Privacy Impact Assessment Update
for the

Forensic Services Division System

DHS/USSS/PIA-017(a)

May 8, 2020

Contact Point
Kelli A. Lewis
Forensic Services Division
United States Secret Service
202-406-5274

Reviewing Official
Dena Kozanas
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The United States Secret Service (USSS) Forensic Services Division System (FSDS) provides the Forensic Services Division (FSD) organization with a suite of applications that facilitate its support of the Secret Service mission. FSDS applications provide authorized users with resource and case tracking functionalities, automated handwriting recognition capability, and the ability to capture finger and palm prints. The Secret Service is conducting this Privacy Impact Assessment (PIA) Update to document enhancements to the Live-Scan Application and the addition of three new applications: QualTrax, Mideo CaseWorks, and Laboratory Information Management System (LIMS).

Overview

The mission of Forensic Services Division (FSD) is to support the United States Secret Service (USSS) in the following ways: conduct timely and accurate forensic examinations of latent print and questioned document evidence obtained through standard law enforcement activities, assist with training and consultation, and provide visual communication requirements. The applications that comprise FSDS include: Forensic Services System (FSS), Laboratory Information Management System (LIMS), Forensic Information System for Handwriting (FISH), CaseWorks, QualTrax, and Live-Scan.

Forensic Services System (FSS) - FSS contains the FSD Vault – Case Tracking database. This system is used primarily by FSD employees, but potentially other USSS employees, who have a valid need to access resources on these systems to perform work related tasks.

The FSD Vault is a case tracking database that is used to enter, search, and retrieve cases submitted to FSD for forensic examinations or other examinations submitted in support of the investigative and protective mission of the Secret Service. The entry screen allows personnel to input tracking information for all evidence that enters the FSD Vault from Secret Service offices and outside agencies.

Laboratory Information Management System (LIMS) – LIMS is a comprehensive case management system that integrates evidence tracking, analytical results, reports, and lab management information allowing for a system to track all cases and evidence submitted to FSD for forensic examinations from Secret Service offices and outside agencies.

Forensic Information System for Handwriting (FISH) – The FISH system is an automated archive handwriting recognition system used to search new letters containing threats to Secret Service protected individuals or protected facilities/events against previously submitted material. FISH is used by the FSD to identify individuals or groups that may pose a risk to USSS protected individuals or protected facilities/events.

Mideo CaseWorks – The CaseWorks application is a digital evidence management system for the maintenance and optimization of images and digital evidence. The eLatent Case

Management Module extends the functionality of CaseWorks by providing specialized tools and features for latent print identification documentation and comparative analysis.

QualTrax Compliance Software – QualTrax documents controls through electronic versioning, tracking, approving and escalation. Workflow is automated for more efficient business processes. The application distributes and tracks testing and training tasks, and reports generation of audits, workflow, and training related data.

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 Federal Bureau of Investigation's (FBI) Next Generation Identification (FBI-NGI) national database for an automated search against over 60,000,000 criminal fingerprint records. 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 Secret Service law enforcement officers who carry concealed firearms is also collected by this application for accountability purposes.

There are 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 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.

Reason for the PIA Update

USSS is updating this PIA to document the enhancement to the FSDS system due to the implementation of three new applications since the previous PIA: Mideo CaseWorks, QualTrax Compliance Software, and LIMS. The Live Scan application has also been updated with the removal of legacy servers and replaced with new servers and updated software.

Privacy Impact Analysis

Authorities and Other Requirements

There have been no changes to the collection authorities since the initial publication of the PIA. 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.

Characterization of the Information

FSDS maintains PII and biographical information for employment and criminal subjects when the Secret Service 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. 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 collects 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.

• Mideo CaseWorks collects photographic images and digital document evidence for the purpose of establishing or verifying the identity of an individual and may be added to case notes and reports as a means of identifying an individual and/or to obtain a fingerprint card from the FBI.

• QualTrax Compliance Software is an electronic platform offering collaboration and does not collect, generate, or retain specific information about individuals.

• LIMS is an evidence and case tracking database. The database collects names, case numbers, case names, reports, and results of examinations in criminal investigations.

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. The Secret Service will not take any action unless the information received has been reviewed by Secret Service 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. In the event that incorrect information is discovered in Live-Scan, only the original collector of the information (Field Office User) has read/write privileges and is responsible for correcting information entered in the application. Read/write privileges have been granted to FSD users to update incorrect information discovered in FISH, Mideo CaseWorks, and the FSD Vault Database. LIMS is a case tracking database; any information updated in FSDS applications will be reflected as cases go through the tracking process. QualTrax is a compliance software; any information updated in FSDS applications will be reflected in QualTrax.

Uses of the Information

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

• FSD Vault – Case Tracking Database information is used to track and update criminal case files as the case progress through the process. It has no connections with other USSS systems.

• FISH software links letters together based on handwriting characteristics, thereby consolidating cases for the Secret Service Protective Intelligence and Assessment Division. The majority of the threatening letters in FISH are of unknown authorship. The information collected is used to determine the origin of threat letters, age and type of ink used to write them, and link to existing cases or new case files and case numbers.

• Live-Scan provides a clean, digitized scan of fingerprints, palm prints, and mug shot images, and biographic information. This collection of data is used for criminal investigation as well as employment background checks.

• Mideo CaseWorks is a digital evidence management system for the maintenance and optimization of photographic images and digital document evidence. When latent fingerprints are developed on an evidence item in the FSDS laboratory, they are digitally captured through photography and imported into CaseWorks. The eLatent Case Management Module extends the functionality of CaseWorks by providing specialized tools and features for latent identification documentation and comparative analysis.

