Department of Justice
Justice Management Division

Privacy Impact Assessment
for
Forfeiture Systems (FS)

Issued by:
Arthur E. Gary
JMD General Counsel and Senior Component Official for Privacy

Approved by: Peter Winn, Acting Chief Privacy & Civil Liberties Officer, Department of Justice

Date approved: June 6, 2018

(May 2015 DOJ PIA Form)

EXECUTIVE SUMMARY

The Forfeiture System-Financial System (FS-FinSys) and Forfeiture System-Non-Financial System (FS-Non-FinSys)—collectively referred to as Forfeiture Systems, or the Forfeiture System (FS)—supports Federal Government participants in the United States Department of Justice (DOJ or the Department) Asset Forfeiture Program[1] by providing a consolidated asset forfeiture management solution for administrative and judicial cases. FS tracks information and supports the Asset Forfeiture Program's operational and management business functions for all phases of the asset forfeiture process. FS accesses an inventory database that stores and processes asset forfeiture data maintained by DOJ and Federal Government participants.[2] FS allows DOJ analysts and Federal Government participants to generate and distribute custom reports to perform data analyses. FS also aids users in status inquiries, equitable share reporting, collaboration using SharePoint, management analysis, and other functions involved in the execution of the FS mission.

A Privacy Impact Assessment (PIA) has been conducted because personally identifiable information (PII) is collected, used, and maintained in FS, including but not limited to, the names and relevant information about owners, victims, agents, attorneys, custodians, petitioners, paralegals and legal assistants, district judges, case handlers, and State and Local (S&L) law enforcement agents involved in the forfeiture of specific assets.

Section 1: Description of the Information System

Provide a non-technical overall description of the system that addresses:

(a) The purpose that the records and/or system are designed to serve;

> FS is managed by the DOJ Asset Forfeiture Management Staff (AFMS), and supports the Federal Government participants in the DOJ Asset Forfeiture Program. FS provides a consolidated asset forfeiture management solution for both administrative and judicial cases to track information and support the Asset Forfeiture Program's operational and management business functions for all phases of the asset forfeiture life-cycle, including the following major business processes:

---

[1] The Asset Forfeiture Program encompasses the seizure and forfeiture of assets that represent the proceeds of, or were used to facilitate, federal crimes. More information on the DOJ Asset Forfeiture Program can be found at: https://www.justice.gov/afp.

[2] The "Federal Government participants" referred to throughout this PIA are those DOJ components and outside agencies that participate in the Asset Forfeiture Program. This includes, but is not limited to, the DOJ Criminal Division, Money Laundering and Asset Recovery Section; Bureau of Alcohol, Tobacco, Firearms and Explosives; Drug Enforcement Administration; Federal Bureau of Investigation; United States Marshals Service; United States Attorneys' Offices; United States Postal Inspection Service; Food and Drug Administration, Office of Criminal Investigations; Department of Agriculture, Office of the Inspector General; Department of State, Bureau of Diplomatic Security; and the Defense Criminal Investigative Service. More information on the Federal Government participants in the Asset Forfeiture Program can be found at: https://www.justice.gov/afp/participants-and-roles.

- Abandonment of property seized;
- Seizure of forfeitable assets;
- Transfer and custody of seized assets;
- Automation of legal notification and publication requirements;
- Receipt and processing of claims contesting the government's grounds for forfeiture;
- Petition receipt and processing;
- Criminal and civil litigation and administrative proceedings;
- Providing:
  - additional case information to Federal, State, and Local Law Enforcement members of an Organized Crime Drug Enforcement Task Force (OCDETF);
  - monetary restitution to victims resulting from the criminal conviction of an individual's or organization's violation of asset forfeiture laws; and/or
  - summary and detailed reports during each phase of the asset forfeiture lifecycle;
- Asset forfeiture lifecycle and final decision processing pertaining to the official use of assets, disposition of assets, equitable sharing between Federal, State, and Local law enforcement agencies, assets subject to an indictment, restraining order, seizure warrant, or warrant of arrest, income and expense accounting specific to the asset(s), and service of process granted to violators and victims;
- Inventory tracking; and
- Status inquiry.

FS capabilities include system administration, management decision support, document generation, and other procedural functions.

(b) The way the system operates to achieve the purpose(s);

FS is comprised of two main subsystems—FS-FinSys and FS-Non-FinSys–that support Federal Government participants in the DOJ Asset Forfeiture Program. These subsystems provide a consolidated asset forfeiture management solution for administrative and judicial cases.

