Drug Enforcement Administration

Privacy Impact Assessment
for the
Financial Information & Reporting System (FIRST)

Issued by:
David J. Mudd
Senior Component Official for Privacy
Drug Enforcement Administration

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

Date approved: September 9, 2020

Points of Contact and Signatures*

*COMPLETE SIGNATURE PAGE IS IN PDF VERSION SUBMITTED BY DEA AND APPROVED BY CPCLO ON SEPTEMBER 9, 2020.

COMPONENT PRIVACY POINT OF CONTACT (POC) Name: Mary C. Donovan Office: Infrastructure & Config Mgmt. SIBC Phone: 202-307-1257 Bldg./Room Number: Lincoln Place, E-3219 Email: Mary.C.Donovan@usdoj.gov	**PIA AUTHOR** (if different from POC) Name: Andrew M. Kenny Office: Office of Finance, Financial Systems Section Phone: 202-307-7215 Bldg./Room Number: Lincoln Place, E-8001 Email: Andrew.M.Kenny@usdoj.gov
SECURITY REVIEW OFFICIAL (Component CIO/OBD Executive Officer/OCIO Staff Director/JMD Staff Director) Name: Andrew M. Kenny Office: Office of Finance, Financial Systems Section Phone: 202-307-7215 Bldg./Room Number: Lincoln Place, E-8001 Email: Andrew.M.Kenny@usdoj.gov Signature: _____ Date signed: _____	**SENIOR COMPONENT OFFICIAL FOR PRIVACY** (if designated; otherwise POC) Name: David J. Mudd Associate Chief Counsel Drug Enforcement Administration Office: Technology Law Section, CCS Phone: 202-598-2707 Bldg./Room Number: Lincoln Place, E-12161 Email: David.J.Mudd@usdoj.gov Signature: _____ Date signed: _____

DOJ PIA APPROVING OFFICIAL

Peter A. Winn
Chief Privacy and Civil Liberties Officer (Acting)
Director, Office of Privacy and Civil Liberties
U.S. Department of Justice
(202) 616-9108

Signature: _____

Date signed: _____

THIS PAGE IS FOR INTERNAL ROUTING PURPOSES AND DOCUMENTATION OF APPROVALS. UPON FINAL APPROVAL, COMPONENTS SHOULD REMOVE THIS PAGE PRIOR TO PUBLICATION OF THE PIA.

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 Office of Finance (FN) directs the Drug Enforcement Administration (DEA)'s financial management, financial systems, and financial training programs. Financial Information & Reporting System Tool (FIRST) is a collection of applications designed and built by FN to support the financial management community and to facilitate financial management business processes. FIRST is a data warehouse that contains feeds from multiple DEA systems. The complete list of each application and its specific mission statement can be found in section 2 of this PIA.

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.

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

The main purposes of FIRST are to help automate financial management processes, to improve DEA operational efficiency, and to provide the finance management community with information required to complete their duties. The system also implements preventative and detective controls in financial management process.

At its core, FIRST is an Oracle data warehouse used for administrative matters with data feeds from several systems. In addition to the data layer, FIRST provides a robust framework of libraries to support application development. Some of the applications developed in FIRST collect additional information from the end user as required by the business case.

FIRST is comprised of several web application modules (see section 2.1(b) for more info); a brief purpose or mission statement for each is listed below.

- **Allowance Manager and Administrative Officer Management**
  The purpose of this module is to allow the Allowance Manager and Administrative Officer to be set for each office. These are two important roles in many of the financial management processes and several FIRST modules assign permissions based on the assignments set in this module.

- **Case Interface**
  The case interface automates the process of loading case reference data into the financial

system. DEA policy requires that the case number be recorded on certain transactions and this interface insures that the most up to date case information is available in the financial system.

- **Check Deposit Log**
  The check deposit log facilitates the transfer of checks received by the field to HQ. The check information, reason for the payment, and accounting information are recorded in the log prior to mailing the check(s) to HQ for deposit.

- **Contract Portfolio**
  The contract portfolio module is an organizational tool to help the contract specialists in the Office of Acquisitions manage their contracts. The financial system has all the information, but in different modules/locations. This tool simply organizes the information in a way to make it easier for the specialist to get what they need. It also has a small data collection piece where the contract Contracting Officer Representative can be identified and their training certification requirements tracked.

- **DARTs Interface**
  The DEA Analysis and Response Tracking System (DARTs) interface automates the process of recording obligations for approved investigative expenses for title III wires and PEN registers in the financial system.

- **e-1190**
  Employees working in foreign posts are entitled to cost of living adjustments (COLA) and in some cases, separation maintenance allowance (SMA) and living quarters allowance (LQA). This system handles the workflow/validations for requesting these allowances and automates the process of creating the bi-weekly payments in the financial system.

