Drug Enforcement Administration

Privacy Impact Assessment
for Depot Tracking System (DTS)

Issued by:
James Robert Bryden
Senior Component Official for Privacy
Drug Enforcement Administration

Approved by: Andrew McFarland
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: July 23, 2025

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

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

The Depot Tracking System (DTS) is a web-based application hosted on the Drug Enforcement Administration (DEA) Firebird Network. DTS was developed to meet the needs of the Information Systems Division's Depot, which tracks DEA's warehouse IT Equipment, incoming equipment, delivery of equipment for all DEA offices to and from and return of equipment to vendors. DTS provides an automation of the following functionalities:

- Asset Management – High Value, classified, and chain of custody
- Inventory Tracking
- Asset Tracking – complete lifecycle history (pre- July 2010 history in notes field)
- Logistics – Receiving and Shipping
- Repair & Maintenance tracking
- Warranty Fulfillment

Though not necessarily required, DTS can and does contain the names of and certain members of the public associated with the DEA's IT hardware lifecycle transactions (e.g., individuals involved with delivery, warranty claims, repair services, returns and vendor points of contract).

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 Depot Tracking System was developed to provide the functionalities required for properly managing receipt of equipment, shipping of equipment to DEA offices, tracking the location of equipment stored in the warehouse, monitoring inventory of equipment at the warehouse, and generating inventory reports. DTS contains information about inventory hardware types, what office has particular items, and the office points-of-contact. The functionalities and purpose of this system are asset management of equipment, shipping and receiving, repair and maintenance tracking, warranty fulfillment and inventory tracking that resides in DEA's information technology warehouse. DTS tracks receipt, location, shipment, and disposal of warehouse equipment through recording the DEA number, Serial Number, and location etc. This includes maintenance support for the pieces of equipment. Therefore, DTS collects equipment description, location within the depot, office destination and DEA points-of-contact. The system may retain certain records submitted in response to specific requests, which could include

Personally Identifiable Information (PII). This information is used exclusively for shipment-related purposes, such as identifying the individual's place of work or designated site location. DTS does not explicitly require the collection of PII of third parties, however, in some instances, DTS also contains the names and contact information of certain members of the public associated with IT equipment delivery, warranty claims, repair services, and returns.

DTS access requires two authentication methods for depot personnel. Authorized users have permission and role-based system access ability. First the users must sign-on in Firebird; then each must log into the DTS using a separate identification and password to access the system. This allows for the user to conduct inventory capabilities. Authorized non-depot users with a need-to-know requirement are granted "Read Only" access. The information is electronic and in hard copy. This information is used by the Information Systems Division (TC) to manage inventory located within the depot. The DTS user must log into the application and use menu driven options to search for data records. There are no personal identifiers used. Data records are searched and retrieved by DTS queries utilizing DEA numbers, Serial Numbers, etc., to identify location(s) of the equipment.

Authorized users/roles consist of Administrator Account and User Account. The DTS System Administrator role is assigned and managed by the Engineering and Integration section and the Commercial off the Shelf Operation and Management (COTS O&M) team. The administrator is responsible for the creation, distribution, and management of user accounts. User accounts are created by the DTS System Administrator with access privileges. Authorized government and DEA contractor personnel may be granted either an Administrator Account or User Account. Contractor personnel have permission and role-based system access and use the computers located at the depot. Contractors create, collect, use, process, store, maintain, and disseminate information using DTS.

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
X	Statute	• 21 U.S.C. § 801, et seq, Controlled Substances Act; • 5 U.S.C. § 301 • 44 U.S.C. § 3101, and • 44 U.S.C. § 3506 (b)(4)
	Executive Order	
	Federal Regulation	
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

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

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C, and D	Federal Government Personnel to include Task Force Officers, Liaison for a government agency and/or military, Contractors,and certain USPER and non-USPERs involved in DEA's IT lifecycle transactions. .
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			
Personal mailing address			
Personal e-mail address			
Personal phone number			
Medical records number			

(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
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices	X	A, B,	Device Serial Number/DEA number of DOJ/Component Employees, Contractors, and Detailees and Other Federal Government Personnel
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			

