# United States Department of Justice
# Justice Management Division


## Privacy Impact Assessment
for the
Forfeiture Systems General Support Services (FS-GSS)

Issued by:
Morton Posner
Senior Component Official for Privacy

Approved by: Jay Sinha
Senior Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: April 25, 2025

*(May 2022 DOJ PIA Template)*

## Section 1: Executive Summary

***Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)***

The Forfeiture Systems General Support System (FS-GSS) delivers enterprise computing services and infrastructure support to the Department's Asset Management Forfeiture Staff (AFMS) Asset Forfeiture Program. The overall purpose of the system is to manage and deploy various information technology (IT) and automated data processing applications designed to execute specific roles and responsibilities in support of the AFMS's Asset Forfeiture Program. The FS-GSS will serve as the main access point to current and new Asset Forfeiture Program related information systems. The system collects and contains various types of personally identifiable information (PII) such as name and address, email address, financial account identifiers, other physical property identifiers, and legal narratives supporting case activity. To manage, maintain, support, operate and use the system, specific applicant information is collected from federal, state, local, law enforcement agency employees and/or contract personnel. To execute the asset forfeiture business mission, information is collected from the subject(s) of an investigation or civil or criminal case. Information is collected, maintained, and disseminated with other federal agencies for civil and criminal law enforcement purposes, intelligence activities, and administrative matters to analyze and execute the various stages of the asset forfeiture lifecycle.

FS-GSS includes all IT network operations, system architecture, system infrastructure, software development lifecycle operations, user account management, access control functions, identity management functions, IT peripheral tools, and cybersecurity operations and initiatives all contained within the overall Department IT and cybersecurity operations. Specifically, FS-GSS provides the IT infrastructure supporting the applications contained within the system boundaries of Forfeiture Systems – Financial System (FS-FinSys) and Forfeiture Systems – Non-Financial System (FS-Non FinSys). FS-GSS is designed to ensure that all IT network operations provide the most efficient methods to execute the asset forfeiture business mission by using automated data processing models. In addition, the FS-GSS manages the IT network operations and applications to support all federal, state, and local agencies that participate and/or are assigned specific functions within the asset forfeiture program. To manage, maintain, support, operate and use the system, specific applicant information is collected from federal, state, local, law enforcement agency employees and/or contract personnel. To execute the asset forfeiture business mission, information is collected from the subject(s) of an investigation or civil or criminal case.

The system documents and tracks the stages of the asset forfeiture lifecycle such as the seizure, advertisement and notification, storage, expense and income management, forfeiture, and disposal of seized property. Other activities, such as the results of criminal or civil legal proceeding, are also captured in the system. The system also records the seized property activities by state and local law enforcement agencies participating in the asset forfeiture. The information contained in the system is used to conduct and track all aspects of the asset forfeiture lifecycle in accordance with applicable laws. The information in the system may be analyzed and shared with other federal agencies in an effort to correlate or substantiate the methods and patterns of illegal activity conducted by subjects

and/or corresponding business entities.

This Privacy Impact Assessment (PIA) is being conducted as a new project specifically intended for FS-GSS to include the system boundaries of the Forfeiture Systems – Financial System (FS-FinSys) and Forfeiture Systems – Non-Financial System (FS-Non FinSys). A PIA is required by the privacy protections of the E-Government Act of 2002 and the Office of Management and Budget's implementing guidance (M-03-22).

## Section 2: Purpose and Use of the Information Technology

***2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.***

The purpose of the FS-GSS is to manage and deploy IT and automated data processing applications designed to execute the specific roles and responsibilities in support of the Asset Forfeiture Program mission. Information in the system is collected, maintained, and disseminated for civil and criminal law enforcement purposes, intelligence activities, and administrative matters to analyze and execute the various stages of the asset forfeiture lifecycle. The information may be analyzed and shared with other federal agencies in support of ongoing asset forfeiture or financial investigations, or other civil or criminal law enforcement case activities. Also, information sharing with other federal agencies is essential because criminal methods of operation may be detected, and the execution of specific asset forfeiture processes becomes more efficient.

