Privacy Impact Assessment Update

for the

Forensic Service Division System

DHS Reference No. DHS/USSS/PIA-017(b)

May 6, 2024

Homeland Security

Abstract

The United States Secret Service (USSS) Forensic Services Division System (FSDS) provides the Forensic Services Division (FSD) with a suite of applications that facilitates its support of the Secret Service mission. FSDS applications provide authorized users with evidence and case tracking functionalities, automated handwriting recognition capability, and the ability to digitally examine and store fingerprints and palm prints. The USSS is conducting this Privacy Impact Assessment (PIA) update to discuss sharing personally identifiable information (PII) with the U.S. Department of Homeland Security (DHS) Office of Biometric Identity Management's (OBIM) Automated Biometric Identity System (IDENT)[1] and the National Capital Regional Automated Fingerprint Identification System (NCR AFIS), a regional fingerprint database including Fairfax County, Virginia; Washington, D.C.; and Montgomery and Prince George's Counties, Maryland. In addition, this Privacy Impact Assessment update documents how Forensic Services Division examiners can route Live-Scan collected known fingerprint records and latent prints through the Federal Bureau of Investigation's (FBI) Next Generation Identification (NGI) system for searching through IDENT.

Overview

FSDS is an intranet accessible information system utilizing intranet and web technologies hosted, maintained, and managed at USSS Headquarters (HQ). FSDS provides the Forensic Services Division organization with a suite of applications that facilitates its support of the Secret Service investigative and protective missions. The Forensic Services Division supports the USSS mission by conducting timely and accurate forensic examinations of latent print and questioned document evidence obtained through standard law enforcement activities; assisting with training and consultation; conducting pre-employment and criminal polygraphs; and providing visual communication requirements such as graphic design, photography/videography, geospatial, and 3D modeling support. The applications that comprise FSDS include JusticeTrax Laboratory Information Management System (LIMS), Forensic Information System for Handwriting (FISH), Mideo CaseWorks, Qualtrax Compliance Software, and Live-Scan. FSDS collects information

[1] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT), DHS/OBIM/PIA-001 (2012), *available at* https://www.dhs.gov/privacydocuments-office-biometric-identity-management-obim. DHS is in the process of replacing IDENT with the Homeland Advanced Recognition Technology System as the primary DHS system for storage and processing of biometric and associated biographic information. For more information about the Homeland Advanced Recognition Technology System, please *see* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE HOMELAND ADVANCED RECOGNITION TECHNOLOGY SYSTEM (HART) INCREMENT 1, DHS/OBIM/PIA-004 (2020), *available at* https://www.dhs.gov/privacydocuments-office-biometric-identity-management-obim.

regarding members of the public, USSS employees (federal personnel and contractors), and employees of other federal agencies. The description of each application is discussed below in greater detail.

JusticeTrax Laboratory Information Management Systems (LIMS & LIMS Portal) – This application is a comprehensive case management system that integrates evidence tracking, analytical results, reports, and lab management information, thus resulting in a system to track all cases and evidence submitted to the Forensic Services Division for forensic examination by Secret Service offices and outside agencies.

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

Mideo CaseWorks – This 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 identification documentation and comparative analysis.

Qualtrax Compliance Software – Qualtrax is a leading provider of compliance software for forensic laboratories. Qualtrax documents quality controls through electronic versioning, tracking, approval, and escalation. Workflows are automated for more efficient business processes. The application distributes and tracks testing and training tasks, and reports generation of audits, workflows, and training related data.

Live-Scan – Live-Scan electronically captures fingerprints and palm prints without using black fingerprint ink. The Live-Scan technology provides a digitized scan of biographic information, fingerprints, palm prints, and mug shot images that are electronically transmitted to the FBI's Next Generation Identification[2] for an automated search against over 81,400,000 criminal fingerprint records. The Secret Service Live-Scan Program (SSLSP) is an enterprise-wide initiative with 124 Live-Scan booking stations deployed to Secret Service offices throughout the United States, including Puerto Rico. Live-Scan collects digitized scans of fingerprints, personally identifiable information, and biographical information of the public, USSS employees, contractors supporting USSS, and employees of other federal agencies for criminal investigation as well as employment background checks.

