# Privacy Impact Assessment

**for the**

# Comprehensive Financial Investigative System

**DHS Reference No. DHS/USSS/PIA-030**

**August 13, 2020**

Homeland Security

## Abstract

The United States Secret Service (USSS) Investigative Support Division (ISD) uses the Comprehensive Financial Investigative System (CFIS) in support of data capture to maintain records for financial investigations from case initiation to completion. CFIS provides ISD with tools for the analysis, tracking, archiving, and retrieval of lawfully obtained financial documents in support of these financial investigations. USSS is conducting this Privacy Impact Assessment (PIA) because CFIS collects and maintains personally identifiable information (PII) regarding subjects of criminal financial investigations.

## Overview

CFIS acts as a repository to support all USSS financial investigations from case initiation to completion.[1] USSS uses the information collected during financial investigations to analyze financial data to identify individuals and groups who may engage in criminal activity. Authorized personnel use CFIS for analyzing the collected financial data for potential patterns and anomalies. Advanced visualization and analytical capabilities allow rapid evaluation and proof of investigative theories as well as discovery of additional schemes, evidence, co-conspirators, and illicit funds and assets. Beginning with tracking of lawfully obtained financial records, to include subpoenaed records, CFIS simplifies the organization, archival, and retrieval of documents.

CFIS is used only for financial analysis, using documents such as bank statements, brokerage statements, credit card statements, checks, deposit tickets, wire transfer reports, Automated Clearing House (ACH) reports, debit memos, invoices, and receipts. CFIS does not interface with other USSS investigative systems used for maintaining case files and evidence. USSS investigative analysts and agents create a case number that can be entered into CFIS for tracking and analysis. They also input data into CFIS based on the information collected from lawfully obtained financial records. This information is confirmed at various steps in the ISD investigative process.

All bank, brokerage, and credit card statements that are scanned or imported into CFIS need to be associated with an Intelligent Document Analyzer (IDA). IDAs are templates that allow for importing of information from financial files. Once these documents are uploaded to the CFIS database, a query using trend and pattern analysis can then be run against the data, and reports can be generated. The reports identify links between statement transactions and show the flow of funds. In addition, the generated reports and analyses may serve as supporting evidence for investigations and prosecutions.

[1] Actual case files are maintained separately in the appropriate case management system.

The speed, accuracy, and analytical capabilities of CFIS allow authorized users to efficiently and effectively track and analyze financial information in support of the USSS investigative mission.

# 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?

USSS is authorized to collect information maintained in CFIS pursuant to 18 U.S.C. §§ 1029(d), 1030(d), 3056, and 3056A.

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

SORN coverage is provided by DHS/USSS-001 Criminal Investigation Information,[2] which covers the collection of criminal records related to individuals being investigated by the Secret Service in connection with USSS' criminal law enforcement functions, including investigating counterfeiting offenses, financial institution fraud, computer and telecommunications fraud, false identification documents, access device fraud, advance fee fraud, and electronic funds transfer fraud.

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

No. The Authority to Operate for CFIS is pending completion of this PIA. This is a new project and has an anticipated date of completion of January 2021.

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

The data captured within CFIS is maintained in accordance with the following record schedules: N1-087-10-006: Asset Seizure and Forfeiture Records,[3] N1-87-89-002: Field Office

[2] DHS/USSS-001 Criminal Investigation Information, 76 Fed. Reg. 49497 (August 10, 2011), *available at* https://www.dhs.gov/system-records-notices-sorns.

[3] NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, REQUEST FOR RECORDS DISPOSITION AUTHORITY, RECORDS SCHEDULE NUMBER N1-087-10-006, U.S. SECRET SERVICE, ASSET SEIZURE AND FORFEITURE RECORDS (2010), *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0087/n1-087-10-006_sf115.pdf.

Investigative Records,[4] and N1-87-92-002: Investigative Program Records.[5] In general, USSS 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 CFIS for a period that corresponds to the specific case disposition assigned.

In addition, 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. USSS will follow these retention periods once approved.