***2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)***

| Authority | Citation/Reference |
|---|---|
| Statute | 18 U.S.C. § 981, Civil forfeiture; Civil Asset Forfeiture Reform Act (CAFRA) of 2020 (codified at 18 U.S.C. § 983, General rules for civil forfeiture proceedings); 18 U.S.C. § 984, Civil forfeiture of fungible property; and 18 U.S.C. § 985, Civil forfeiture of real property; 28 U.S.C. § 524(c); the Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3551, et seq. |
| Executive Order | |
| Federal regulation | |
| Agreement, memorandum of understanding, or other documented arrangement | |
| Other (summarize and provide copy of relevant portion) | |

## Section 3: Information in the Information Technology

***3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.***

| (1) General Categories of Information that May Be Personally Identifiable | (2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| *Example: Personal email address* | *X* | *B, C and D* | *Email addresses of members of the public (US and non-USPERs)* |
| **Name** | X | A, B, C, and D | Name of DOJ employees and other federal government personnel and ~~of~~ members of the public (US and non-USPERs) |
| **Date of birth or age** | X | C and D | This information is not required but may be provided by the public |
| **Place of birth** | X | C and D | This information is not required but may be provided by the public |
| **Sex** | | | |
| **Race, ethnicity, or citizenship** | | | |
| **Religion** | | | |
| **Social Security Number (full, last 4 digits or otherwise truncated)** | X | C and D | This information is not required but may be provided by the public |
| **Tax Identification Number (TIN)** | X | C and D | The TINs of businesses to identify seized property. Also, the TINs of vendors hired by the agency to provide services (e.g., those associated with the moving and/or storage of seized property) |
| **Driver's license** | X | C and D | This information is not required but may be provided by the public |
| **Alien registration number** | | | |
| **Passport number** | | | |
| **Mother's maiden name** | | | |
| **Vehicle identifiers** | X | C and D | VINs as needed identify specific seized property |
| **Personal mailing address** | X | C and D | Personal mailing addresses of members of the public (US and non-USPERs) |

| (1) General Categories of Information that May Be Personally Identifiable | (2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| **Personal e-mail address** | X | C and D | This information is not required but may be provided by the public |
| **Personal phone number** | X | A, B, C, and D | This information is not required but may be provided by federal and contract personnel, and the public |
| **Medical records number** | | | |
| **Medical notes or other medical or health information** | | | |
| **Financial account information** | X | C and D | Bank Account numbers used to identify seized property |
| **Applicant information** | | | |
| **Education records** | | | |
| **Military status or other information** | | | |
| **Employment status, history, or similar information** | | | |
| **Employment performance ratings or other performance information, e.g., performance improvement plan** | | | |
| **Certificates** | | | |
| **Legal documents** | | C and D | This information is not required but may be provided by the public |
| **Device identifiers, e.g., mobile devices** | X | A, B, C and D | For C and D, the information is collected to identify seized property. The information is not collected for A and B, but may be provided by federal and contract personnel |
| **Web uniform resource locator(s)** | | | |
| **Foreign activities** | | | |
| **Criminal records information, e.g., criminal history, arrests, criminal charges** | X | C and D | This information is not required but may be provided by the public |
| **Juvenile criminal records information** | X | C and D | This information is not required but may be provided by the public |
| **Civil law enforcement information, e.g., allegations of civil law violations** | X | C and D | This information is not required but may be provided by the public |
| **Whistleblower, e.g., tip, complaint, or referral** | | | |
| **Grand jury information** | N/A | C and D | This information is not required but may be collected by a federal agency |
| **Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information** | | | |