[2] *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.

The information collected and maintained within FSDS is used to support the Secret Service's investigative and protective mission. Correspondence and forensic reports containing personally identifiable information are maintained in the Forensic Services Division evidence official correspondence files and are maintained in accordance with applicable USSS records retention policies. Information collected that becomes part of a case is retained in FSDS in accordance with data retention policies and protocols.

FSDS shares personally identifiable information with the Department of Justice (DOJ) Joint Automated Booking System (JABS)[3] and Civil Applicant System (CAS)[4] as well as the FBI Criminal Justice Information Services (CJIS).[5] FSDS uses individual identification numbers such as the FBI's Universal Control Number (UCN) and Automated Biometric Identity System's Fingerprint Identification Number (FIN), state identification numbers, name, and date of birth as Social Security Number (SSN) alternatives when available to protect privacy. Data exchanged is encrypted.

All DHS personnel that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take all applicable agency required privacy and information security training before accessing PII and/or SPII as well as required annual refresher training.

Reason for the PIA Update

USSS is updating the Privacy Impact Assessment to document FSDS sharing personally identifiable information with the following systems: IDENT and the National Capital Regional Automated Fingerprint Identification System, a regional fingerprint database including Fairfax County, Virginia; Washington, D.C.; and Montgomery and Prince George's Counties, Maryland.

The Forensic Services Division sends latent fingerprint and palm prints collected during investigations to OBIM's Biometric Support Center (BSC) via email. OBIM's Biometric Support Center examiners then query IDENT, which issues a report to USSS. In addition, Forensic Services Division examiners may route latent prints through the existing FBI NGI pathways for IDENT searching.[6] The Forensic Services Division manages the Live-Scan system for the USSS, which is used to submit known fingerprint records through the NGI pathway for IDENT searching

[3] *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.
[4] *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.
[5] *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.
[6] USSS currently uses the FBI pathway to search IDENT due to technical considerations between FSDS and IDENT. In the future, USSS plans to use a new direct connection with HART. This is discussed in the Information

The National Capital Regional Automated Fingerprint Identification System allows Forensic Services Division fingerprint specialists to search and retain unidentified latent prints in the National Capital Regional Automated Fingerprint Identification System via a standalone workstation located within the USSS Forensic Services Division. The National Capital Regional Automated Fingerprint Identification System is only used for local cases. The latent prints are searched via the standalone workstation against the following regional systems: Fairfax County, Virginia; Washington, D.C. (DC-AFIS); and Montgomery and Prince George's Counties, Maryland (RAFIS). Candidate lists, including biographic and biometric information, are returned to the Forensic Services Division via the National Capital Regional Automated Fingerprint Identification System for comparison to the latent prints. If candidates require additional comparison, complete known records can be obtained by USSS personnel either in person from the arresting agency or via database retrieval from the National Capital Regional Automated Fingerprint Identification System. Live-Scan is not connected to the regional National Capital Regional Automated Fingerprint Identification System.

This Privacy Impact Assessment update also documents the recently approved National Archives and Records Administration (NARA)records retention schedule for USSS Investigative Records.

Privacy Impact Analysis

Authorities and Other Requirements

There have been no changes to the collection authorities since the initial publication of the Privacy Impact Assessment. 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 authorities include Pub. L. 92-544 (Title II) and Pub. L. 107-56 (Title II). Supplemental regulatory authorities include 28 CFR 0.85, Part 20, and 50.12.

The DHS/USSS-001 Criminal Investigation Information,[7] DHS/USSS-003 Non-Criminal Investigation Information,[8] and DHS/USSS-004 Protection Information System[9] are system of records notices (SORN) that apply to the collection, use, maintenance, and dissemination of personally identifiable information by FSDS. A new, comprehensive agency schedule for Investigation Records (DAA-0087-2021-0001) covers several general categories of USSS

Sharing Section below.

