United States Department of Justice
Justice Management Division

Privacy Impact Assessment

for the

Forfeiture Amazon Web Services (FS-AWS)

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:	March 2, 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.)

Amazon Government Cloud provides Platform-as-a-Service (PaaS) operations in support of the Department of Justice (DOJ) Justice Management Division (JMD) Asset Forfeiture Management Staff (AFMS). AFMS is legally required to advertise to the public and interested parties, property seized as a result of administrative, civil, and criminal asset forfeiture proceedings. The Forfeiture Systems, Amazon Web Services (FS-AWS) is the Cloud system that allows the storage of seized asset advertisement text in .pdf format. In addition, FS-AWS provides a mechanism to search through the advertisement text using various data fields related to the seized assets. The official Government web site for public noticing of interested parties when an asset is seized is Forfeiture.gov (www.forfeiture.gov). To allow the user on-line access to the seized asset advertisement, FS-AWS is hosted on the Forfeiture.gov website. The Forfeiture Systems, Financial System (FS-FinSys)[1] is the system used to generate the advertisement text in .pdf format and transmit the files to FS-AWS for storage. FS-AWS prepares the .pdf files for posting to the Forfeiture.gov website and provides members of the public the ability to search for seized asset data using criteria such as keywords, property description, name, and address, city, state.

When a public user opens the Government web site, the user is informed that the items listed are not for sale and is presented with menu options regarding the operation of Forfeiture.gov. Usage instructions explain the processes for both basic and advanced advertisement searches. The user may proceed to enter data in specific fields to narrow the scope of the search for seized assets.

In addition, the www.forfeiture.gov web site allows a public user to file a claim contesting a seizure activity and request to have the matter litigated in U.S. District Court. Alternatively, the public user may file a petition which is the method for individuals and entities with no allegations of criminal activity against, to declare their ownership interest in property seized by law enforcement agencies. The instructions to file a claim or petition and corresponding documents or forms are provided to the public user. The public user will submit the claim or petition form, generally in PDF format, to the Government. FS-AWS only displays text with instruction to file a claim or petition. FS-AWS is not the application used to collect this information. FS-NON-Financial System and FS-Financial System include the applications to collect and store claim and petition information[2].

A Privacy Impact Assessment (PIA) has been conducted because FS-AWS is used for authorized purposes to maintain, use, and disseminate information in identifiable form, including, but not limited to, names and personal contact information. This information is linked or linkable to individuals and are considered personally identifiable information (PII).

[1] FS-Financial System is covered by separate privacy documentation.
[2] FS-NON-Financial System is covered by separate privacy documentation.

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-AWS information technology is to provide a publicly available method to disseminate seized property information in accordance with applicable asset forfeiture statutes and regulations. The advertisement of seized property is publicly accessible on a continuous basis and grants all owners, businesses, and/or other interested parties the ability to claim and/or petition for the return of the property pursuant to asset forfeiture laws. The seized property information may be shared with other Department components, and federal, state, local, and tribal agencies in support of administrative, civil, and criminal asset forfeiture proceedings. Components and agencies may share information to identify subjects in a related case, analyze and identify greater criminal network activity, and to overall strengthen and support asset forfeiture case processing and legal proceedings. In addition, information is shared with other components and agencies to track, monitor, and process federal financial activities related to the asset forfeiture proceedings.

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.
Executive Order	
Federal regulation	28 C.F.R. Part 8.9, Notice of administrative forfeiture.
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	(Federal Rules of Civil Procedure, XIII. Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions, Rule G, Forfeiture Actions in Rem); Federal Rules of Criminal Procedure, Rule 32.2, Criminal Forfeiture (section (b)(6)).

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	C and D	Names of members of the public (US and non-USPERs)
Date of birth or age			
Place of birth			
Sex			
Race, ethnicity, or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers	X	C and D	VIN collected to identify specific seized property
Personal mailing address			
Personal e-mail address			
Personal phone number			
Medical records number			
Medical notes or other medical or health information			
Financial account information	X	C and D	Financial account information collected to identify specific seized property
Applicant information			
Education records			

(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

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			
Device identifiers, e.g., mobile devices	X	C and D	Mobile devices, other electronic equipment identifiers such as serial number or model number collected to identify specific seized property
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			

(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

- **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**			
- **User passwords/codes**			
- **IP address**	X	C and D	IP address collected by on-line auditing resource intended to capture IP address
- **Date/time of access**			
- **Queries run**	X	C and D	Audit log produce by resource designed to capture IP address
- **Contents of files**			
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 (International requests for legal assistance in asset recovery are subject to various treaty and other obligations and may often implicate issues of diplomatic sensitivity or require coordination with other related investigations, domestic or foreign. They accordingly require consultation with the	X	Department of Defense, Defense Criminal Investigative Service, State Department, Diplomatic Security Service, Food and Drug Administration, Immigration and Customs Enforcement, the Internal Revenue Service, Tax and	X

Government sources:					
		DOJ's Money Laundering and Asset Recovery Section (MLARS) and Office of International Affairs (OIA, International Sharing)		Trade Bureau, US Coast Guard, US Department of Agriculture, US Postal Inspection Service, Secret Service	
Other (specify):					

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	JMD provides direct login access to AFMS users and administrators.
DOJ Components				
Federal entities				
State, local, tribal gov't entities				
Public	X	X		Property seized for advertisement is publicly available
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X	X		Public users may file a claim contesting a seizure activity and request to have the matter litigated in U.S. District Court.
Private sector				
Foreign governments				
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.