- **E2 Account Management**
  This is the request form and account administration tool used by DEA to manage access to the E2 travel system. It handles all the approval workflow, system validations, and helps the field administrators manage their routing pools.

- **Employee Record Review Tool**
  This tool was built in partnership with the Human Resources Division to provide the administrative officers and supervisors with personnel information about their assigned staff. It also provides a mechanism for administrative officers to inform HR staff of "report to duty dates", and other organizational assignment information when an employee transfers, enabling timely processing of personnel actions.

- **FIRST Account Management**
  This is an account request and management tool used by a majority of the FIRST applications. It provides all the workflow and validation for access requests. It also provides a tool for the FIRST security team to assign, change, revoke, and

re-certify access in response to the request form or other triggering events such as user termination or suspension.

- **FIRST Application Support Toolbox**
  This is an internal tool used by Financial Systems to monitor batch processing of United Financial Management System (UFMS) jobs and monitor various FIRST system processes.

- **FIRST Portal**
  This is the main launch site for FIRST applications and provides several key financial management dashboard style reports for the financial management community.

- **FIRST Software Change Request**
  This is the tracking module used by Financial Systems to track FIRST application changes. It tracks PM/developer assignments and handles the workflow required for the FIRST software development life cycle.

- **Fleet Inventory**
  This is the electronic inventory system for all vehicles (cars, planes, boats, etc.). It facilitates the inventory, review, and certification of the data stored in the DEA property system.

- **Hazardous Waste Interface**
  The hazardous waste interface automates the process of paying approved invoices for disposal of hazardous waste.

- **Imprest Management**
  The imprest management module automates the process of establishing, increasing, and decreasing imprest fund accounts. This module handles the request, workflow, system checks, and administration of all imprest fund changes and interfaces with the financial system to record the transactions.

- **Informant Interface**
  The informant interface automates the process of creating/updating informant vendor codes in the financial system. No PII data is loaded, only the numeric informant identifier from the informant tracking system.

- **Obligation Management**
  The obligation management module was built to address an audit issue with undelivered orders. The tool helps the financial management staff ensure that undelivered orders are properly reconciled and documented. It provides a reconciliation, review, and certification process for each open obligation on a quarterly basis.

- **Occupancy Reconciliation Inventory System**
  This tool is used to track DEA lease/building information and is used by

facilities management to help ensure that the space requirements for each office are met and within the guidelines put in place by the General Services Administration (GSA). It tracks logical and physical assignment for all DEA employees and contractors that use DEA space. It requires quarterly certification by each office to ensure the data is accurate.

- **Payment Notification**
  The payment notification system uses the payment schedule information from UFMS to send custom messages to DEA employees and cashiers, letting them know that their payments have been processed and they should expect payment (typically via ETF) within a few days. Imprest Cashiers rely on these emails as validation that their imprest replenishment packages were processed.

- **Payment Card Authorization Official (PCAO) Certification**
  This module facilitates the process of reviewing and certifying all purchase card charges by the purchase card-approving official. It serves as a financial management control providing better oversite of the purchase card program.

- **Property Inventory Management**
  This is the electronic inventory system for all non-vehicle property. It helps ensure that property is accounted for and interfaces with the property system to ensure that it is properly recorded.

- **State Department Interface**
  The Department of State handles all of the financial transactions with foreign entities on behalf of the DEA. This module helps automate the process of recording these transactions in the DEA financial system.

- **Table of Organization Management System**
  This module is used to manage the DEA's organizational structure and all the authorized positions along with the associated accounting codes.

- **Transit Subsidy**
  This module facilitates the tracking and reconciliation of employees enrolled in the transit subsidy program.

- **UFMS Account Management**
  This module provides the request form, approval workflow, and administration for accounts in the financial system. Access to the financial system is tightly controlled and audited. This tool helps ensure that proper segregation of duties checks and other system checks are run before the account is added. It also helps with reconciliations to ensure that the permissions assigned by the security administrator match the approved request.

- **UFMS Report**
  This module provides reports that are needed by the financial management community. It is a read-only application and the reports are primarily based on

information from the financial system.

- **Fleet Inventory and Reconciliation**
  This module automates the process of reconciling and processing fleet card charges in the financial system. It also facilitates the tracking/certification of home to work authorization from primary assigned vehicles.

- **Vendor Management**
  This module provides the request form and approval workflow for all vendor records in the financial system. Employee vendor records are added automatically via the National Finance Center (NFC) process, but all other DEA vendors requests are managed by this module.

