DOJ Privacy Impact Assessment (PIA) Template

Part One: Is a PIA required?

Instructions for Questions 1-4: If you answer "yes" to **any** of Questions 1-3 **and** Question 4, go on to the next question. If you answer "no" to **all** of Questions 1-4, please briefly describe the IT system that is at issue, and submit this document for review under the PIA process.

1. Are you developing or procuring a new IT system or project that collects, maintains, or disseminates information about individuals?

   Yes. Performing a technical refresh of the legacy application, migrating existing business rules and functionality from mainframe architecture to server based architecture, for this reason we have concluded that a Privacy Impact Assessment is required.

2. Are you initiating a new electronic collection of information under the Paperwork Reduction Act?

   No

3. Are you making a change to an existing IT system that creates new privacy risks?

   a) Are you applying a new technology to an existing system that significantly changes how information is managed in the system?

   No

   b) Are you making a change in business processes:
      i. that merges, centralizes, matches or otherwise significantly manipulates existing databases?

      No

      ii that results in significant new uses or disclosures of information or incorporation into the system of additional information?

      No

   c) If this information has been collected previously:
      i. Are new or significantly larger groups of people being impacted?

      No

      ii. Is new data being added resulting in new privacy concerns?

      No

iii. Is data being added from a commercial or public source?

No

4. Is this information individually identifiable? (Does this pertain to specific individuals who can be identified either directly or in conjunction with other data?) If no, submit this document for review under the PIA process. If yes, continue to the next question.

Yes

Instructions for Questions 5-7: If you answer "yes" to any of Questions 5-7, submit the required documentation for review under the PIA process. If you answer "no" to a question, continue on to the next question.

5. Does this information pertain only to government employees or contractors? If yes, submit this document for review under the PIA process. If no, continue to the next question.

No

6. Has a PIA or similar evaluation been conducted? If yes, does the existing PIA address the questions in Part Two? If yes, submit the existing PIA with this document for review under the PIA process. If no, continue to the next question.

No

7. Is this a national security system as defined at 40 U.S.C. 11103? If yes, please attach verification and submit this document for review under the PIA process. If no, continue to Part Two.

No

Part Two: Preliminary PIA (Routine database systems)

1. Identify the component system sponsor and the point of contact (name, job title, phone number, fax number, room number, and email address).

Asset Forfeiture Management Staff
Jade Tavaglione, Asst Director, CATS
202/353-4344 (tel)
202/616-8100 (fax)
20 Massachusetts Avenue NW, Suite 6400
jade.Tavaglione@usdoj.gov

2. Identify the component system developer and the point of contact (name, job title, phone number, fax number, room number, and email address).

Asset Forfeiture Management Staff
Neill Roe, Information Technology Specialist
202/616-1897 (tel)
202/616-8100 (fax)
20 Massachusetts Avenue NW, Suite 6400
neill.d.roe@usdoj.gov

3. Please provide a general description of the system, including the purpose of the system.

System Description: The CATS is a Sensitive-But-Unclassified (SBU) database system which stores and processes asset forfeiture data maintained by DOJ entities and others. The data is used to support annual financial statement preparation and audit and for Congressional reporting, as well as to enable management to meet a wide range of accountability regarding seized and forfeited assets. Only non-sensitive information is allowed for processing within the CATS application. CATS performs functions involved in the execution of the asset forfeiture program including; tracking, inventory, status inquiry, notice production, advertising property production, equitable sharing reporting, and management decision support. CATS capabilities include system administration, data inquiry, document generation, and other procedural functions.

4. Please describe the types of records that will be contained in the system and the categories of individuals to whom the records pertain.

Major categories and types of records/reports available in CATS are listed below:

Seizure -	**Information pertaining to the seizure location, agency, applicable statute(s), property and individuals from whom the property was seized.**
Custody -	**The temporary and permanent guardianship for the seized property, managing the asset while in Federal care.**
Notice -	**Data used to inform interested parties of the seizure, the circumstances surrounding the seizure, and the remedies available to them.**
Claims -	**Data associated with receiving a claim from parties wanting to contest the forfeiture of seized property or assert any valid liens.**
Petitions -	**Data related to receiving and processing of appeals of parties who desire full or partial pardon of the forfeiture of seized property.**
Forfeiture -	**Data pertaining to administrative and judicial forfeiture**

decisions, disposal arrangements, and notifications to other agencies that forfeiture has occurred.