### 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 CFIS is not covered by the PRA.

## Section 2.0 Characterization of the Information

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

CFIS maintains information on persons under investigation for financial crimes. The following documents may be included: domestic and foreign financial documents such as bank statements, brokerage statements, credit card statements, checks, deposit tickets, wire transfer reports, ACH reports, debit memos, invoices, and receipts. A case number is created and entered into CFIS for analysis, tracking, and retention by the investigative analysts and agents. In addition to the documents listed above and the PII captured in those, CFIS records also include:

- Names
- Address
- Email addresses

[4] NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, REQUEST FOR RECORDS DISPOSITION AUTHORITY, RECORDS SCHEDULE NUMBER N1-87-89-002, U.S. SECRET SERVICE FIELD OFFICE INVESTIGATIVE RECORDS (1992), https://foiamapper.com/record-systems/n1-087-89-002_sf115.pdf.

[5] NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, REQUEST FOR RECORDS DISPOSITION AUTHORITY, RECORDS SCHEDULE NUMBER N1-87-92-002, U.S. SECRET SERVICE, INVESTIGATIVE PROGRAM RECORDS (1993), *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0087/n1-087-92-002_sf115.pdf.

- Telephone numbers
- Credit card numbers
- Financial account numbers

CFIS analyzes the financial information input by investigative analysts and agents to support ongoing financial investigations. The system does not interface with or receive information from any other systems.

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

For all individuals under investigation, the following documents may be included in CFIS: domestic and foreign financial documents such as bank statements, brokerage statements, credit card statements, checks, deposit tickets, wire transfer reports, ACH reports, debit memos, invoices, and receipts. CFIS collects this information through subpoenaed records and data that has been lawfully provided by financial institutions.

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

CFIS uses subpoenaed records and data that has been lawfully provided by financial institutions. No data in CFIS comes from commercial or publicly available sources.

## 2.4 Discuss how accuracy of the data is ensured.

Information is checked for accuracy during the criminal investigative process. USSS investigative analysts and agents input data into CFIS based on lawfully obtained financial records. This information is confirmed at various steps in the ISD investigative process.

## 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 CFIS relies on information from third parties - financial institutions.

**Mitigation:** This risk is partially mitigated. USSS will not take any action unless the information received has been reviewed by USSS employees engaged in 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. Additionally, USSS personnel are trained to look at the totality of the information, and one piece of evidence is not used as the sole basis for action.

# Section 3.0 Uses of the Information

## 3.1 Describe how and why the project uses the information.

The information collected and maintained within CFIS is used in support of the accomplishment of USSS' investigative mission. USSS uses the information collected during financial investigations to analyze financial data to identify individuals and groups who may be engaging in criminal activity. Authorized personnel use CFIS for analyzing the collected financial data for patterns and anomalies.

## 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.

Yes. Authorized personnel use CFIS for analyzing the collected financial data for patterns and anomalies.

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

Only authorized USSS investigative analysts and agents have access to CFIS and its data. No individuals outside of USSS have technical access.

## 3.4 Privacy Impact Analysis: Related to the Uses of Information

**Privacy Risk:** There is a privacy risk that information maintained within CFIS 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. USSS has implemented strict access controls within the system, which is housed on a closed network, as well as stringent information management processes. Access to CFIS is only provided to USSS personnel who have a valid need to know to 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 investigative responsibilities. Additionally, system and privacy-specific training is provided to USSS employees engaged in criminal investigation activities to ensure that all individuals with access to data maintained within CFIS are aware of the proper methods for handling information.

# 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.

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. However, the DHS/USSS-001 Criminal Investigation Information SORN and this PIA provide notice regarding the collection of information and the sharing and uses associated with data maintained within CFIS. The final rule for the applicable SORN officially exempts the system from portions of the Privacy Act.[6]

## 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 collection and particular uses of the information in CFIS.

## 4.3 Privacy Impact Analysis: Related to Notice

**Privacy Risk:** There is a risk that individuals under investigation will not be provided with notice that their information has been collected by USSS and stored in CFIS.

**Mitigation:** This risk is partially mitigated. Due to the investigatory nature of CFIS, providing notice to individuals under investigation is not always feasible. Providing this notice could impede law enforcement investigations and would undermine the purpose of CFIS and the USSS mission. However, the DHS/USSS-001 Criminal Investigation Information SORN and this PIA provide notice and identify the data collected and maintained by this system, as well as the routine uses and sharing of that information.

# Section 5.0 Data Retention by the Project

## 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 N1-087-10-006, 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 may be retained indefinitely. Information that is collected but does

[6] Final Rule for Privacy Act Exemptions, 74 Fed. Reg. 45087 (August 31, 2009), *available at* https://www.dhs.gov/system-records-notices-sorns.

not become part of an investigative case file, per existing retention schedules established and/or approved by NARA, is destroyed/deleted when no longer needed for administrative, legal, or audit purposes.