(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
Proprietary or business information	X	A, B, C and D	Company Name / Office location and phone number(s) of DOJ/Component Employees, Contractors, and Detailees and Other Federal Government Personnel,and certain USPERs and Non-USPERs involved in DEA's IT lifecycle transactions
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	Audit logs derived from logins of DOJ/Component Employees, Contractors, and Detailees.
- **User passwords/codes**	X	A	Audit logs derived from logins of DOJ/Component Employees, Contractors, and Detailees
- **IP address**	X	A	Audit logs derived from logins of DOJ/Component Employees, Contractors, and Detailees

(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
- **Date/time of access**	X	A	Audit logs include date/time the database is accessed by DOJ/Component Employees, Contractors, and Detailees
- **Queries run**			
- **Content of files accessed/reviewed**			
- **Contents of files**			
Other types (please list all other types of identifying information collected 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		Hard copy: mail/fax		Online	
Phone		Email			
Other (specify):					

Government sources:					
Within the Component		Other DOJ Components		Online	
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify):					

Non-government sources:					
Members of the public	X	Public media, Internet	X	Private sector	X
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	The information is shared within the DEA for the purpose of managing technical issues including user access to the DTS portal.
DOJ Components	X			The information is shared within DOJ components for the purpose of validating DOJ component user identities and need for access to DTS portal.
Federal entities				
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
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.

No: The data won't be shared or made public.

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.

General notice is provided to individuals by a system of records notice (SORN) being drafted by DEA specifically for Inventory Systems to be published in the Federal Register in the near future.

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.

DTS itself does not specifically require the collection of PII for most transactions. However, the system may retain certain records submitted in response to specific requests which could include PII. This information is used exclusively mainly for shipment-related purposes, such as identifying the individual's place of work or designed site location. Additional PII may be retained regarding IT lifecycle transactions, where individuals provide or are asked to provide Point of Contact information related to such transactions (e.g., warranty claims, repair work, etc.).

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.

Access to these records is permitted under the Privacy Act and is also outlined in the Portal at DEA.gov/FOIA and in Justice/DOJ–004, *Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records*. Specifically, all requests for access to these records must be in writing and should be addressed to DEA's Freedom of Information and Privacy Act Unit (CCAR). The request should include a general description of the records sought and must include the requester's full name, current address, date of birth, and place of birth. The request must be signed, dated and either notarized or submitted under penalty of perjury (i.e., DOJ-361 form).

DEA's public-facing website contains a Privacy Act webpage which provides members of the public with instructions for filing a request for access to information about themselves to DEA. The website also contains procedures for filing a request for record correction or amendment to DEA.

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):** The initial certification of DTS was granted July 10, 2013, according to JCAM records for an inclusion as a Minor Application into the Firebird accreditation boundary. However, DTS is no longer part of the Firebird accreditation boundary and requires an independent accreditation per the CISO. According to the DTS Revision 5 Transition & Reauthorization Extension Memo which was signed on March 3, 2023**,** DTS has an ATO extension with a new expiration date of September 30, 2025.
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:** DTS was assigned the security category of Low as defined in FIPS-199 based on the aggregation of the information of several different and seemingly innocuous types of information (e.g., first/last name, email, device serial number, phone numbers and business address).
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** DEA monitors the information system on a continuous basis for changes to the information system or its operational environment, the information system security and privacy plan boundaries, or other conditions. DEA conducts security impact analyses of system associated changes, update of the information system's security plan and other relevant information system documentation, such as the system privacy plan, as appropriate, throughout the information system's lifecycle. DEA reports changes in the security or privacy status of the system to appropriate officials on a regular basis. Significant changes to the system require reauthorizations by the DEA Authorizing Official. Significant changes that effect the information system's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of PII are reviewed and assessed by OPCL prior to reauthorization by the Authorization Official. DEA ensures that the appropriate officials are made aware, in a timely manner, of

