Federal Bureau of Investigation

Privacy Impact Assessment
for the
Financial Reporting Application (FRA)

Issued by:
Erin M. Prest, Privacy and Civil Liberties Officer

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

Date approved: July 5, 2023

EXECUTIVE SUMMARY

The Federal Bureau of Investigation's (FBI) Financial Reporting Application (FRA) is a financial and procurement report management system owned by the FBI Finance and Facilities Division (FFD). The FRA is a financial data analysis application that is a comprehensive web-based enterprise reporting tool used by the FFD and FBI staff with financial and/or procurement responsibilities to create reports using data from multiple systems, most notably the FBI's United Financial Management System - Secret Domain (UFMS-S), which contains classified information. The data used in FRA reflects the combined data from these systems to provide a complete financial analysis and reporting application.

The FRA is an application that organizes the data into standard or customized reports. The FRA provides a user the ability to temporarily view the data report and/or to download the data reports to a specific FRA format (e.g., Microsoft Excel, HTML 5 basic) in a user-chosen location outside of the FRA . The FRA was implemented to improve the reporting functions of the financial management and procurement operations across the FBI. An FRA Privacy Impact Assessment (PIA) is being conducted because the FRA uses and disseminates financial management and procurement data including personally identifiable information (PII) such as names, Social Security Numbers (SSNs), and financial account information.

FRA is currently housed in the FBI's Secret Cloud on Premises (S-COP), but is planned to migrate to an Amazon Web Services (AWS) Secret Commercial Cloud Services (SC2S) environment, with a projected go live date of November 2024.

Section 1: Description of the Information System

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

FRA is an FBI Secret Enclave (FBISE) application that provides users the ability to view financial data in user-friendly reports. The reports are viewed through web browser software on the FBI Intranet. UFMS-S is the primary origin of the data, but FRA also uses data from other systems, as well as data directly input by FRA users.

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

FRA allows users to view the data stored in UFMS-S and other systems via web browser and to create reports based on this data. In addition, FRA provides a portal with which specific users can input data directly for the purpose of generating Travel W-2 forms.

FRA is an application built using WebFOCUS, a commercial-off-the-shelf product that allows users to view and process data using Internet technology with a graphical user interface to navigate various menus by typing commands. The FRA creates an interface to data and the functions are easier to use than those provided by UFMS-S and other FBI systems that provide data to FRA.

FRA enables end users to run reports and obtain real time[1] financial data. FRA can produce both standard and custom financial reports that can be exported into multiple file formats. FRA reports can be scheduled by the user to run at desired intervals (e.g., hourly, daily, weekly, etc.) with saved search criteria. FRA users are able to view the FRA reports or have them sent to another FRA format and location of their choice, within the limited options available, as discussed below. The FRA transfer of data from the source systems to other locations, such as Excel spreadsheets on an individual drive, is direct, with no permanent holding area in the FRA. The FRA has a temporary holding area that is used only while processing the data transfers. Once data is downloaded from the FRA to another location, the FRA user then has control over where the data is stored and how long the data is retained. To support analytic and historical reporting, the user can save the information to any network drive accessible through FBINet.

The FRA also gives users the ability to benchmark their data against other units, sections, divisions, branches, projects, or programs. For example, a Field Office financial analyst is able to view (in a temporary FRA hold file) and/or download (into a graphic or spreadsheet report) summary data for all purchase card transactions for that Field Office and to compare that data with the same type of data for another Field Office. The summary data used to compare and benchmark between organizations may include PII in a limited number of circumstances. Standard FRA reports containing PII will include PII in the related benchmarking reports, such as the Travel W-2 forms and FRA's Vendor Reports (as discussed in Sections 1(c) and (d), below).

Once the report format is selected, the user then selects the desired data source. The user's role-based access authorizations and restrictions also determine the sources available to that specific user. Users who have been granted approval to view specific data in UFMS-S are allowed to use and view that same data in FRA reports.

The data sources can be aggregated information across offices or specific information about an individual. For example, a government purchase card specialist would use a report format that displays the purchase-card activity of an FBI employee and then choose the individual's information to display in that report. Also, that same government purchase card specialist would also use a report format that displays the purchase-card activities at the FBI Unit level and then choose the FBI Unit's information to display in the report.

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

FRA uses and disseminates financial transaction, accounting, budget, procurement, vendor, asset, and personnel data chiefly collected and maintained by other systems. This data is based on different types of transactions including, but not limited to, payroll, invoices, credit/debit card transactions, and journal entries. The journal entries are the same as those typical to other financial systems, and include information such as the date/time, amount of the transaction, the type of transaction [i.e., credit/debit], and the account used in transaction.

[1] Real time is defined as less than 30 minutes old.

Because some of this data pertains to classified FBI programs, the system is generally classified at the Secret level, though it can issue Unclassified reports that only contain Unclassified information.

