose of the system, which is to collect, use, and store information concerning individuals who are the subject of criminal and non-criminal investigation and/or may pose a threat to Secret Service protectees. However, requests to amend records will be considered on a case-by-case basis if made in writing to the Secret Service's FOIA/PA Officer.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

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

FSDS has a robust audit trail that logs any action by users and administrators. The FSDS system logs user activity, locks sessions after twenty minutes of inactivity, limits access to only authorized individuals, prevents account access after three unsuccessful login attempts, and warns users that unauthorized, improper use or access to the system may result in disciplinary action as well as civil and criminal penalties. Additionally, all queries and information received are kept in the system log files for audit and quality control purposes. The logs are audited by the system owner.

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

FSDS users receive training on how to use the system by a user's guide. Additionally, FSDS users are required to complete DHS and USSS-mandated annual privacy and security training to ensure their understanding of the proper handling and securing of PII. These users are also trained on the use of the FBI-NGI and the privacy implications associated with the system. Also, DHS has published the "Handbook for Safeguarding Sensitive PII," providing employees and contractors with 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?

FSD protects PII within FSDS by implementing security groups within Microsoft Active Directory. Employees requiring access to FSDS are given permission to access information after written authorization from appointed business owner(s). Only USSS authorized users have access to FSDS systems. All system users are assigned a unique password and user ID. When the system is installed on the employee's computer, specific rights and permissions are granted. The FSDS systems will be accessible using employee's secure and individual credentials.

DHS physical and information security policies dictate who may access USSS computers and filing systems. Specifically, DHS Sensitive Systems Policy Directive 4300A outlines information technology procedures for granting access to Secret Service computers. Access to the system is strictly limited to authorized Secret Service FSD employees who have a legitimate need to know in the furtherance of their role and responsibilities.

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?

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 office.

Responsible Officials

Kelli A. Lewis
Supervisory Physical Scientist
Forensic Services Division
Office of Investigations
U.S. Secret Service
Department of Homeland Security

Latita Payne
Privacy Officer
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.