| (1) General Categories of Information that May Be Personally Identifiable | (2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| **Procurement/contracting records** | | | |
| **Proprietary or business information** | | | |
| **Location information, including continuous or intermittent location tracking capabilities** | | | |
| ***Biometric data:*** | | | |
| - **Photographs or photographic identifiers** | N/A | C and D | This information is not required but may be provided by the public |
| - **Video containing biometric data** | | | |
| - **Fingerprints** | | | |
| - **Palm prints** | | | |
| - **Iris image** | | | |
| - **Dental profile** | | | |
| - **Voice recording/signatures** | | | |
| - **Scars, marks, tattoos** | | | |
| - **Vascular scan, e.g., palm or finger vein biometric data** | | | |
| - **DNA profiles** | | | |
| - **Other (specify)** | | | |
| ***System admin/audit data:*** | | | |
| - **User ID** | X | A and B | User identification code of person authenticating to the system |
| - **User passwords/codes** | X | A and B | Password used by person authenticating to the system |
| - **IP address** | X | A, B, C, and D | IP address collected by audit logging application and system tools |
| - **Date/time of access** | X | A, B, C, and D | Date and time of access collected by audit logging application and system tools |
| - **Queries run** | X | A, B, C, and D | Queries executed to monitor and evaluate system access and usage |
| - **Contents of files** | X | A and B | Contents of files collected to ensure appropriate access and use of Department data |
| **Other (please list the type of info and describe as completely as possible):** | | | |

### *3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)*

**Directly from the individual to whom the information pertains:**

| | | | | | |
|---|---|---|---|---|---|
| In person | X | Hard copy: mail/fax | | Online | |
| Phone | | Email | | | |
| Other (specify): | | | | | |

| **Government sources:** | | | | | |
|---|---|---|---|---|---|
| Within the Component | X | Other DOJ Components | X | Other federal entities | X |
| State, local, tribal | X | Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer) | X | | |
| Other (specify): Asset Forfeiture Policy Manual, International Forfeiture | | | | | |

| **Non-government sources:** | | | | | |
|---|---|---|---|---|---|
| Members of the public | | Public media, Internet | | Private sector | |
| Commercial data brokers | | | | | |
| Other (specify): | | | | | |

## Section 4: Information Sharing

***4.1 Indicate with whom the Component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.***

| **Recipient** | **How information will be shared** | | | |
|---|---|---|---|---|
| | **Case-by-case** | **Bulk transfer** | **Direct log-in access** | **Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.** |
| Within the Component | X | X | X | Data shared with DOJ employees/contractors. |

| Recipient | How information will be shared | | | |
|---|---|---|---|---|
| | **Case-by-case** | **Bulk transfer** | **Direct log-in access** | **Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.** |
| | | | | Data shared via direct login or email communication with personnel on a need-to-know basis. Data is shared to conduct internal business activities, to identify patterns or methods of criminal operations, to improve overall case investigations, to dismantle criminal enterprises and organizations that violate forfeiture statutes. In addition, the component asset forfeiture program is subject to an annual audit of financial data related to civil or criminal forfeiture case processing.<br>Access controlled via Two-Factor Authentication with "least privileged" and "need-to-know" role-based policies applied.<br>Data in-transit and stored data is encrypted. |
| DOJ Components | X | X | X | Data shared with DOJ employees/contractors. |

| Recipient | How information will be shared | | | |
|---|---|---|---|---|
| | **Case-by-case** | **Bulk transfer** | **Direct log-in access** | **Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.** |
| | | | | Data shared via direct login or email communication with component representatives on a need-to-know basis. Data is shared to identify patterns or methods of criminal operations, to detect regional or national criminal activity of suspected organizations, to enhance overall case investigations, and to dismantle criminal enterprises and organizations that violate forfeiture statues. Also, information is shared as an essential process in the pre-seizure planning and post seizure activities. In addition, the Department's asset forfeiture program is subject to an annual audit of financial information related to civil or criminal forfeiture case processing. Access controlled via Two-Factor Authentication with "least privileged" and "need-to-know" role-based policies applied. Data in-transit and stored data is encrypted. |

| Recipient | How information will be shared | | | |
|---|---|---|---|---|
| | **Case-by-case** | **Bulk transfer** | **Direct log-in access** | **Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.** |
| Federal entities | X | X | X | Data shared with the State Department, Department of Defense (DOD), the Food and Drug Administration (FDA), United States Department of Agriculture (USDA), United States Coast Guard (USCG), Treasury Department, Alcohol and Tobacco, Tax and Trade Bureau (TTB), United States Customs and Border Patrol (USCBP), the United States Secret Service (USSS), Immigration and Customs Enforcement (ICE), Internal Revenue Service (IRS), United States Postal Inspection Service (USPIS). |