Not applicable. Seized asset information in FS-AWS is publicly available via Forfeiture.gov, but is not intended for "Open Data" and/or for research or statistical analysis 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.

FS-AWS does not collect PII from users of Fofeiture.gov. Included on the forfeiture.gov website are links that the public user may select to submit a claim of ownership interest or a petition for the return of the property. These links provide a path to a separate application contained within the FS-NON-Financial System (FS-NON FinSys) boundary. FS-AWS allows users of the website to view, search, and print advertisements of seized assets. FS-AWS provides notice of, and is maintained in accordance with, DOJ's privacy policy. The collection, use, sharing, or other processing of an individual's PII is conducted by separate applications contained within the FS-Financial System (FS-FinSys) and FS-NON-Financial System (FS-NON FinSys) boundaries. Once the PII is collected within the two system boundaries mentioned above, the seized asset information data that is appropriate for public advertisement is posted to FS-AWS.

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 FS-AWS. The information in the system is collected from the Consolidated Asset Tracking System (CATS), a web application that system that is designed to track, throughout the forfeiture life cycle, assets seized by federal law enforcement agencies. AFMS employs FS-AWS to maintain and disseminate seized asset information identified for public notice via Forfeiture.gov. Consent is not required for uses of the information that fall within the statutes and regulations governing the Asset Forfeiture Program.

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):** ATO completed on September 9, 2022; ATO expires on September 9, 2025. **If an ATO has not been completed, but is underway, provide status or expected completion date:** **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:** No POAMs assigned.
	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:** The FIPS 199 designation for FS-AWS is Moderate. The information posted for public advertisement is retrieved from the FS-Financial System which maintains data categorized as sensitive but unclassified. Specific data displayed in the public advertisement may be considered PII. The FS-Financial System maintains a FIPS 199 designation of Moderate. In addition, FS-AWS information technology is supported by FS-GSS which contains sensitive but unclassified information. The FS-GSS maintains a FIPS 199 designation of Moderate. Because of FS-AWS dependence on FS-Financial System and FS-GSS to operate as intended, the FIPS 199 designation of moderate is applied to FS-AWS**.**
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse.**

	The computer servers supporting FS-AWS are built with secure configuration policies such as the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs). IBM Endpoint Lifecycle Management System (ELMS) is deployed to continuously monitor and identify component assets. Vulnerability assessments and risk management procedures are executed on a weekly and monthly basis on operating systems (OS), software applications, and database resources. Amazon Web Services (AWS) devices are built and provisioned using Amazon Machine Images (AMI) to ensure appropriate secure configuration policies are applied. Software protection applications such as a 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 FS-AWS. In addition, AWS 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). The AWS Virtual Private Cloud (VPC) Firewall provides in-depth security protection through ACL to manage access within the VPC. AWS Elastic Load Balancer in VPC is used to hide internal resource information from being visible to external internet users. AWS Web Application Firewall (WAF) and CloudFront network monitoring are deployed to provide security protection at the edge location for the FS-AWS public facing application through inspecting "hits" to applications hosted in the AWS environment**.**
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 audit 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 prevention system (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) for review. In addition, the Amazon Web Services (AWS) CloudTrail IT traffic monitoring service is used to audit AWS accounts and Application Programming Interfaces (API) data transmissions on a continuous basis**.**
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 conduct specific privacy-related training in addition to the foundational privacy-related training included in the 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?

FS-AWS is a Cloud environment consisting of AWS GovCloud and AWS-S3 for storage in AWS Commercial Cloud. Access to the FS-AWS system is protected by network tools and services such as the Department's Trusted Internet Connection (TIC) for traffic inspection over the Virtual Private Network (VPN), CrowdStrike Endpoint Detection and Response (EDR) for network monitoring, and AWS Web Application Firewall (WAF) services to secure and control access to data. All Windows and Linux Server technical specifications such as random-access memory (RAM) size, hard disk space or size, and processor configuration and speeds are in accordance with Department standards and requirements. All pertinent system application patches and updates are applied using the respective Windows or Red Hat Linux server device recommendations. Also, secure configuration settings are deployed in accordance with Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG's), National Institute of Standards and Technology (NIST) recommendations, Vendor recommended security settings, Red Hat Linux upgrades, and recommended computer security best practices. After standard technical specifications, secure configuration settings, and system applications are deployed, additional server configuration settings are applied according to Server Build Documentation and Checklist instructions used to ensure all monitoring agents (IBM BigFix, Infrastructure Analysis, System Center Configuration Manager (SCCM), etc.) are installed and latest patches are applied. AFMS conducts monthly operating system (OS), web application, and database vulnerability assessments, in accordance with Department IT security policy.