(b) the way the system operates to achieve the purpose(s):

FIRST is a collection of modules coupled with an Oracle relational database management system (RDMS). The Oracle database stores information pulled from the financial system (UFMS), the personnel system (NFC), the time & attendance system (webTA), the network active directory, and data collected from users via the individual modules.

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

FIRST maintains, uses, and disseminates the following type of information:

- NFC records – Employee personnel records, taskforce officer information, and contractor information.
- Financial system records – Data from the DEA financial system (payroll, transaction history, account numbers, vendors, credit cards statements, property information, etc.). It may include Social Security Number (SSN) bank account, information, address, and other PII.
- Time and Attendance records –Timecard, leave, and profile information from the DEA time and attendance system.
- Dependent privacy data – Most of the privacy data contained within FIRST is obtained through other systems. The only privacy data originated within FIRST are the names, birthdate and addresses of dependents for DEA employees that are assigned to unaccompanied overseas duty.

(d) who has access to information in the system:

FIRST modules are only accessible from the DEA's intranet Firebird and it uses windows authentication to identify users. FIRST relies on a custom-built role based security model to obtain application permissions based on the user's network account. Access to FIRST applications is granted by the FIRST security administrator in response to an electronic access request form. Access to certain applications can also be inherited from permissions granted a user in the financial system UFMS. Each module is role based and the user is given specific permissions according to the assigned role. Access is tightly controlled and audited by the FIRST security team. All users with access have an approved form (either FIRST or UFMS) and are required to re-certify annually. Additional checks and controls are in place to ensure the

correct user roles/permissions are assigned for each application.

(e) how information in the system is retrieved by the user:

Information for individuals can be retrieved by name or SSN.

(f) how information is transmitted to and from the system:

The data is primarily transmitted at the application level through secure sockets layer (SSL) via the browser, but some "power users" use secure file transfer and database communication protocols as well.

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

FIRST connects with other systems. It has data feeds from the DEA's financial system (UFMS), the personnel system (NFC), the T&A system (WebTA), and Concorde.

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

FIRST is considered a major application, but is a child of Firebird (DEA network) and inherits many of its controls from this parent.

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	31 U.S.C. 3512; 44 U.S.C. 3101.
	Executive Order	
X	Federal Regulation	64 Fed. Reg. 29069.
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in

Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	*X*	A, B, C	Vendor info (invitational traveler).
Date of birth or age	*X*	A, C	NFC records and/or family of employee in foreign post - required for allowance form approval & calculations.
Place of birth			
Gender	*X*	A	NFC records
Race, ethnicity or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	*X*	A, C	NFC records and/or vendor info, spouse for foreign post assignment.
Tax Identification Number (TIN)	*X*	A, C	NFC records, Vendor Info
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	*X*	A, C	NFC records, Vendor Info
Personal e-mail address	*X*	A, C	NFC records, Vendor Info
Personal phone number	*X*	A, C	NFC records, Vendor Info
Medical records number			
Medical notes or other medical or health information			
Financial account information	*X*	A, C	Vendor Info
Applicant information			
Education records			
Military status or other information	X	A	NFC record
Employment status, history, or similar information	X	A	NFC record

(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
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices	X	A	Property record in UFMS
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	X	C	UFMS
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**			
- **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	Network, UFMS, FIRST
- **User passwords/codes**			
- **IP address**	*X*	A	

(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	
- **Queries run**	*X*	A	
- **Content of files accessed/reviewed**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):			

*SSNs are required on various financial forms (i.e. Payee Request IRS W-9, Foreign Allowance Request electronic SF-1190, etc.) processed in FIRST and passed along to UFMS for payment and IRS reporting purposes. FIRST is a financial data warehouse that stores financial records including UFMS, NFC Payroll/Personnel, and other financial data, which includes SSNs. FIRST utilizes the SSN to link individual payments and other information together as needed from other systems.

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

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

Government sources					
Within the Component	✓	Other DOJ components	✓	Other federal entities	✓
State, local, tribal		Foreign			
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	Information will be shared to support the Office of Finance in financial management activities.
DOJ Components				
Federal entities	X			Information will be shared with the National Finance Center and UFMS).
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
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.***

N/A.

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 by JUSTICE/DOJ-001, "Accounting Systems for the Department of Justice," 69 Fed. Reg. 31406 June 3, 2004 and OPM/GOVT-001, "General Personnel Records," 77 FR 73694 December 11, 2012; 80 FR 74815 November 30, 2015. In addition to the general notice, a Privacy Act (e)(3) notice is provided when collecting information directly from the individual.

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.

Individuals do not have the opportunity to decline to provide information. There is no practical means to allow the individual to decline having the information entered into FIRST because data processed by FIRST is gathered from other systems such as the UFMS and NFC. Individuals may be able to voluntarily provide information to those systems. Individuals will receive a Privacy Act (e)(3) notice at the point of collection, which provides information on the effects, if any, of not providing all or any part of the requested information.