[7] *See* DHS/USSS-001 Criminal Investigation Information, 85 Fed. Reg. 64523 (October 13, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.

[8] *See* DHS/USSS-003 Non-Criminal Investigation Information, 76 Fed. Reg. 66937 (October 28, 2011), *available at* https://www.dhs.gov/system-records-notices-sorns.

[9] *See* DHS/USSS-004 Protection Information System, 85 Fed. Reg. 64519 (October 13, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.

investigative records maintained in FSDS. The comprehensive schedule was approved by NARA on March 21, 2024. Several legacy retention schedules also apply to FSDS records. These include N1-087-10-001 (Live-Scan) and N1-087-06-002 (Forensic Information System for Handwriting).

Characterization of the Information

The Forensic Services Division Laboratory sends latent fingerprints and palm prints collected during investigations to OBIM's Biometric Support Center via email. OBIM's Biometric Support Center examiners then query IDENT, and issue a report to USSS. The request sent to OBIM includes the Forensic Services Division case number and information specific to the examiner requesting the search. A record of the report containing the results of the search is provided by OBIM and is maintained by FSDS. Additionally, Forensic Services Division examiners may search IDENT via FBI NGI, which returns a candidate list that is maintained in FSDS. Known fingerprints that are collected on Live-Scan devices are routed through the FBI to IDENT for searching.

Forensic Services Division Fingerprint Operations Branch (FOB) examiners may search latent fingerprints and palm prints collected during investigations in the National Capital Regional Automated Fingerprint Identification System. The National Capital Regional Automated Fingerprint Identification System returns a candidate list that is reviewed by Fingerprint Operations Branch examiners. Unique identifiers for any identification or inconclusive conclusions are recorded in FSDS so that full exemplars may be obtained.

Privacy Risk: There is a risk that USSS may receive inaccurate biometric data from other government databases (e.g., the Automated Biometric Identity System or the National Capital Regional Automated Fingerprint Identification System).

Mitigation: This risk is partially mitigated. The Secret Service will not take any action based on information received by other government agencies 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 and who have assessed the information for accuracy and reliability. However, because USSS does not control what information the FBI, DHS, and NCR AFIS share with USSS, this risk cannot be fully mitigated.

Uses of the Information

There are no changes to the way FSDS uses this information.. The information collected by and maintained in FSDS is used in support of the Secret Service's 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.

The DHS Automated Biometric Identity System (IDENT) facilitates Forensic Services Division fingerprint specialists' search and retention of unidentified latent prints. Reports or candidate lists, including biographic and biometric information, are returned to the Forensic Services Division. Known fingerprints that are collected on Live-Scan devices are routed through the FBI to IDENT for searching.

The National Capital Regional Automated Fingerprint Identification System facilitates Forensic Services Division fingerprint specialists' search and retention of unidentified latent prints in the regional automated fingerprint identification systems via a standalone workstation. The latent prints will be searched via the standalone Automated Fingerprint Identification System workstation against the following regional automated fingerprint identification systems: Fairfax County, Virginia; Washington, D.C. (DC-AFIS); and Montgomery and Prince George's Counties, Maryland (RAFIS). Candidate lists, including biographic and biometric information, are returned to the Forensic Services Division via the National Capital Regional Automated Fingerprint Identification System.

Privacy Risk: There is a risk that information received through the sharing arrangements and then maintained in 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. Secret Service has implemented strict access controls within the system, which is housed on a closed network, and adheres to stringent information management processes. Access to FSDS is only provided to USSS personnel who have a valid need to know the information to perform work-related tasks. This ensures that each user has access to only the data for which they have a need to know to perform their protective or investigative responsibilities. Moreover, system and privacy-specific training is initially, and yearly thereafter, 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

This Privacy Impact Assessment Update and the corresponding privacy documentation and/or notice requirements for the DHS Automated Biometric Identity System (IDENT), FBI NGI, and the National Capital Regional Automated Fingerprint Identification System provide notice for how information may be shared between agencies.