FS-FinSys is comprised of the Consolidated Asset Tracking System (CATS) and the CATS Ad-Hoc Reporting Tool (CART):

- CATS is a web application that accesses an inventory database which stores and processes asset forfeiture data maintained by DOJ and Federal Government participants. Some of the data is owned by other agencies of the Federal Government, and DOJ serves as custodian for the data.

- CART allows DOJ analysts and certain Federal Government participant users to generate and distribute custom reports to perform data analysis using the Business Objects Enterprise Product Suite, a commercial off the shelf software product.

FS-Non-FinSys is comprised of SharePoint[3] portals and non-financial applications that aid users in status inquiries, equitable share reporting, collaboration, management analysis, and other functions involved in the execution of the FS mission. The SharePoint portals are used by Federal employee and contractor users for project collaboration, information delivery, and document management. The custom FS-Non-FinSys applications that have PII include:

- Forfeiture.gov—Forfeiture.gov is the public facing webpage for publically available information on Federal forfeiture actions.[4] Notices of administrative, civil, and criminal forfeiture actions are permitted on a government internet site and are available on Forfeiture.gov. This website is maintained consistent with the DOJ privacy policy,[5] and its servers are managed by AFMS and contain a comprehensive list of pending forfeiture notices from Federal Government participants.

- eDocs—eDocs is a document storage and retrieval application integrated with CATS to standardize uploaded file attributes/metadata based on asset information. This portal has the built-in capability to retrieve information by using a defendant's name. Other portals are designed to retrieve information using only Asset ID or related case information.

- Equitable Share Portal—The Equitable Share Portal (eShare) is a website accessible only to S&L law enforcement agencies to electronically submit and track the status of their Equitable Sharing requests. An "Equitable Sharing" request is a mechanism used by the Department of Justice to distribute an equitable share of forfeited property and proceeds to participating S&L law enforcement agencies that directly participate in an investigation or prosecution that result in a federal forfeiture. Each participating S&L law enforcement agency is required to submit an authorized Equitable Sharing request for a percentage of the forfeited proceeds or property. eShare has the built in capability to retrieve information by name of the submitter of the Equitable Sharing Request Form.

- Online Claim and Petition Application—The Online Claim and Petition (OCP) is a public facing online web application, available through Forefiture.gov, designed to allow individuals the ability to electronically file a claim of interest in the property or a petition contesting the forfeiture of property seized by the United States Government. The OCP application is managed by FS using backend services that consist of an Interface that transfers data to CATS and acts as a front-end monitor for the OCP application. Upon initial entry of data into OCP, the system auto-generates a tracking number that uniquely identifies each claim or petition filed. The claim or petition information is automatically merged, including all other supporting

[3] This PIA covers JMD's use of SharePoint only as it relates to FS. Other DOJ uses of SharePoint may be covered by other privacy documentation.
[4] The Forfeiture.gov webpage is publically available at: https://www.forfeiture.gov/.
[5] All DOJ websites are governed by the DOJ Website Privacy Policy, available at: https://www.justice.gov/doj/privacy-policy.

documents attached by the public user, and uploaded to the eDocs application as a single .pdf file. The merged documents will be immediately available in CATS via the existing eDocs link. The CATS and eDocs link will provide a complete record of the claim or petition filed by the public user. The relevant agencies responsible for the claim or petition are notified via email message and conduct the claim or petition evaluation process in accordance with the Federal statutes of asset forfeiture.

(c) The type of information collected, maintained, used, or disseminated by the system;

FS covers persons and economic entities involved with the ownership of, or claims upon, property seized for forfeiture under specified federal statutes and law enforcement policies. These persons and economic entities include owners, victims, individuals possessing or controlling the property, other parties provided notification of the seizure, lienholders, parties filing claims in contest of the seizure, attorneys, custodians, petitioners, paralegals assistants, district judges, case handlers, and S&L law enforcement agents. The FS forfeiture categories include information such as:

- Asset identification (Asset ID) and description;
- Names and relevant information about owner(s), victim(s), agents, attorneys, custodians, petitioners, paralegals assistants, district judges, case handlers, and S&L law enforcement agents;
- Property address, agency address;
- Property ownership details;
- Possession and custodianship details;
- Information of other parties involved in the forfeiture of a specific asset;
- Claims and claimant information; and
- eDocs documents (e.g., pictures, notices, memos) associated with the forfeiture of a specific asset.