| | | | | |
|---|---|---|---|---|
| | | | | Data shared via direct login or email communication with respective Agency counterparts. Data is shared with other federal entities to identify patterns or methods of criminal operations, to detect regional or national criminal activity of suspected organizations, to improve overall case investigations, and to dismantle criminal enterprises and organizations that violate forfeiture statues. AFMS is responsible for the management and operation of the Seized Assets Deposit Fund (SADF) and Asset Forfeiture Fund (AFF) which is subject to an annual financial audit. Seizures of cash/currency, value of securities in brokerage accounts, or value of bank financial accounts are deposited in the SADF. Upon the issuance of the final order of forfeiture or conclusion of forfeiture proceedings, the value of funds deposited in the SADF is transferred and deposited into the AFF. DOJ Components and other federal entities participating in the asset forfeiture program may contribute the funds placed in the SADF or AFF. Also, information is shared for analysis by the Department OIG, other DOJ Financial Management Units, or Congressional representatives. The Department's asset forfeiture program is subject to an annual audit of financial information related to civil or criminal forfeiture case processing. Access controlled via Two-Factor Authentication with "least privileged" and "need-to-know" role-based policies applied. |

| Recipient | How information will be shared | | | |
|---|---|---|---|---|
| | **Case-by-case** | **Bulk transfer** | **Direct log-in access** | **Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.** |
| | | | | Data in transit and stored data is encrypted. |
| State, local, tribal gov't entities | X | X | X | Data is shared to encourage participation in the asset forfeiture program among state, local, tribal law enforcement agencies. Data such as investigative information and/or the status of a civil or criminal case activity is shared. Also, the Department's asset forfeiture program is subject to an annual audit of financial information, specifically forfeited proceeds or property distributed to state, local, tribal entities for the participation in asset forfeiture case activities.<br>Data shared via direct login or email communication with agency counterparts on a need-to-know basis. Access is controlled via Two-Factor Authentication with "least privileged" and "need to know" role-based policies applied. Data in transit and stored data is encrypted. |
| Public | X | | | Direct login access is not granted to members of the public. Data is shared via the advertisement of specific seized property information and/or the submission of a personal notice of seizure via USPS mail to the owners and/or persons with an interest in the seized property. Also, the public may submit a Freedom of Information Act (FOIA) request to share information. |

| Recipient | How information will be shared | | | |
|---|---|---|---|---|
| | **Case-by-case** | **Bulk transfer** | **Direct log-in access** | **Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.** |
| Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes | X | | | Direct login access is not granted to legal counsel, parties, witnesses, courts, or other judicial tribunals for litigation purposes. Data is shared with the legal counsel or attorney representative employed by the owner or persons with a legitimate or legal interest in the seized property. Also, legal counsel may submit a FOIA request to share information. |
| Private sector | X | | | Access is not granted to private sector representatives. Data is shared via the public advertisement of specific seized asset information. The private sector may submit a FOIA request to share information. |

| Recipient | How information will be shared | | | |
|---|---|---|---|---|
| | **Case-by-case** | **Bulk transfer** | **Direct log-in access** | **Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.** |
| Foreign governments | X | | | Direct login access is not granted to foreign government personnel. Because criminal actors may launder and conceal their criminal proceeds in multiple jurisdictions around the world, federal prosecutors and law enforcement agencies may share investigative information to pursue and recover forfeitable assets beyond the borders of the United States. In addition, consistent with the United States' international obligations, act affirmatively on incoming requests by other countries for assistance in restraining, forfeiting, and repatriating assets found in the United States that are forfeitable under foreign law. The Department's asset forfeiture program is subject to an annual audit of financial information related to civil or criminal forfeiture cases. |
| Foreign entities | | | | |
| Other (specify): | | | | |

***4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the federal government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.***

FS-GSS information will never be released to the public for "Open Data" purposes.

## Section 5: Notice, Consent, Access, and Amendment

***5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of***

***Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.***

The applicable System of Records Notices (SORNs) (see Sec. 7.2, below) provide generalized public notice of the collection, use, and sharing of FS-GSS information. No other notice specific to the collection, use, and sharing of the individual's PII is provided.

***5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.***

There is no opportunity for individuals to voluntarily participate in the collection, use, or dissemination of information in the system. The information is collected because of an alleged violation of asset forfeiture statute and/or civil or criminal law.