Disposal - **Pre-forfeiture and post-forfeiture disposal instructions from the investigative agencies or the court through the U.S. Attorney. Disposition of the physical asset involves any one of several different methods and closing the file on the asset after final disposition has occurred.**

Sharing - **Data pertaining to equitable sharing requests by a State or local law enforcement agency and the recommendation/decision made by the seizing agency and/or the U.S. Attorneys Office.**

Official use - **Data pertaining to the proper authorizations to use a forfeited asset and the transfer to a particular agency.**

Financial - **Financial data pertaining to seized property.**

System - **Administrative functions and facilities including security and access control.**

Abandonment - **Data identifying an abandoned asset and abandoned asset claim**

Service - Of Process **Data tracking documents served or executed by the USMS.**

5. What is the volume of records that will be contained in the system, including approximate number of people impacted?

There are approximately 820K records currently in the database that contain information on parties (specifically, names, TIN, SSN, location of interested parties)

6. What is the purpose for which the system data will be used, including how it will be used and who will use it?

CATS PURPOSE:

a) **<u>Extent to which system data is used to identify previous criminal offenses, identify individuals subject to the criminal justice process, or conduct criminal or intelligence investigations</u>;**

The System covers individuals involved with the ownership of or claims upon property seized for forfeiture under specified federal statutes and law enforcement policies, including owners, individuals possessing or controlling the property, other parties provided notification of the seizure, lienholders,

parties filing claims in contest of the seizure, petitioners, U.S. Attorneys, Investigative Agents and contractors of the Government. CATS data is not used to identify previous criminal offenses, or to identify individuals subject to the criminal justice process. Some individuals from whom property is seized may be subject to the criminal justice process, but CATS is not used as a source for this information. CATS is not used to conduct criminal or intelligence investigations.

Asset ID numbers, Seizure numbers, Asset Descriptive identifiers such as VINS, license numbers, model numbers, and agency case numbers, have been declared exempt from release to the public under FOIA Exemption (7)(F). The Privacy Act bars disclosure of any record which is contained in a system of records that falls within a FOIA exemption.

b) <u>Extent to which system data is required by statute to be maintained and used solely as statistical records</u>;

CATS data is used to support annual financial statement preparation and audit and for Congressional reporting, as well as to enable management to meet a wide range of accountability regarding seized and forfeited assets. A significant portion of the data is required by statute to be maintained and used for aggregate and statistical reporting purposes. Data on individuals is also required to assure the government fulfills fiduciary responsibility and can return property to the appropriate individual as circumstances warrant.

c) <u>Extent to which system data is used to determine suitability, eligibility, or qualifications for Federal employment, access to classified information or promotion</u>.

The CATS system is not used for any of these purposes.

7. What are the sources of the information?

Federal Government Investigative Agencies (ATF, DEA, FBI, USPIS) are responsible for entering and maintaining all seized assets in CATS, as well as all applicable notification, petition, equitable sharing, and forfeiture information. USAO personnel enter judicial forfeiture data and decisions on applicable equitable sharing requests. The USMS is responsible for entering most property management and disposal information, as well as financial transactions associated with the aforementioned activity into CATS.

8. With whom will the information be shared outside of the Department?

CATS is a closed system where data is only available to components of the Asset Forfeiture Program. Users for each component may <u>view</u> most of the data in CATS; however, each component is limited by its role within asset forfeiture as to what data they may input into CATS.

Certain information derived from CATS is published on the DOJ website in accordance with USC 28 524(c)(6)(A)(i thru vii). This data has been sanitized of all identifiers (case numbers, names, etc.) and therefore has no impact on individual privacy.

9. Is providing information voluntary? If yes, are individuals informed that they may decline to provide information?
No, information is initially captured from law enforcement activities.

10. Do individuals have an opportunity to consent to particular uses of the information? If yes, how can individuals grant consent?

No. Individuals have the opportunity to exercise their legal rights, including actions such as claims on seized property and defense against forfeiture.

11. How will the information be secured (e.g., administrative and technological controls)?

The information is secured in compliance with DOJ safeguarding policies such as access controls, infrastructure security, intranet controls, and application security.

12. Is this information covered by a Privacy Act System of Records Notice? If yes, provide the Federal Register Citation. If not, is one being created?

No. In accordance with our response to question 1, Part I, we are in the process of preparing a Federal Register notice.

13. Is this information covered by a Computer Matching Agreement? If yes, please attach

No

14. Is this a Major Information System as defined in OMB Circular A-130 and A-11 (Section 300-4). If yes, please include identifying information and complete Part Three.

Yes - UPI Code - 011-03-01-03-01-1020-00-407-191

15. Is this system of such significance or sensitivity, or is the impact on privacy such that the system requires special consideration of privacy risks? If yes, please briefly explain and complete Part Three.

No

16. Analysis: PIAs must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA.

Because this effort is a technology refresh, the business rules have long-standing been in effect. The origination of long-standing business rules and logic stems from the participating agencies and their law enforcement missions.

Part Three: Further Analysis (Major Information Systems, etc.)