	information and the information system when it cannot be appropriately protected or secured, and that such is given a high priority for upgrade, replacement, or retirement.
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:** The audit logs are reviewed based off alerting received from Splunk, CrowdStrike, and Vectra, which occur when an alert is activated (may not be daily). The applicable system administrators of DTS also review application audit logs. (Hybrid control: DEA CORE reviews alerts received from Vectra and CrowdStrike that feed into Splunk, which is DEA's log management tool, and contact the system owner.) The system owner is responsible for complying with all guidelines, policies, and laws; the ISSO for DTS is responsible for validating that users comply with said governance while DEA's TCVV (Cybersecurity Operations, Response, and Engineering Unit) enforces actions based upon an infraction (cybersecurity incidents, policy violations). TCVV will perform validation for compliance to governance during risk assessments which are scheduled (ATO renewal or continuous monitoring audit) or remediation efforts against the system during a cybersecurity investigation.
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**. Yes, all contracts have the necessary, proper, and accurate privacy and security-related 0 clauses (i.e., DOJ Clause 02, *Contractor Privacy Requirements*; and DOJ Clause 05, *Security of Information and Information System*) and language required listed in each contract awarded within DEA.
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:** In addition to DOJ's foundational privacy training, DEA conducts incident response training annually and throughout the year covering responses to incidents where PII is compromised. The component has a requirement for all employees to include contract employees to complete the mandated Cyber Security Awareness Training annually.

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?

Physical privacy and security controls:

Physical access control measures are in place to protect DTS data. DTS's server has been deployed in a DEA secured data center. This data center provides physical protection for all hosted systems to include servers, switches, and other devices employed to support the

DEA mission. The data center utilizes numerous safeguards to include guards who monitor the facility. Entry includes two sets of doors, the first utilizes Personal Identity Verification (PIV) Card which is scanned for entry. The second door requires use of the PIV as well as the associated individual PIN. Cameras have been deployed at critical locations to include entry ways. Metal Detectors have been employed for any visitors that do not have a PIV. All physical controls for DTS are inherited from the data center.

In addition to the above-stated protective measures, DEA buildings are guarded and monitored by security personnel, cameras, access badges with picture identification, and other physical security measures.

Technical privacy and security controls:

Through the utilization of specific access controls and data protection techniques deployed, access to this data is controlled by system administrators and authorized personnel that have a need to know based on their job duty and position within the organization. This information is used to create access controls and separation of duty. DTS utilizes the following technical controls to protect the data:

- Database encryption for data at rest
- Disk Encryption
- Transport Layer Security (TLS) for data encryption in transit
- Data Loss Prevention (DLP) software

Administrative privacy and security controls:

Numerous processes/controls have been implemented by DEA to ensure collected data is required, and relevant. These processes include:

- Assigning account managers for information system accounts;
- Establishing conditions for group and role membership;
- Limiting DTS software licenses to a small number of specified DEA employees who need system access to perform their duties.
- Making DTS accessible only through DEA's Firebird information management single sign-on utilizing PIV cards for user identification and access control. Furthermore, DTS requires an additional User ID and password protected entry point into the system for all system users.
- Access to the system itself is protected and monitored by authentication controls, role-based access controls, and system auditing.
- Specifying authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
- Requiring approvals by for requests to create information system accounts;
- Ensuring the system creates, enables, modifies, disables, and removes information system accounts in accordance with DOJ Order 0904: Cybersecurity Program and applicable information system policy and procedures;

- Monitoring the use of information system accounts;
- Notifying account managers:
  - When accounts are no longer required;
  - When users are terminated or transferred; and
  - When individual information system usage or need-to-know changes;
- Authorizing access to the information system based on:
  - A valid access authorization;
  - Intended system usage; and
  - Other attributes as required by the organization or associated missions/business functions;
- Reviewing accounts for compliance with account management requirements.

- DTS users must read and sign DEA's IT Rules of Behavior. Moreover, all users must complete annual DOJ security awareness training.

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.)

Records are retained and disposed of in accordance with the National Archives and Records Administration's (NARA) General Records Schedule 4.2-020 which provides for destruction 6 years after final agency action or 3 years after final adjudication by the courts, whichever is later.

Section 7: Privacy Act

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

_____ No. __x__ Yes.

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

JUSTICE/DOJ-001, Accounting Systems for the Department of Justice, 69 Fed. Reg. 31406 (Jun. 03, 2004) (full text); 71 Fed. Reg. 142 (1-3-2006); 75 Fed. Reg. 13575 (3-22-2010); 82 Fed. Reg. 24147 (amendments) (May 25, 2017).