(d) Who has access to information in the system;

All FS user accounts are configured to allow only authorized users access to the data they have privileges to access based on a "need to know." Authorized users may include employees and contractors from DOJ, Federal Government participants, and S&L law enforcement agencies. The exceptions to this are the Forfeiture.gov, eShare, and OCP applications in the FS-Non-FinSys system, which are publically accessible via the internet. The Forfeiture.gov site provides the official public noticing of forfeiture related actions as required by law. Although publicly accessible via the Internet, access to the eShare application by S&L law enforcement representatives is authorized and managed by FS.

(e) How information in the system is retrieved by the user;

The FS users' access to the system is controlled by a single sign-on mechanism identified as Single Authentication. The FS contractor support staff may be able to access the

system information directly by logging into applications and databases.

Information for FS-FinSys is accessed via the CATS application and/or CART. Information in FS-Non-FinSys applications is retrieved using built-in standard and custom queries and reports. The Forfeiture.gov, OCP, and eShare applications are available via publically accessible Internet websites. Forfeiture.gov does not require user authentication to access the information. Conversely, eShare requires appropriate identification and authentication prior to allowing access to the application.

(f) How information is transmitted to and from the system;

FS information is transmitted electronically in a secure encrypted manner via the DOJ Justice Unified Telecommunications Network (JUTNet). All FS user accounts are configured to allow only authorized users access to the data they have privileges to access based on "need to know." All information transmitted on Forfeiture.gov is done via the Hyper Text Transfer Protocol Secure (HTTPS) protocol using Secure Sockets Layer (SSL) encryption, compliant with the Federal Information Processing Standard Publication (FIPS) 140-2.[6] FS employs a two-way transfer of data specifically intended as a means to acknowledge receipt of the public notification and confirm its successful posting. No data intended for public notification is contained in the two-way transmission.

(g) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects);

FS have existing interconnections with the following information systems:

- Drug Enforcement Administration (DEA) Integrated Information Technology for Investigative Management and Case Tracking (CONCORDE)-DEA Statistical Management and Asset Recovery Tracking System (SMARTS);
- Justice Consolidated Office Network, Criminal Division (CRM-JCON IIA);
- U.S. General Services Administration Federal Asset Sales System (FAS);
- FS-General Support System / Single Authentication;
- Justice Unified Telecommunications Network (JUTNet);
- Justice Operations Services Staff Infrastructure Services;
- U.S. Customs and Border Protection Seized Assets and Case Management System (SEACATS);
- Unified Financial Management System (UFMS); and
- Bureau of Alcohol, Tobacco, Firearms and Explosives National Field Office Case Information System (NFOCIS);

FS also maintains existing and planned interconnections with information and information systems maintained by internal DOJ components, such as the DOJ Criminal

[6] NIST FIPS 140-2 can be found at: https://csrc.nist.gov/groups/STM/cmvp/standards.html.

Division, Money Laundering and Asset Recovery Section (MLARS), and the OCDETF. FS also maintains existing and planned interconnections with information and information systems maintained by Federal Government participants, such as United States Postal Inspection Service, United States Secret Service, and the Department of Treasury. Such interconnections are limited to those used to facilitate the FS purpose in supporting the Asset Forfeiture Program and providing a consolidated asset forfeiture management solution.

(h) Whether it is a general support system, major application, or other type of system.

FS-FinSys is a major application that is a Sensitive-But-Unclassified (SBU) inventory database system. FS-Non-FinSys is a minor application.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated.

(Check all that apply.)

Identifying numbers					
Social Security	X	Alien Registration		Financial account	X
Taxpayer ID	X	Driver's license		Financial transaction	X
Employee ID		Passport		Patient ID	
File/case ID	X	Credit card			
Other identifying numbers (specify): Prisoner ID, Business Taxpayer Identification Number (TIN). Although not required, a SSN or TIN may appear on documentation stored in the eDocs application repository.					

General personal data					
Name	X	Date of birth		Religion	
Maiden name		Place of birth		Financial info	X
Alias	X	Home address	X	Medical information	
Gender	X	Telephone number	X	Military service	
Age		Email address		Physical characteristics	
Race/ethnicity	X	Education		Mother's maiden name	
Other general personal data (specify):					

Work-related data					
Occupation		Telephone number	X	Salary	
Job title	X	Email address	X	Work history	
Work address	X	Business associates			

Work-related data
Other work-related data (specify): MLARS Online SharePoint application may include other work-related data, such as prior agency(s) or occupational titles. This application is only accessible to Federal employees and contractors.