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 information in FS-AWS is retained for 15 years after the final disposition of the forfeited asset. Disposition authority: Consolidated Asset Tracking System, N1-060-06-006 (Destroy/delete 15 years after final disposition of the forfeited asset).

<u>Section 7</u>: 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.

DOJ users and members of the public have the ability to search for seized asset data in the system on Forfeiture.gov using criteria such as keywords, property description, individual name, and address, city, state.

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 FR 29170 (5-19-2006)
72 FR 3410 (1-25-2007) (rescinded by 82 FR 24147)
82 FR 24147 (5-25-2017)
E6-7571.pdf (govinfo.gov); and

DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records
64 FR 73585 (12-30-1999)
66 FR 8425 (1-31-2001)
72 FR 3410 (1-25-2007) (rescinded by 82 FR 24147)
82 FR 24147 (5-25-2017)
86 FR 37188 (7-14-2021)
2021-14986_-_doj-002_sorn_update.pdf (justice.gov)

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.***

A potential threat to privacy exists in light of the information used, maintained, and publicly shared by FS-AWS on Forfeiture.gov. This information pertains to individuals who have property seized as the result of administrative, civil, or criminal forfeiture actions, and may include, but may not be limited to name, personal contact information, financial account number, and/or vehicle identification number. The advertisement of seized assets/property us publicly posted for a designated time period, as necessary to provide interested parties and/or subjects of the forfeiture proceedings sufficient opportunity to petition for or claim ownership of the assets.

The information in FS-AWS sourced by CATS is often retrieved directly from individuals who are the subject of asset forfeiture actions. However, other sources of information may be used to accurately identify subjects or gather additional evidence, including the federal agency conducting the financial investigation, or state or local law enforcement agencies conducting civil or criminal investigations. This information is initially collected, stored, and processed by the CATS application. A subset of this information, that is deemed appropriate for release to the public and may include PII, is posted to FS-AWS as a .pdf document and presented in the form of a public advertisement. An essential mechanism included in the forfeiture proceedings is the collaboration among federal and state or local law enforcement agencies that participate in the asset forfeiture program. Investigative information sharing and analysis of methods of operation used by criminals and criminal organizations are used to collect evidence and secure a successful forfeiture of seized property to the government.

After the seizure of property for administrative forfeiture is executed, the federal agency is required by law to send notification of the seizure of property to interested owners or parties, by use of United States Postal Service mail, within sixty (60) days from date of seizure or ninety (90) days from date of seizure by a state or local law enforcement agency. In addition, to serve notification to other potential interested parties or owners, the federal agency is required by law to publicly advertise the seized property on the internet for thirty (30) consecutive calendar days. The internet advertisement of seized property is executed by FS-AWS. The operations performed to collect the information and prepare for notification and public advertisement are conducted in the CATS application. The federal agency completes the required notification to the interested party(s) or subject(s) of the seizure to ensure awareness of the collection of PII, its use, and the methods to contest the federal seizure and forfeiture proceedings in accordance with law. The federal agency executes the required notification to the interested party(s) or subject(s) of the seizure to ensure awareness of the collection of PII, its use, and the methods to contest the federal seizure and forfeiture proceeding in accordance with law.

To mitigate privacy risks, there are existing technical, administrative, and physical limits on the type of information that may be collected within FS-AWS, including, but not limited to, 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. DOJ policies also require that components, including AFMS, to the greatest extent practicable upon collection or creation of PII, ensure the accuracy, relevance, timeliness, and completeness within the system. Additionally, the type of information in the system is governed by the various authorities delineating DOJ forfeiture responsibilities and authorizing the collection, maintenance, and use of the information to carry out such responsibilities. These authorities are listed above, as well as in the various Privacy Act System of Records Notices that apply to the information in FS-AWS.

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. Finally, AFMS maintains Memoranda of Agreement (MOUs) with other DOJ components and federal government participants, whereby all parties mutually agree to terms that include the processes and procedures for handling the data collected as part of the Asset Forfeiture Program. For the state and local law enforcement agencies, the Department's Criminal Division/Money Laundering and Asset Recovery Section (CRM/MLARS) maintains Memoranda of Agreement (MOU) and Certification documents in reference to rules and requirements for participating in the Asset Forfeiture Program. AFMS manages the applications used by CRM/MLARS and the state and local law enforcement agencies to facilitate the collection of information and corresponding agreements. The applications are contained within the FS-Non FinSys.

For information about security controls that have been applied to FS-AWS, please see the responses to questions 6.1 and 6.2, above.