• QualTrax Compliance Software is an electronic platform offering collaboration (similar to SharePoint) with version control, tracking, approving and escalation of case files. Workflow is automated for more efficient business processing. The application distributes and tracks testing and training tasks, and reports generation of audits, workflow and training related data.

• LIMS is an evidence and case tracking database used to manage investigations.

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 provided only to Secret Service personnel who have a valid need to know 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 to perform his/her protective or investigative responsibilities. Additionally, system and annual 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.

Notice

There are no changes in the notice provided with this system.

Data Retention by the project

There are no changes to data retention with this system.

Information Sharing

FSDS continues to share information 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. Live-Scan connects to the Department of Justice (DOJ) Joint Automated Booking System (JABS)[1] and Civil Applicant System (CAS)[2] as well as the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS).[3] A Memorandum of Understanding (MOU) between USSS, and the Federal Bureau of Investigation (FBI) component of the DOJ is in place for all interconnections. FSDS has not changed the process however updates have been made to hardware to enhance the process. The three new apps do not have external interconnections. The FSDS management oversees information sharing in routine operations[4] such as through the DOJ CAS.

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

Mitigation: The risk is mitigated through the limiting of disclosure of information by authorized Secret Service employees engaged in law enforcement activities who are trained on FSDS. Authorized Secret Service users may only share the data pursuant to routine uses specified

[1] *See* DOJ Justice Management Division (JMD) The Joint Automated Booking System PIA for more information on this system and the information it collects, uses, and maintains, *available at* https://www.justice.gov/sites/default/files/jmd/legacy/2014/06/27/jabs.pdf.

[2] *See* DOJ Civil Applicant System (CAS) PIA for more information on this system and the information it collects, uses, and maintains, *available at* https://www.justice.gov/sites/default/files/jmd/legacy/2014/04/26/cas_privacy_impact_assessment_sep28.pdf.

[3] *See* DOJ FBI Criminal Justice Information Services (CJIS) PIA for more information on this system and the information it collects, uses, and maintains, *available at* https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments.

[4] *See* DHS/USSS-004 Protection Information System, 76 FR 66940 (October 28, 2011), *available at* https://www.govinfo.gov/content/pkg/FR-2011-10-28/html/2011-27883.htm

in the DHS/USSS-001 Criminal Investigation Information SORN,[5] the DHS/USSS-003 Non-Criminal Investigation Information SORN,[6] and DHS/USSS-004 Protection Information SORN.[7] The Secret Service may share FSDS information with other federal, state, local, and foreign[8] agencies for law enforcement purposes, and all sharing will be determined on a case-by-case basis. Lastly, the Secret Service 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.

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.

Redress

There are no changes to the redress process. Individuals seeking access to any record containing information maintained within FSDS, or seeking to contest the accuracy of its content, may submit a Freedom of Information (FOIA) and/or Privacy Acts (PA) request to the Secret Service. Individuals, regardless of citizenship or legal status, may request access to their records. Access requests will be directed to the Secret Service's Disclosure Officer, Communications Center (FOIA/PA), 245 Murray Lane, Building T-5, Washington, D.C. 20223. Requests will be processed under both FOIA/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 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, Secret Service 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/PA request are available at http://www.dhs.gov/foia.

---

[5] *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.

[6] *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.

[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] The following agencies make up the International Organized Crime Intelligence & Operations Center: U.S. Department of Justice (DOJ), Federal Bureau of Investigation (FBI), U.S. Immigration and Customs Enforcement (ICE), U.S. Department of Homeland Security (DHS), U.S. Drug Enforcement Administration (DEA), Internal Revenue Service (IRS), The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), U.S. Postal Inspection Service, U.S. Department of State, U.S. Department of Labor (DOL), U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN) and International Criminal Police Organization (INTERPOL).

The mechanism for requesting correction of information contained within FSDS are outlined in the SORNs associated with this system. Further notice is provided through this PIA.

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

Mitigation: This risk is partially mitigated. Individuals can request access to information about themselves under the FOIA/PA, 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 Disclosure Officer.

Auditing and Accountability

FSDS has a robust audit trail that logs any action by users and administrators. The FSDS system logs user activity, locks sessions after a period of inactivity, limits access to only authorized individuals, and prevents account access after a number of unsuccessful login attempts. It also reminds users that unauthorized, improper use or access to the system may result in disciplinary action as well as civil and criminal penalties to encourage proper use of the system. 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.

FSDS users receive training on how to use the system by a user's guide. Additionally, FSDS users are required to complete DHS and Secret Service-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,"[9] providing employees and contractors with additional guidance.

Access to the system is strictly limited to authorized USSS FSDS employees who have a legitimate need to know in their role and responsibilities as stated in DHS Sensitive Systems Policy Directive 4300A, explaining information technology procedures for granting access to Secret Service computers. Employees requiring access to FSDS are given permission to access information after written authorization from appointed business owner(s). 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 system is accessible using employee's

[9] See handbook for Safeguarding Sensitive PII, available at https://www.dhs.gov/sites/default/files/publications/dhs%20policy%20directive%20047-01-007%20handbook%20for%20safeguarding%20sensitive%20PII%2012-4-2017.pdf

secure and individual credentials. FSDS protects PII within FSDS by implementing security groups. DHS physical and information security policies dictate who may access Secret Service computers and filing systems.

Responsible Official

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

Approval Signature

Original, signed copy on file at the DHS Privacy Office.

_____

Dena Kozanas
Chief Privacy Officer
Department of Homeland Security