Distinguishing features/Biometrics - N/A					
Fingerprints		Photos	X	DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Voice recording/signatures		Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify): Photos of Federal employees or contractors may appear in the MLARS Online SharePoint application.					

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	X
IP address	X	Queries run	X	Contents of files	X
Other system/audit data (specify): eDocs may store specific documents found in the case files.					

Other information (specify)
These systems do contain a comment field where agencies can enter any free-form text which could potentially contain PII.

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains					
In person	X	Hard copy: mail/fax	X	Online	X
Telephone	X	Email	X		
Other (specify):					

Government sources					
Within the Component	X	Other DOJ components	X	Other federal entities	X
State, local, tribal	X	Foreign	X		
Other (specify): Information collected from state, local, tribal, or foreign entities is inputted to the system by users at DOJ or Federal agencies.					

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

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

A potential threat to privacy in light of the information collected is that the system will collect and/or maintain more information than is relevant and necessary to accomplish the Department's official duties. DOJ and Federal Government participants in the Asset Forfeiture Program are the data owners, and are the responsible parties for collection limits and accuracy determinations. In order to assist in mitigating these risks, the investigative agency informs the party that only supporting evidence may be submitted. In addition, there are existing technical, administrative, and physical limits on the type of information that may be collected within FS, including but not limited to, the statutory protections afforded certain information under the Privacy Act of 1974 and DOJ policy, which limits the type and quantity of information collected to only information that is relevant and necessary to accomplish a purpose of the Department. To further mitigate these risks, on an annual basis, all users undergo mandatory Computer Security Awareness Training (CSAT) and acknowledge Information Technology Rules of Behavior for their respective agency. Finally, AFMS maintains Memoranda of Agreement (MOAs) or Inter Connection Documents (ICDs) for interconnected systems with other DOJ components, Federal Government participants, and S&L law enforcement agencies where all parties mutually agree to terms that include processes and procedures on the data collected as part of the Asset Forfeiture Program.

Another potential threat to privacy in light of the sources of the information is the risk that the collected information is inaccurate because much of the information maintained by FS is not collected directly from the data subject. As a host of information and repository of communications, FS itself is not the original collection platform for much of the information that it maintains. For example, documents attached to emails or stored in collaboration repositories for official business purposes may contain information that was created before they are entered in FS and outside of the Asset Forfeiture Program. In order to mitigate such risks, Department policies require that components, to the greatest extent practicable upon collection or creation of PII, ensure the accuracy, relevance, timeliness, and completeness of information within the system.

Additionally, because DOJ personnel from multiple components use FS to help carry out their missions, the type of information sent through or stored in the system is governed by the various authorities delineating component forfeiture responsibilities and authorizing the collection and maintenance of forfeiture information to carry out such responsibilities. These authorities are listed in the various Privacy Act System of Records Notices (SORNs) that apply to the information in Asset Forfeiture Program depending on the nature of such information, how it is retrieved, and the Federal Government participants responsible for the information. In the SORNs, the agency

describes the scope of the categories of records that may be collected as well as the categories of individuals about whom information may be collected. These SORNs also describe how an individual whose information is maintained in the system of records may request an amendment to a record believed to be inaccurate, irrelevant, untimely, or incomplete.

FS offer additional controls such as unique user IDs with the least privileges, data integrity checks, data format constraints, security logs monitoring, virus checking, storage protection, transactional buildup and recovery with end-point encryption, and firewalls for secure routing and to regulate all internal-external communications to and from JUTNet. For information about security controls that have been applied to Forfeiture Systems, please see the responses to questions 6.1 and 6.2.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
X	For criminal law enforcement activities	X	For civil enforcement activities
	For intelligence activities	X	For administrative matters
	To conduct analysis concerning subjects of investigative or other interest	X	To promote information sharing initiatives
X	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
X	For litigation		
	Other (specify):		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

FS information is used for the execution, reporting, and management of the asset forfeiture process by AFMS on behalf of DOJ and its Federal Government participants. The information is used to track assets in the government's control and notify parties with an ownership or economic interest in the assets in government custody. Additionally, the information is used for management reports and monitoring performance of the program. FS assists Federal Government participants in facilitating certain types of Federal forfeiture actions,[7] including:

- Criminal forfeiture—Criminal forfeiture actions are brought as a part of the criminal prosecution of a defendant. It is an *in personam* (against the person) action and requires that

[7] More information on the types of Federal forfeiture actions can be found at: https://www.justice.gov/afp/types-federal-forfeiture.

the government indict (charge) the property used or derived from the crime along with the defendant. If the jury finds the property forfeitable, the court issues an order of forfeiture.