Employees and contractors assigned access to Department information and information technology do not have the opportunity to voluntarily participate in the collection, use or dissemination of information in the system. Employees' and contractors' consent to the collection or specific uses of their information by acknowledging the Department's Information Systems Warning Banner presented while accessing the information system. The Department's Information Systems Warning Banner is displayed in three (3) versions. 1.) Full Banner for users assigned access to information using the Department's information technology, 2.) Short Banner for user assigned access to Department information and information systems, and 3.) Mobile Device Banner for user accessing the Department's information and information systems using a mobile device. In addition, employees and contractors are presented the general user and/or privileged user rules of behavior that require acknowledgment by signature prior to gaining access to information and information systems. The general and privileged rules of behavior include rules related to Privacy Act of 1974 records and the use and maintenance of personally identifiable information (PII).

***5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.***

The Privacy Act permits an individual to gain access to records or any information pertaining to that individual which is contained in a system of records (here, JMD-022), subject to certain limitations and exemptions. The Department processes all Privacy Act requests for access to records under both the Privacy Act and the Freedom of Information Act (FOIA), 5 U.S.C. § 552. The Privacy Act also permits an individual to request an amendment or correction of a record pertaining to that individual, subject to certain limitations and exemptions. A request for amendment or correction of a Department of Justice record can be made by appearing in person or writing directly to the Department component that maintains the record.

## Section 6: Maintenance of Privacy and Security Controls

***6.1 The Department uses administrative, technical, and physical controls to protect information.***

***Indicate the controls below. (Check all that apply).***

| | |
|---|---|
| X | **The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):**<br>FS-GSS's ATO was completed on May 10, 2022, and will expire on May 11, 2025.<br>**If an ATO has not been completed, but is underway, provide status or expected completion date:**<br>**Unless such information is sensitive and release of the information could pose risks to the Component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** There are no POAMs that may be made public. |
| | **This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:** |
| X | **This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** FS-GSS is categorized as a Moderate-impact system, in accordance with Federal Information Processing Standards (FIPS) 199 – Standards for Security Categorization of Federal Information and Information Systems. To support the FIPS 199 designation of Moderate, the information contained in FS-GSS is categorized as sensitive but unclassified. FS-GSS does not manage high value assets (HVA) as defined by DOJ IT security policy. The loss of confidentiality, integrity, or availability of information may result in the delay of time sensitive forfeiture proceedings such as the advertisement and notification of seized property. Any delay in this specific legal requirement may result in a significant expenditure of additional funds to ensure the completeness of the advertisement and notification of seized property. Also, significant delay in required asset forfeiture actions may result in the return of seized property prior to any forfeiture proceedings. This premature return of seized property will void all pre-seizure planning activities, designated seizure / forfeiture proceedings, related expenses, and agency manpower deployments. In addition, any loss of data or potential data compromise could result in severe conditions such as the potential identification of federal agents and the possible harm, injury, or death that may occur. |
| X | **Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** As standard operating procedure, the computer servers supporting this project are built with secure configuration policies such as the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG's). Department approved monitoring agents such as IBM Endpoint Lifecycle Management System (ELMS) are deployed to monitor and identify component assets. On a weekly and |