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. USSS will adhere to any changes approved by this effort.

### 5.2 Privacy Impact Analysis: Related to Retention

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

**Mitigation:** This risk is mitigated. USSS has implemented provision of proper records retention training to all system users and conducts periodic audits of the system. The information in CFIS will be retained for the timeframes outlined in the retention schedules in Section 5.1, consistent with general law enforcement system retention schedules and as necessary to complete the USSS 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.

## 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.

CFIS 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. CFIS 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 CFIS 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 USSS mission and is consistent with the routine uses

contained in the DHS/USSS-001 Criminal Investigation System SORN. Information is shared pursuant to Memoranda of Understanding (MOU) or through sharing between USSS personnel, including those law enforcement officials assigned to a joint investigation or with prosecuting agencies. CFIS data will be shared if doing so will further law enforcement efforts conducted by USSS or its law enforcement counterparts, 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 CFIS.

Additionally, 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. Any disclosure of PII would be listed in correspondence on official USSS letterhead in response to a request from a law enforcement agency. Correspondence containing PII is maintained in the ISD evidence vault or official correspondence files and is maintained in accordance with applicable USSS records retention policies.

Additionally, all ISD systems, to include CFIS, require the use of audit logs which record transactions within the systems, as well as transactions external to the systems that are manually sent to 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. Only USSS employees engaged in law enforcement activities who are trained on CFIS may disclose this information as system access is only provided to these individuals. Authorized USSS users may only share the data pursuant to routine uses specified in the DHS/USSS-001 Criminal Investigation Information SORN. USSS may share information from CFIS 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

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

Individuals seeking access to any record containing information maintained within CFIS, or seeking to contest the accuracy of its content, may submit a Privacy Act request to USSS. Individuals, regardless of citizenship or legal status, may also request access to their records under the Freedom of Information Act (FOIA). Access requests should be directed to the USSS 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 CFIS, all or some of the requested information may be exempt from access pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests.

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 USSS' investigatory mission, information contained within this system may be released or amended. Instructions for filing a FOIA or Privacy Act 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?

Due to the law enforcement nature of CFIS, records may be excluded from the amendment and certain redress provisions of the Privacy Act. However, the procedures outlined in Section 7.1 provide information on how individuals can similarly correct inaccurate or erroneous information.

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

The mechanism for requesting correction of information contained within CFIS are outlined in the SORNs associated with this system. 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 not have the ability to correct that information.

**Mitigation:** This risk is partially mitigated. Individuals can request access to information about themselves under the FOIA and Privacy Act, and, for those who are eligible, may also request that their information be corrected. However, the nature of CFIS 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 investigation. However, requests to amend records are still considered on a case-by-case basis.

# 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?

Training is prioritized to ensure system administrators and personnel only use information in accordance with practices mentioned in this PIA. CFIS users adhere to DHS Rules of Behavior and receive hands-on training to operate the system.

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

CFIS 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. DHS has also published the "Handbook for Safeguarding Sensitive Personally Identifiable Information,"[7] providing personnel with additional guidance. Additionally, CFIS users receive training on how to use the system by a user guide.

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

USSS protects PII by implementing security groups within Microsoft Active Directory. Employees requiring access to CFIS are given permission to access information after written authorization from appointed business owner(s)/system owner(s). Access to the system is limited to authorized USSS employees who have a legitimate need to know in their role and responsibilities as stated in DHS Sensitive Systems Policy Directive 4300A,[8] explaining information technology procedures for granting access to USSS computers. When access is

[7] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, HANDBOOK FOR SAFEGUARDING SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION, https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information (last visited August 3, 2020).
[8] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, DHS 4300A SENSITIVE SYSTEMS HANDBOOK, https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook (last visited August 3, 2020).

authorized, CFIS is accessible using employee's personal identity verification.

### 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.

## Contact Official

Jada Keltz
Investigative Support Division
United States Secret Service
U.S. Department of Homeland Security
(202) 680-0373

## Responsible Official

Christal Bramson
Acting Privacy Officer
United States Secret Service
U.S. Department of Homeland Security

## Approval Signature

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

_____

Dena Kozanas
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717