Some of the data used by FRA involves personnel and financial data that is related to individuals. This data, described in Section 2.1, only concerns FBI personnel (including federal government employees, contractors, and Task Force Officers). Additionally, some UFMS-S data reported in FRA includes FBI information on individual debtors and creditors of the FBI, including vendors and individual recipients of FBI benefits, grants, and funds.[2] These transactions are captured within the financial system of record and are made available through the reporting system.

As a requirement of the Federal Information Security Modernization Act of 2014 (FISMA), the FRA System Administrator runs an access audit log report that contains the Network ID and name of every user that has signed onto the FRA. The time of the access or access attempt is recorded on the report as well.

The FRA limits the amount of UFMS-S PII used to produce reports. FRA has the potential to collect any data in UFMS-S; however, not all of this data is currently collected by FRA (e.g., telephone number and e-mail address are not currently used by FRA). Moreover, if an FRA report includes sensitive data (for example, vendor names from a restricted investigation), the sensitive data can be excluded from the FRA report by the user.

In addition, FRA collects, uses, and disseminates PII and other data manually entered by the Finance and Facilities Division (FFD)/Accounting Section/General Ledger Unit (GLU) for the sole purpose of generating Travel W-2 forms. As FFD's Travel Request Initiation and Payment (TRIP) system cannot generate Travel W-2 forms to cover the reimbursements that FBI employees receive for official travel, GLU uses FRA to pull information from UFMS-S and compiles it with TRIP information and other information manually entered into FRA specifically for the purpose of generating these forms.[3]

(d) who has access to information in the system

To access the information about individuals, as described in Section 1(c), FRA users must have special access privileges with a documented justification for "need-to-know" in the Enterprise Process Automation System (EPAS) workflow for user groups and developer groups.

EPAS affords FRA users the proper level of access by logging in through a single sign-on process via an FBI Active Directory group. The web software used by FRA is configured to rely on the approved Active Directory group in order to display queried results to the user.

[2] UFMS-S information reported in FRA includes "vendor" contact and billing information, such as Taxpayer Identification Numbers (TIN). In addition to information on business organizations and their representatives, UFMS-S vendor information can also include sole proprietor businesses and other individuals (e.g., expert witnesses, court reporters). For those individuals who do not have a business TIN, the individual's SSN is captured in UFMS-S. In addition, some individuals use their SSN as their business TIN.

[3] For records retention purposes, the Travel W-2 data is considered to be wholly derivative of other FBI systems supplying data to FRA, including information manually entered into FRA. Accordingly, records retention schedules for the originating systems are applicable.

Users requesting any type of FRA access must submit a System Access Request (SAR) through the EPAS system with the appropriate justification for each type of data included in the request. Each SAR is reviewed and must be approved by 1) the applicant's supervisor (Unit Chief/or designee, 2)the FRA System or the Technical Lead.

FBI personnel with access to UFMS-S are granted access to the FRA, including FFD personnel and FBI personnel with financial and/or procurement responsibilities in other Divisions by submitting a SAR through EPAS Other FBI personnel with access to the FRA include FRA developers, system administrators, and security administrators. When necessary, FRA system administrators rely on the vendor for WebFOCUS to provide technical software support. The vendor has a team with appropriate clearances to access the FBI's enclave that hosts FRA.

The FRA uses the existing access control measures within the FBISE's corporate domain infrastructure to provide authenticated user access to the FRA system. Users who view data in FRA must submit a SAR request, with appropriate leadership approvals and justifications, independent of whether or not they have been granted access to view the data in their source systems. For example, approximately ten staff members in the Accounting Section of FFD have been given access to the substantial amounts of PII (including name, SSN, home address, wages, and taxes paid) in order to produce the Travel W-2 form, which is provided to FBI employees in January every year. Separately, staff members in the Accounting Section and Procurement Sections of FFD have access to this PII in FRA, including vendor name and SSN/Taxpayer Identification Number (TIN) data in Vendor Reports, in order to provide analysis of vendor activities.

Also, users with particular financial or procurement responsibilities have the ability to produce FRA reports with limited PII. For example, users with procurement responsibilities have the ability to view and download purchase card transaction data that include vendor names, which might consist of the names of individuals. In addition, travel specialists have the ability to view or download travel data that include travelers' names, travel locations, and purpose of travel. Only the names of vendors and travelers are available to such FRA users; no other PII, such as financial account or credit card numbers, are available to such FRA users. Vendor names and traveler names are in many of the FRA reports. All travel related reports have the name of the traveler. All expenditure reports have the name of the vendor that was paid.

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

General access to FRA is available to the user from an FBISE client workstation via a web browser interface from standard FBISE workstations by typing "FRA" in the browser address line. Additional, special access is available through report building software on licensed FBISE workstations. These licensed workstations are only provided to trained personnel and not to general users.