Please note: DEA is currently in the process of preparing a SORN specifically for Inventory Systems to be published in the Federal Register.

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?

a. Potential Threats Related to Collection of the Information

Privacy Risk: DEA may collect and maintain more personal information than necessary to accomplish DEA's official duties and its mission.

Mitigation: This risk is mitigated. DTS data fields are limited to ensure that the system only collects personal information that are necessary to accomplish its mission (e.g., contact information of vendor; contact information of person who receives equipment).

Privacy Risk: Individuals may be unaware their PII is being collected and cannot meaningfully consent to the collection of their PII.

Mitigation: This risk is mitigated. DTS only collects specific data (e.g., contact information of vendor; contact information of person who receives equipment) that is relevant to its purpose.

Privacy Risk: Individuals may be unaware of DEA processes to access, amend, and dispute their PII when collected for non-criminal investigation purposes.

Mitigation: This risk is mitigated. Access to these records is permitted under the Privacy Act and is also outlined in JUSTICE/DOJ–004, *Freedom of Information, Privacy Act, and Mandatory Declassification Review Records*. Specifically, all requests for access to these records must be in writing and should be addressed to DEA's Freedom of Information and Privacy Act Unit (CCAR). The request should include a general description of the records sought and must include the requester's full name, current address, date of birth, and place of birth. The request must be signed, dated and either notarized or submitted under penalty of perjury (i.e., DOJ-361 form).

DEA's public-facing website contains a PA webpage which provides members of the public with instructions for filing a request for access to information about themselves to DEA. The website also contains procedures for filing a request for record correction or amendment to DEA.

b. Potential Threats Related to Use and Maintenance of the Information

Privacy Risk: DEA may use PII in a manner incompatible/inconsistent with the intended uses of or specified purposes for collection of the information.

Mitigation: This risk is mitigated. DTS only collects the personal information (such as contact information of vendor and contact information of person who receives equipment) which is necessary to accomplish the sole purpose of DTS operations—tracking and distribution of IT equipment. As such, it is compatible and consistent with the specific purposes and intended uses only. All individuals that are associated with

DTS are required to attend yearly role-based privacy training. In this training personnel are instructed on the importance of using information only for its intended purpose.

Privacy Risk: Potential for a system breach by physical intrusion or technical exploitation of the data at rest or in transit.

Mitigation: This risk is mitigated. Security protections that authorize and limit a user's access to information within the system mitigate this risk. For example, consistent with FISMA and NIST security controls, transmissions of DEA non-public data occur only through secure methods, e.g., Virtual Private Networks (VPN), Secure File Transfer Protocol (FTP), Secure Sockets Layer (SSL), or other encryption. The system also has the capacity to monitor the system users and to track their activities in the system. The DTS system administrators are also provided with annual training on the PA, and they ensure that all information DEA maintains on individuals is appropriately safeguarded. See also, protections listed at Section 6.2, above.

Privacy Risk: Data may be retained longer than necessary, which may reduce the relevance and timeliness of the data.

Mitigation: This risk is mitigated. No physical Records in DTS are not kept. They will be disposed. Once they are scanned to the DTS servers. No hard copy is kept.

c. Potential Threats Related to Dissemination of the Information

Privacy Risk: DEA personnel may access the information without a need to know or disclose PII to an inappropriate party or for an improper purpose.

Mitigation: This risk is mitigated. Only a small number of DEA employees and contractors, who are trained and knowledgeable of the IT Rules and Behavior and DOJ security measures, have access to DTS. The DTS system is only accessible through DEA's Firebird information management single sign-on utilizing the Personal Identity Verification (PIV) card for user identification and access control. Furthermore, those permitted to use DTS are also required to have unique and personalized User ID and password protected entry into the system. Information is shared on a need-to-know basis only, and via email, mail, facsimile, or phone in accordance with Department policies. When shared within the Department, other components are required to conform to Department policies to prevent or mitigate threats to privacy through disclosure, such as maintaining the integrity of application. PA-protected information (i.e., records responsive to requests that contain any PII) is sent to requesters via encrypted e-mail.