Individuals also do not have the opportunity to consent to particular uses of the information. Privacy data contained in FIRST is used in support of DEA financial management activities. Most of the privacy data contained in FIRST concerns compensation, benefits, reimbursements, and payment for services. It is obtained through other systems (i.e. UFMS) and organizations (i.e. National Finance Center). Subsequent entry of additional privacy data is ordinarily entered by a third party and/or expands on an existing record of the individual in the system. Regarding the case of third party entry, there is no method to provide an opportunity for consent or use of the information. Some systems that FIRST draws data from, such as the UFMS, may provide an individual the opportunity to consent at the point of collection.

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.

FIRST obtains data through other systems, which themselves may have procedures to allow individuals to gain access and modify information. In the limited cases where an individual expands their own record, they do so voluntarily to ensure appropriate compensation, benefits, reimbursements or payments associated with their work with DEA. DOJ maintains procedures to process requests under the Privacy Act at 28 C.F.R. Part 16, Subpart D, Protection of Privacy and Access to Individual Records Under the Privacy Act of 1974.

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).

✓	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: 09/27/2017 If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date:
✓	A security risk assessment has been conducted.

✓	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: All relevant security controls are implemented.	
✓	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: A subset of security controls are evaluated annually per DOJ guidance.	
✓	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: The core controls identified by DOJ are reviewed annually.	
✓	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.	
✓	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.	
✓	The following training is required for authorized users to access or receive information in the system:	
	✓	General information security training
		Training specific to the system for authorized users within the Department.
		Training specific to the system for authorized users outside of the component.
		Other (specify):

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?

Access to SSN and other PII data is tightly controlled through system roles. Only users who need the information for a defined purpose are granted access.

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.)

Financial related records are replicated from the Unified Financial Management System (UFMS). Retention periods are dictated by UFMS and are greater than seven years. FIRST does not maintain these records or associated privacy data for periods longer than those established by UFMS.

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 FR 31406 June 3, 2004.

OPM/GOVT-001, "General Personnel Records," 77 FR 73694 December 11, 2012; 80 FR 74815 November 30, 2015.

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 Threats Related to Information Collection

Collecting and maintaining more personal information than necessary to accomplish the DEA's official duties is always a potential threat to privacy. FIRST collects and maintains only information about an individual that is relevant and necessary to accomplish DEA's financial responsibilities. The data obtained is solely focused on those necessary attributes used to support financial transactions of DEA personal and support staff, such as name, address, and SSN. PII not relevant to individual(s) pay or cost reimbursements are not collected or maintained by FIRST. In this regard, data collection is minimized to that which is essential for transactions and operations to be conducted in accordance with financial guidelines and requirements.

b. Potential Threats Related to Use of the Information

Potential threats to privacy as a result of the DEA's use of the information in the FIRST system include the risks of unauthorized access to the information, threats to the integrity of the information resulting from unauthorized access, improper disposal of information, and/or unauthorized disclosure of the information.

An accidental exposure of privacy information is the greatest potential threat. DEA mitigates risks by granting access internal to DEA users after an employee and/or contractor has obtained the required security clearance and the proper access request form and/or identity validation has occurred. The risk associated with this threat is low given that few users have access to the privacy information maintained within FIRST. Furthermore, an exposure would involve multiple careless steps such as printing the data, mishandling the hardcopy or copying the digital data into a file and then sharing it with other individuals or entities not authorized to access the privacy data. Mandatory annual security awareness training for DEA personnel and contractors addresses the proper and safe handling of privacy data. Lastly, FIRST users are required on an annual basis to re-visit and comply with the DOJ Rules of Behavior which details the need to safeguard, protect and not misuse privacy information collected and maintained with FIRST.

c. Potential Threats Related to Dissemination

Security measures in place to safeguard sharing of information include: IT monitoring tools; firewalls; intruder detection and data loss prevention mechanisms; and system audit logs. In addition, DEA has established minimum auditable events based on DOJ IT security requirements. The information system produces audit records, at a minimum that establish what type of event occurred, when and where it occurred, the source of the event, outcome of the event, and the identity of any user or subject associated with the event.

Given that FIRST is not exposed and does not have access to the Internet, the risk of compromise to privacy data within the system by malicious intent or malware is very low. FIRST does not transmit privacy data to other internal systems, and other DEA systems cannot access privacy data housed within it, thereby eliminating the threat of inappropriate unauthorized access. The primary potential threat to privacy arises from an insider threat. Users with access to the privacy data could accidentally or maliciously disclose the information accessed. 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.