1. Please briefly describe the impact on privacy.

   The impact on privacy is low, primarily due to the association of asset ownership or parties. Privacy information is collected on property owners, attorneys of record, interested third parties, and assorted other classifications as they pertain to asset ownership. The CATS team assessed several aspects of authenticating customers identity for inquiry of asset information transactions. This inquire-type action is executed by government employees and government contractors to enable all application users to query the system for asset information. The result set can be viewed on the screen or printed in report form. Generally, asset information is available for all users to query. An exception is probable-cause related information, which is accessible only to users with agency-specific and office level permission attributes. This data can contain sensitive and privacy related information but remains unclassified.

2. Please describe the alternatives to design, collection, and handling of the information that would have a lesser impact on privacy and the rationale for not selecting each such alternative, as well as the final decision.

   Because this effort is a technology refresh, the business rules have long-standing been in effect. The origination of the business rules and logic stems from the participating agencies and their law enforcement missions.

3. What measures are in place to mitigate identified risks?

   The information is secured in compliance with DOJ safeguarding policies such as access controls, infrastructure security, intranet controls, and application security.

4. How will data collected from sources other than Department records and individuals be verified for accuracy?

   All data captured within the CATS application is derived from the participating agency's business rules. The business rules are documented as object specifications and validation rules are injected into the application workflow.

5. How will data be checked for completeness?

   The CATS application enforces workflow processes which prohibit out of sequence entry of information. The information that is captured is validated on all required data fields.

6. Is the data current? How do you know?

   The system is reliant on the field customers entering data into the system. The system does not require real or near-real time processing or data capture. Summary reports are generated and reviewed weekly, quarterly, and annually to ensure

information is accurately captured and represented.

7. Are the data elements described in detail and documented? If yes, what is the name of the document? If not, please do so.

The Data Description Document is captured and maintained in a relational database that can be printed as needed. The database is called the CATS Data Model.

8. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

CATS is a closed system where data is only available to components of the Asset Forfeiture Program. Access to the system is limited to agency approved individuals only. Users for each component may view most of the data in CATS; however, each component is limited by its role within asset forfeiture as to what data they may input into CATS.

Certain information derived from CATS is published on the DOJ website in accordance with USC 28 524(c)(6)(A)(i thru vii). This data has been sanitized of all identifiers (case numbers, names, etc.) and therefore has no impact on individual privacy.

9. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Please explain.

All processes that are being implemented comply with the DOJ security procedures 2640.2D. The application is an intranet system that has incorporated a second firewall to prevent unauthorized internal DOJ traffic.

10. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.

Information can be retrieved using standard boolean search logic. Result sets can be retrieved by several factors, including personal identifiers.

11. What are the potential effects on the due process rights of individuals of: consolidation and linkage of files and systems; derivation of data; accelerated information processing and decision making; use of new technologies?

Individuals continue to have the opportunity to exercise their legal rights, including actions such as claims on seized property and defense against forfeiture. The information is used to track the life cycle of the asset, the monetary effect of the asset, and summary effect on the Asset Forfeiture Fund.

12. How are negative effects to be mitigated?

Risks and plausible mitigation are identified in the CATS Identity Authentication Assurance Level report provided to the DOJ CIO (Attachment)

13. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?

Asset Forfeiture Fund participant users, managers, AFMS report management team members, and database system administrators.

14. How will the determination be made as to who will have access to the data?

From the agency perspective, the CATS User Group representative is the authorized agent for requesting access to the system for their component agency. Support personnel and management access is authorized by the CATS security manager. The criteria for access is maintained by the CATS security manager and access accounts are verified annually.

15. Are criteria, procedures, controls, and responsibilities regarding access documented?

The CATS security manager maintains access control procedures, criteria, roles, responsibilities and validation requirements. The security manager captures this information and maintains it within the scope of the CATS Certification and Accreditation documents.

16. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?

Currently all users who have been granted access can query and view data contained in the system. The premise of the system is to enable users from all participating agencies the ability to view the life cycle of the assets they are responsible for tracking.

17. Do other systems share data or have access to data in this system? If yes, explain.

Yes, DEA is provided a weekly extract of DEA oriented data. This extract provides summary level information as it pertains to DEA activities only. The extract does not include all aspects of the CATS database and does not include party related information.

18. Who will be responsible for protecting the privacy rights of individuals affected by the interface?

The DEA Office of Finance, Financial Systems Section Chief is responsible for the data once they receive the extract, as stated in our Service Level Agreement with the DEA SMARTS application.

19. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?

No, but not confirmed with DEA.

20. Who is responsible for assuring proper use of the data?

Daniel C. Gillette, Chief
Financial Systems Section
Office of Finance
DEA

21. What are the retention periods of data in this system?

The data is not archived. All data is retained for access.

22. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?

N/A

23. Is the system using technologies in ways that the Department has not previously employed? If yes, how does the use of this technology affect individual privacy?

No

24. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain and indicate what controls will be used to prevent unauthorized monitoring.

No.

25. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain and indicate what controls will be used to prevent unauthorized monitoring.

No.