The extract and load process for data used by FRA is automated via programming scripts created by the FRA Team/FRA Team Developers (privileged users) using WebFOCUS.

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

FRA accesses real-time data from other systems using a web browser interface in FBINET. FRA's underlying software, WebFOCUS, is a web tool that allows users to view and process data using Internet technology with a graphical user interface (GUI). WebFOCUS is configured to allow access to host applications using a web browser and provides a user-friendly GUI for viewing and creating reports directly from host databases. The extract and load process for data used by FRA is automated via programming scripts created by the FRA Team/FRA Team Developers (privileged users) using commercial off-the-shelf software.

FRA is currently hosted on the Secret Cloud on Premises (S-COP, formerly known as the Distributed Application Virtual Environment-FBI Secret Enclave, or DAVE-FBISE).[4] All data transmitted to and from FRA are encrypted in transit using Advanced Encryption Standard (AES) 128 bit encryption.

Data is accessed through reporting or data servers (i.e., WebFOCUS Reporting Server [WFRS], WebFOCUS Data Migrator Server [WFDM]) which reside on a Windows Server and on an Enterprise Server. The primary server is in the Windows environment housed in S-COP. The secondary server is housed on the Enterprise Server.

Unlike other data accessible through FRA, GLU employees input Travel W-2 data directly into FRA via the web browser interface for viewing/reporting in FRA. Travel W-2 data ultimately resides in the Data Analytics Services - Financial Information Repository Environment (DAS-FIRE).

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

FRA currently interfaces with the following systems/subsystems to access their data (described in Section 1(c)) for reporting the following types of data:

- UFMS-S (multiple subsystems) - personnel, vendor, asset, and financial data;
- HR Source – personnel and payroll data;
- DAS-FIRE - personnel, vendor, asset, and financial data;
- EPAS/ TRIP - travel data;
- Asset Management System (AMS) - asset data;
- Phoenix- Contracts and contractor data;
- Facilities Integration Tool (FIT) - building information (e.g., addresses, city, state, square footage, contract names).

All of these data sources are independent systems with their own storage, user input, and interfaces, and are covered by their own privacy documentation.

[4] FFD currently plans to migrate FRA from S-COP to the AWS SC2S commercial cloud environment. This move will not change any of the functionality described in this PIA, nor will it change the access to PII – only the hosting environment will change. Currently, the FRA Cloud (FRA-C) project is under development on AWS GovCloud, with a plan to test in the AWS SC2S pre-production environment by June 2023, and a production date of November 2024.

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

FRA is a controlled, restricted application that is not open to all users within the FBI, but can be used to prepare regularly scheduled financial reports, as well as ad hoc reports, by providing access to UFMS-S data and other data available within the FRA, as noted above.

Section 2: Information in the System[5]

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

(Check all that apply.)

Identifying numbers					
Social Security	x	Alien Registration		Financial account	x
Taxpayer ID	x	Driver's license		Financial transaction	x
Employee ID	x	Passport		Patient ID	
File/case ID	x	Credit card	x		
Other identifying numbers (specify): TIN; File/case ID only includes number, without any other associated information..					

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

Work-related data					
Occupation		Telephone number	x	Salary	x
Job title		Email address	x	Work history	
Work address	x	Business associates			
Other work-related data (specify): Vendor data also include business name, company ID number, and business financial account information.					

Distinguishing features/Biometrics					
Fingerprints		Photos		DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Voice recording/signatures		Vascular scan		Dental profile	

[5] FRA's overall certification and accreditation is Moderate in Confidentiality, Moderate in Integrity, and Moderate in Availability.

Distinguishing features/Biometrics	
Other distinguishing features/biometrics (specify): N/A	

System admin/audit data					
User ID	x	Date/time of access	x	ID files accessed	x
IP address	x	Queries run	x	Contents of files	
Other system/audit data (specify): N/A					

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

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

Government sources					
Within the Component	x	Other DOJ components		Other federal entities	
State, local, tribal		Foreign			
Other (specify): N/A					

Non-government sources					
Members of the public		Public media, internet		Private sector	X
Commercial data brokers					
Other (specify): Non-government sources of PII in FRA are limited to individual creditors and debtors, as described in Section 1(c).					

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

The FRA is a web-accessible reporting tool accessed via the FBISE that is used to execute and obtain financial reports with information collected from UFMS-S and other systems. It provides the ability to view financial data graphically (e.g., pie charts, bar charts, tables). The data used in FRA reflect data from UFMS-S and other systems, which can contain classified information.