- Civil judicial forfeiture—Civil judicial forfeiture actions are brought as an *in rem* (against the property) action brought in court against the property. The property is the defendant and no criminal charge against the owner is necessary.

- Administrative forfeiture—Administrative forfeiture actions are *in rem* actions that permit the federal seizing agency to forfeit the property without judicial involvement.

The investigative agencies assigned the authority to seize and/or forfeit property investigate a broad range of criminal violations by integrating the use of asset forfeiture into the agency's overall strategy to eliminate targeted criminal enterprises. The forfeiture authority granted to the investigative agency allows the agency to conduct asset forfeiture proceedings in an effort to remove the proceeds and property acquired through criminal activity. In addition, various investigative agencies may form a joint asset forfeiture venture to coordinate resources, conduct an analysis of previous criminal activity, or document patterns and practices in use by networks or individuals involved in illegal activity. The agency granted legal authority is responsible for the prosecution of both criminal and civil actions against property used or acquired during illegal activity. Also, the agency granted specific asset forfeiture authority handles civil and criminal litigation, provides legal support to the investigative and legal agencies, establishes policy and procedure, coordinates multi-district asset seizures, administers equitable sharing of assets, acts on petitions for remission, and coordinates international forfeiture and sharing. An essential tool to support asset forfeiture is the equitable sharing program which grants the authorization to share federal forfeiture proceeds with cooperating S&L law enforcement agencies.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

	Authority	Citation/Reference
X	Statute	-21 U.S.C. § 881 – Civil Forfeitures -21 U.S.C. § 853 – Criminal Forfeitures -18 U.S.C. § 1956 – Money Laundering -18 U.S.C. §§ 1961–1968 – Racketeer Influenced and Corrupt Organization Act (RICO)
	Executive Order	
X	Federal Regulation	28 C.F.R. Part 9
X	Memorandum of Understanding/agreement	Various MOAs and ICDs detailing the terms of access and use of interconnected systems with other DOJ components, Federal Government participants, and S&L law enforcement agencies. In general, other DOJ, Federal, and S&L law enforcement agency systems access data hosted on the FS Information Technology System

		(FSITS) application and database server in the Production environment via JUTNet. All aspects of the extract file creation, data transfer, and database load processes are automated with no manual intervention required.
X	Other (summarize and provide copy of relevant portion)	DOJ Policies: - Asset Forfeiture Policy Manual, 2016. - The Attorney General Guidelines on Seized and Forfeited Property, 9-118.000

3.4 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 collecting agencies retain the hardcopy of forfeiture case files for 7 years, which are then placed in federal archives in accordance with applicable authority. Hard copies are maintained for 15 years in the Federal Archive after final disposal from agencies. However, the electronic data is not destroyed, but maintained on a database or archived to several databases. Disposition Authority (Maintain with case file – N1-060-06-006), (Destroy/Delete 15 years after final disposition of the forfeited asset – N1-060-06-006, Item 001), (Destroy/Delete when superseded or obsolete – GRS 3.1, Item 051).

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

The consolidation, management, and use of FS information for the purpose of facilitating the Asset Forfeiture Program creates certain privacy risks. Specifically, Federal agency employees and contractors with elevated access may modify and manipulate sensitive information and PII, creating external and internal threats to the use of information.

To mitigate the internal threats to FS information, all users of FS information are required to complete annual CSAT training, acknowledge and sign an annual General User Rules of Behavior and Privileged User Rules of Behavior, where applicable, before using FS. Federal personnel must receive an approved completion of a background investigation and/or security clearance prior to receiving access to FS. The authorized privileged accounts assigned to Federal personnel are reviewed by FS on an annual basis to determine an active or non-active status. In addition, the privileged user accounts assigned to authorized Federal personnel are subject to a scheduled review of activity and access to information. FS has also implemented certain use controls and restrictions. Specifically, the Asset Forfeiture Policy Manual, which details the policies governing the Asset Forfeiture Program, details the use and disposition of seized and forfeited property. All FS user

accounts are configured to allow only authorized users access to the data they have privileges to access based on a "need to know." Authorized users may include employees and contractors from DOJ, other Federal Government participants, and S&L law enforcement agencies. All users have unique user IDs and the least privileges.