| | |
|---|---|
| | monthly basis, vulnerability assessments and risk management procedures are executed on operating systems (OS), software applications, and database resources. The Microsoft System Center Configuration Manager (SCCM) Central platform provides Component Administrators the capability to manage and distribute security updates ~~and hotfixes (i.e. security patches)~~ released for Microsoft products only in the FS-GSS IT environment. Software protection applications such as Department approved intrusion detection system (IDS), intrusion prevention system (IPS), malicious software detection, and anti-virus software protections are deployed within the IT network supporting this project. In addition, FS-GSS utilizes the Department Trusted Internet Connection (TIC) and supporting proxy services at the external boundary to provide perimeter security and to protect systems by inspecting inbound and outbound traffic. The Core Enterprise Facility (CEF) firewalls provide secure traffic routing based on an Access Control List (ACL) used by the component's firewall services and other configuration settings (i.e. ports, protocols). Cisco MAB (MAC Authentication Bypass) system is being enforced by the ACS (Access Control Server) to track, manage, and authorize MAC addresses to access network resources via a designated physical port. Perimeter security protections including DOJ TIC, AWS Web Application Firewall (WAF) are placed and configured to protect the instances in AWS GovCloud. Once the traffic is in Virtual Private Cloud (VPC), there are additional layers of security including network ACLs and security groups. Communication between on premise networks and cloud VPC are controlled by multiple layers of firewall rules both at the cloud end as well as at the DOJ on premise. |
| X | **Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** On a weekly basis, the Splunk IT network log monitoring application collects all logs from FS-AWS which include Dynamic Host Configuration Protocol (DHCP) logs, Domain Name Service (DNS) logs, Windows and Linux operating system logs, Firewall, and intrusion protection service (IPS) logs. The Splunk application continuously (in real-time) forwards audit logs to the Splunk Enterprise Security Manager (ESM) at the Justice Security Operations Center (JSOC). |
| X | **Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**. |
| X | **Each Component is required to implement foundational privacy-related training for all Component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** AFMS does not provide privacy-related training specific to FS-GSS. Rather, it relies on the foundational privacy-related training included in the Department's annual Computer Security and Awareness Training (CSAT) and General and Privileged rules of behavior (ROB). |

***6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?***

The following information technology and physical controls are in place to reduce the risk of unauthorized access or disclosure of PII:

- Periodic vulnerability assessment activities such as system weakness discovery, and system patch and update deployment are conducted.
- Detailed operating system log management and potential incident analysis activities are performed.
- Intrusion protection/prevention system and anti-virus tools are deployed on system resources.
- Department-level access control lists are deployed with specific controls granted to designated employee or contractor users of the system.
- Access controls such as account authorization, routine account verification, and role-based security controls for user identification (based on role-based policies of "least privileged" and "need-to-know").
- Two-factor authentication prior to system access.
- Encryption of data in-transit and data-at-rest via IT encryption tools.
- Detection of unauthorized access to the system via scheduled account verification and review of audit logs and configuration file logs.
- The Department's management of physical access controls based on the user's background investigation category and security level.

***6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)***

The applicable records disposition schedule states that information in the system shall be destroyed/deleted 15 years after the final disposition of the seized asset; *See* N1-060-06-006 (Consolidated Asset Tracking System (CATS) (archives.gov)).

## Section 7: Privacy Act

***7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).***

_____ No. __X__ Yes.

***7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:***

JMD-022, "Department of Justice Consolidated Asset Tracking System (CATS)," 71 Fed. Reg. 29170 (May 19, 2006), 72 Fed. Reg. 3410 (January 25, 2007) (rescinded by 82 Fed. Reg. 24147), 82 Fed. Reg. 24147 (May 25, 2017).

JUSTICE/DOJ-002, "Department of Justice Information Technology, Information System, and

Network Activity and Access Records," 86 Fed. Reg. 37188 (July 14, 2021).

## Section 8: Privacy Risks and Mitigation

***When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?***

***Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:***

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical, and physical controls over the information.***

AFMS, Forfeiture Systems (FS) hosts tools, services, and applications that may collect PII, and those systems may collect other sensitive systems operation information to include names, personal e-mail addresses, personal phone numbers, device identifiers, and system admin/audit data (e.g., user IDs, user passwords, IP addresses, date/time of actions, queries run, contents of files). AFMS collection and use of PII, as described here and throughout this PIA, may create certain privacy risks. To mitigate these risks, all data retention is managed according to the National Archives and Records Administration (NARA) requirements and Department associated policies. AFMS does not collect certain data types such as Social Security Numbers and Tax Identification Numbers) from its users, nor from the subjects of an investigation or persons with an interest in the outcome of a case, to minimize the collection of PII. Sources of information come directly from the government and contractor users, subjects of an asset forfeiture investigation, owners of seized assets, or persons with an interest in the seized asset. AFMS manages the systems automatically collecting information, and from external government sources such as other Federal Government agencies where applications hosted by AFMS are offered as a service.