Data Retention by the Project

A new, comprehensive agency schedule for Investigation Records (DAA-0087-2021-0001), which covers several general categories of USSS investigative records maintained in FSDS

was approved by NARA on March 21, 2024.[10] Several legacy schedules that apply to FSDS records have been reviewed and approved by the National Archives and Records Administration. These include N1-087-10-001 (Live-Scan) and N1-087-06-002 (Forensic Information System for Handwriting).

If the latent print sent by USSS to NGI or IDENT is not identified, then the print is enrolled in the respective system's Unsolved Latent File (ULF) and retained until it is identified. USSS, in coordination with the DHS Privacy Office, is developing a memorandum of understanding (MOU), including appropriate privacy safeguards, for the data that will be shared with the National Capital Regional Automated Fingerprint Identification System. No information sharing will occur until the MOU is implemented.

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. The Forensic Services Division sends latent fingerprints and palm prints collected during investigations to OBIM's Biometric Support Center. OBIM's Biometric Support Center examiners then query IDENT and issue a report to USSS. If the latent print is not identified, the print is enrolled in IDENT's Unsolved Latent File (ULF) and retained until it is identified.

Furthermore, Forensic Services Division latent print examiners may search IDENT via FBI NGI and receive a candidate list from IDENT to conduct comparisons and issue reports. Known fingerprint records collected via Live-Scan can be searched in NGI and then routed to IDENT.

The Forensic Services Division also houses a standalone workstation with a direct connection to search latent fingerprints and palm prints against the National Capital Regional Automated Fingerprint Identification System. A memorandum of understanding between USSS and the National Capital Regional Automated Fingerprint Identification System is in development.

Privacy Risk: There is a risk that USSS is sharing more information than necessary with FBI NGI to search DHS IDENT.

Mitigation: This risk is mitigated. First, USSS only shares the minimum amount necessary to conduct a search. Rather than send an entire case file, USSS only shares the print and other non-attributable metadata with FBI to search IDENT. USSS conducts these searches through FBI

[10] This records schedule covers investigative records relating to USSS criminal investigations including financial crimes, counterfeiting crimes, cyber-enabled crimes, associated routine law enforcement transactions, and non-criminal and internal USSS investigations, reviews, and inspections. This schedule is intended to replace disposition schedules related to Investigative Records previously registered by the USSS. *See* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0087/daa-0087-2021-0001_sf115.pdf.

because of NGI's interoperability with IDENT. Additionally, USSS is already searching NGI; therefore, using the FBI as a pathway to search IDENT does not constitute receipt of new data from what FBI would normally receive. If a direct pathway was established between USSS and IDENT, there would still be a need for USSS to search the FBI's NGI system due to the differences in the information contained within the databases.

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 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 the Privacy Act as appropriate to provide the Requestor with all information that is releasable. Given the nature of the information maintained 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, USSS reviews all such requests on a case-by-case basis. Instructions for filing a FOIA or Privacy Act request are available at http://www.dhs.gov/foia.

Auditing and Accountability

All information sharing agreements, memoranda of understanding, and new uses of information are reviewed by the USSS Privacy Office, Office of Chief Counsel, and the respective program office. This includes the appropriate documentation for sharing with OBIM, FBI, and the jurisdictions sharing information through the National Capital Regional Automated Fingerprint Identification System.

Further, access to FSDS is strictly limited to authorized USSS FSDS employees who have a legitimate need to know in their role and responsibilities. The system has a robust audit trail that logs actions by users and administrators. FSDS 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 maintained 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 via 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 personally identifiable information. Applicable users are also trained on the use of FBI-NGI and the privacy implications and safeguards associated with the system.

Contact Official

Christal Bramson
Supervisory Privacy Officer
U.S. Secret Service
Privacy@USSS.DHS.GOV

Responsible Official

Kelli Lewis
Supervisory Forensic Scientist
Forensic Service Division
Office of Investigations
U.S. Secret Service

Approval Signature

Original signed copy on file the DHS Privacy Office.

_____

Mason C. Clutter
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717