To mitigate external risks to FS information, FS has employed intrusion prevention and detection system tools to monitor malicious or suspicious activity on the information systems network. Specific information system configuration settings are deployed to only allow access to information from designated or authorized locations. FS deploys antivirus tools and system firewall rules to monitor, alert, or block suspicious or malicious transmission of data. FS also relies upon Department of Justice level network protection and monitoring tools to alert to potential threats on the information systems network. Finally, data is protected further by having data format constraints, virus protection, data encryption at rest and in transit, storage protection, and firewall rules for secure routing and to regulate all internal-external communications to and from JUTNet. Media and data communication is also protected via secure channels (for example, HTTPS for all public facing websites).

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component	X		X	
DOJ components	X	X	X	
Federal entities	X	X	X	
State, local, tribal gov't entities	X		X	
Public	X			Notice information will also be available via Forfeiture.gov.
Private sector				
Foreign governments				
Foreign entities	X			When related to an international case.
Other (specify):				

AFMS, as the manager of the system, will maintain direct access to all of FS. DOJ components and Federal Government participants, will have direct access to administrative, civil, and criminal forfeiture actions through the collaboration of case information pertaining to specific violators or organizations, the transfer of bulk information pertaining to certain types of criminal activity, direct access to FS, and cooperation with foreign law enforcement entities. Members of the public will

have access to administrative, civil, and criminal forfeiture actions through Forfeiture.gov, submit claim and petition applications through OCP, and may make requests through the Privacy Act and the Freedom of Information Act, where appropriate. S&L law enforcement agencies will have access to the eShare Equitable Sharing requests, as described above in Section 1.

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)

The Department has implemented numerous and varied controls in order to mitigate risks in connection with the sharing of information outside of the Department. Specifically, the Asset Forfeiture Policy Manual, which outlines the policies governing the Asset Forfeiture Program, details the roles and responsibilities of Federal Government participants, including their custodial and seizure authorities. Additionally, all users undergo mandatory CSAT that outlines general privacy protections. All users are required to review and sign Rules of Behavior for their respective agency annually. AFMS has MOAs and ICDs with other DOJ components, Federal Government participants, and S&L law enforcement agencies. The data is sanitized, scrubbed, and/or redacted for congressional inquiries and FOIA requests. For information about security controls that have been applied to FS that further assist in mitigating risks associated with sharing information, please see the responses to questions 6.1 and 6.2.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
X	Yes, notice is provided by other means.	Specify how: To alert individual(s) to the violation of a DOJ asset forfeiture seizure statute, notice letters are mailed to the last known address of the violator and/or other persons who may have an interest in the seized property. Internet and newspaper advertising mediums are also used to alert other individuals who may have an interest, but were not identified in the initial investigation.
	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

	Yes, individuals have the opportunity to decline to provide information.	Specify how:
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: Information about individuals who are alleged to have performed criminal acts is generally not collected directly from such individuals, or is collected in the course of an investigation or case, so individuals do not have an opportunity to decline.

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: Consent is not required for uses of the information that fall within the statutes and regulations governing the Asset Forfeiture Program.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

As detailed above, clear and conspicuous notice is provided, where appropriate. As detailed in Section 7, SORNs have been published in the Federal Register, including but not limited to JUSTICE/JMD-022, Department of Justice Consolidated Asset Tracking System. Additionally, notices of administrative, civil and criminal forfeiture actions have been made available to the public at Forfeiture.gov. However, certain notices and the opportunity of consent is not required for all uses of the information that fall within the statutes and regulations governing of the Asset Forfeiture Program.