To further mitigate any risks associated with these activities, AFMS implements encryption, account management and access controls, auditing, and system monitoring tools to mitigate and protect PII. AFMS has deployed system endpoint protection to detect, stop, or remove malicious software, defend assets against viruses, buffer overflow issues, and prevent malware or hidden files from installing on devices. In addition, AFMS has deployed endpoint encryption to provide policy-controlled encryption of data on removable media such as USB drives, protect the media if lost or stolen, and provide full-disk encryption on laptops.

AFMS makes use of separate privileged and non-privileged user accounts and access is granted based on least privilege and need-to-know requirements. DOJ users (government and contractors) are not provided an opportunity to voluntarily participate in the collection, use or dissemination of

information accessible to AFMS System Administrators. Information is shared on a case-by-case basis within the component, other DOJ Components, other Federal agencies, state and local governments, and foreign governments. Information is shared with the private sector via the Freedom of Information Act (FOIA) policy and procedures. Also, for any risks associated with these activities, AFMS uses encryption and logging controls for mitigation purposes. AFMS makes use of Department IT infrastructure to employ Secure Sockets Layer (SSL) encryption, compliant with the Federal Information Processing Standard Publication (FIPS) 140-2, to protect data in transit between the browser and the user's workstation. In addition, AFMS utilizes Application Layer Firewall and integrated IDS/IPS technology and encapsulates in an IPSEC VPN all data replication/transit between AFMS and the CEF datacenter.

The AFMS ISSO performs continuous monitoring of the security controls within the system to ensure security protections are operating as intended. By Department Order, all DOJ users with access to Department networks, including AFMS, must receive an annual Cyber Security Assessment Training (CSAT). The CSAT course includes information on certain federal information privacy laws, such as the Privacy Act, and requirements for proper handling of PII. The course identifies potential risks and vulnerabilities associated with using DOJ-owned IT systems, provides a review of the user's role in protecting these systems, and establishes guidelines to follow at work and in mobile settings to protect against attacks on IT systems. All employees and contractors must also annually sign a DOJ Rules of Behavior agreement confirming that they have completed this course and that they agree to abide by such requirements reviewed in the course. Failure to successfully complete this training can result in termination of the employee or contractor's access to DOJ computers. Participation in the training course is tracked to ensure that DOJ employees and contractors comply with this training. In conclusion, to ensure the continued relevance and effectiveness of security controls, risk assessments, including privacy and security control assessments are routinely evaluated. In accordance with the NIST Special Publication 800-53 (Rev.5), these assessments include the management, operational, and technical controls to ensure minimization of any privacy risk.

AFMS system controls impacting IT resources, applications, and operations that support the asset forfeiture program are subject to an annual financial audit as outlined in the Federal Information System Controls Audit Manual (FISCAM). The annual IT financial audit is conducted at the direction of the Department Inspector General (IG).

In addition to the collection of information identified in 3.1 above, FS-GSS may also collect information from the individual such as last known address(s) or previous address(s) as necessary to determine the appropriate owner of the seized property. As a result, a strategy to collect specific or fewer data types and minimize the length of time information is retained may not apply regarding forfeiture case processing. Also, forfeiture proceedings may be prolonged where an individual files a claim of ownership, petitions for the return of seized property, or makes a FOIA request.

To encourage collaboration among all agencies participating in the Asset Forfeiture Program, information sharing and analysis of various sources of information is an essential aspect to processing a successful forfeiture case. Information sharing may reveal or identify the method of operation of violators and/or criminal organizations.

The subject individual has allegedly committed a violation of asset forfeiture statute or civil or criminal law which resulted in the seizure of property. The Agencies execute the necessary

requirements to notify the interested party of the seizure and offers the methods to contest the federal forfeiture. Various data types identified as PII are collected in accordance with law. There are also specific procedures in place for subject individuals to contest a forfeiture, request the return of seized property, or file a FOIA request.

The system is subject to periodic security and privacy control assessments, vulnerability risk management, OMB Cybersecurity Policy Recommendations/Requirements or Cybersecurity Executive Order, Department security and privacy control policy, recommended security best practices, and vendor security recommendations. Several IT security tools are deployed to strengthen the impact and effectiveness of the security and privacy controls. In addition, the Department routinely investigates other IT sources, IT tools, and associated vendors to minimize and mitigate privacy risks.