Section 6: Information Security

6.1 Indicate all that apply.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: FS-FinSys:09/20/2013, FS Non-FinSys:10/24/2014 If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date:	
X	A security risk assessment has been conducted.	
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: FS and its subsystems have a security categorization of Moderate. FS, with guidance from the DOJ Office of the Chief Information Officer, Cybersecurity Services Staff, identified enterprise-level security controls to be implemented and tested. To the extent possible, DOJ Common Controls and hybrid security and privacy controls have been inherited from existing systems and programs to reduce the assessment effort and streamline the Security Assessment and Authorization process. The security and privacy controls that have been identified, tested, and implemented to protect against risks identified in the security risk assessment include those listed in DOJ Security and Privacy Assessment and Authorization Handbook v. 9, which provides the framework and direction for performing security assessments and authorizations of all DOJ information systems, as well as those listed in response to question 6.2.	
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: Symantec Endpoint Encryption and Microsoft System Center software are in place. Nessus vulnerability scans of system components are executed weekly. IBM Tivoli Endpoint Lifecycle Management System (BigFix) is in place for continuous monitoring. App Scanner scans for vulnerabilities of databases and websites respectively are also executed quarterly.	
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: Role-based audit logs are kept and reviewed weekly by the FS Information System Security Officer (ISSO).	
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.	
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.	
X	The following training is required for authorized users to access or receive information in the system:	
	X	General information security training
	X	Training specific to the system for authorized users within the Department.
	X	Training specific to the system for authorized users outside of the component.
	X	Other (specify): Acknowledgement of the DOJ Rules of Behavior Including any auditing of role-based access and measures to prevent misuse of information.

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

FS-FinSys was designed and developed in accordance with the DOJ Cybersecurity Standards and the security and privacy controls found in the National Institute of Standards and Technology (NIST), Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, revision 4,[8] to ensure minimal risk to the data. Security controls include the following:

- FS is accessible by DOJ employees and contractors only and utilizes tiered/role-based access commensurate with the end-user's official need to access information.

- The system is protected by multiple firewalls, an intrusion prevention system, real-time continuous monitoring using malicious code detection and protection, encryption, and other technical controls in accordance with applicable security standards (including DOJ Order 0904 and FIPS 140-2).

- All FS users must complete CSAT training annually, as well as read and agree to comply with DOJ information technology Rules of Behavior both prior to accessing the DOJ network and annually thereafter. System administrators must complete additional professional training, which includes security training.

- Audit logging is configured and logs are maintained separate from other system data to help ensure compliance with tiered/role-based access as well as to help safeguard against unauthorized access, use, and disclosure of information. Audit logs can only be accessed by authorized users with privileged access. System administration/audit data is automatically purged at defined intervals and in accordance with applicable retention periods.

- All users must complete CSAT annually, as well as read and agree to comply with DOJ Information Technology Rules of Behavior, prior to accessing FS and annually thereafter.

FS is configured with automatic audit logging which includes logging of FS administrator activity. Further, logs are maintained separate from other system data to help ensure compliance with tiered/role-based access as well as to help safeguard against unauthorized access, use, and disclosure of information.

[8] NIST SP 800-53, and other available NIST resources, can be found at: https://csrc.nist.gov/.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: • JUSTICE/DOJ-002, Department of Justice Computer Systems Activity and Access Records, last published in full at 64 Fed. Reg. 73585 (Dec. 30, 1999), and modified at 66 Fed. Reg. 8425 (Jan. 31, 2001), and 82 Fed. Reg. 24151, 153 (May 25, 2017); • JUSTICE/JMD-022, Department of Justice Consolidated Asset Tracking System (CATS), last published in full at 71 Fed. Reg. 29170 (May 19, 2006), and modified at 82 Fed. Reg. 24151, 153 (May 25, 2017); and • Other published SORNs maintained and controlled by other DOJ components and Federal Government participants with authorities delineating forfeiture responsibilities and authorizing the collection and maintenance of forfeiture information to carry out such responsibilities, depending on the nature of such information and how it is retrieved.
X	Yes, and a system of records notice is in development. • JUSTICE/JMD-022 is in the process of being modified and renamed "Forfeiture Systems," to better articulate to the public the nature and character of the applicable system of records.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

Information in the system about United States citizens and/or lawfully admitted permanent resident aliens is retrieved in the same manner as in FS-FinSys and FS-Non-FinSys. Specifically, information is stored in limited-text and/or free-text data fields and is retrieved by conducting a search of fields such as the unique asset ID, property description (e.g., bank account label, residential or commercial address, personal property), account number, type of asset, name(s), address(es), phone number(s), and other identifying information about owners, victims, agents, attorneys, custodians, petitioners, paralegals, assistants, district judges, case handlers, and state and local law enforcement agents, property and/or agency address, possession and custodianship details, claims and claimant information, and Tax Identification Numbers (of vendors supporting the program).