The FRA gives users the ability to select financial and procurement data imported from other systems, to view such data in a certain type of report design, and then to download that report into other FRA-selected formats and locations selected by the user. The FRA reduces the risks of unauthorized access to PII by providing standard report designs to most users. The FRA also reduces the risks by restricting access to a limited number of users (after approval by FFD), to create their own report designs.

In addition, the FRA limits the amount of PII that users obtain from other systems to produce reports. The FRA uses the existing access control measures within the FBISE's corporate domain infrastructure to require authenticated user access to the FRA system. Users who have been granted approval to view data from systems that provide data to FRA are allowed to view only that same data in FRA reports. For example, only the approximately ten staff members in the Accounting Section of FFD have been given access to the PII, including name, SSN, home address, wages, and taxes paid, needed to produce Travel W-2 forms. In addition, approximately ten additional staff members in the Accounting Section of FFD have been given access to the PII, including vendor name and SSN/TIN, involved in Vendor Reports, which provide analyses of vendor activities.

Also, only users with particular financial or procurement responsibilities have the ability to produce FRA reports with PII, and that PII is limited by their responsibilities (need to know). For example, only users with procurement responsibilities have the ability to view and download purchase card transaction data that include vendor names, which might consist of the names of individuals. In addition, only travel specialists have the ability to view or download travel data that include travelers' names, travel locations, and purpose of travel. Only the names of vendors and travelers are available to such FRA users; no other PII, such as financial account or credit card numbers, are available to such FRA users.

Moreover, when an FRA report includes sensitive data (for example, vendor names from a restricted investigation), the sensitive data can be excluded from the FRA report. The user is not able to view the information in FRA; the user will be able to view such information in UFMS-S, but only if the user already has access to such data in UFMS-S. If a user group wanted access to additional PII for financial or procurement reports, the group must submit a SAR for expanded access to FRA data. If the request is approved, the FRA Systems Administrator would create appropriate permissions and access controls for the group. The FRA System Administrator works with the EPAS and Active Directory teams to create new security groups for the FRA, when appropriate.

Section 3: Purpose and Use of the System

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

Purpose			
	For criminal law enforcement activities		For civil enforcement activities
	For intelligence activities	x	For administrative matters

	To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.	x	For administering human resources programs
	For litigation		
	Other (specify):		

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

Data, to include PII, is collected to support the overall mission of the UFMS-S. The FBI uses biographical information to support operations and accommodate business interaction. FRA uses UFMS-S biographic and banking information to audit, review, compare, and report transactions including compensation, identification, procurement, reporting, and validation. The FRA uses SSNs to report credit card and tax transactions, as well as to audit, review, compare, and report vendor record grouping, ordering, and tracking.

FRA is a web accessible reporting tool that is used to execute and obtain financial reports. It provides the ability to view financial data graphically (e.g., pie charts, bar charts, tables). The reports are built so that users will have the ability to simultaneously point to data located in various data sources, which eliminates the need for users to spend unnecessary time pulling data from various data sources and spreadsheets in order to combine and arrange the information.

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

Authority		Citation/Reference
x	Statute	31 U.S.C. § 3512; 44 U.S.C. § 3101
	Executive Order	
	Federal Regulation	
	Memorandum of Understanding/agreement	
	Other (summarize and provide copy of relevant portion)	

3.4 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

Retention information for FRA falls under two disposition authorities based on what type of record is being reviewed. First, information falling under the retention standards for budget matters can be destroyed six years after the close of the relevant fiscal year, but longer retention is authorized if required for business use. Second, information falling under the retention standards for workload and personnel management accounting can be destroyed three years after the close of the relevant fiscal year, but longer retention is authorized if required for business use.

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.) [In addition to providing a narrative answer, please consult the ISSO/ISSM for the system's NIST 800-122 PII Confidentiality Risk Level, and check the applicable Confidentiality Safeguard Security Controls.]

PII Confidentiality Risk Level: □ **Low** ☑ **Moderate** □ **High**

- Is the system protected as classified; or
- Does the system involve intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system; or
- Is the system critical to the direct fulfillment of military or intelligence missions (excluding routine business or administrative applications, e.g., finance, logistics, personnel management)?

☑ **Yes** □ **No**

If Yes, the system meets the NIST 800-59 definition of a National Security System.

Access controls

X	Access Enforcement: the system employs role-based access controls and enforcement mechanisms. There is no ability to access the underlying database without the front-end interface.
	Separation of Duties: users of de-identified PII data are not also in roles that permit them to access the information needed to re-identify the records. Data in FRA aren't de-identified; PII is restricted based on role. ''PII Users" have access to PII for only those duties that require it.
X	Least Privilege: user roles enforce the most restrictive set of rights/roles for each user group.
X	Remote Access: remote access is prohibited or limited to encrypted communication channels.

	User-Based Collaboration and Information Sharing: automated mechanisms are in place for matching PII access authorizations to access restrictions, such as contractual/MOU/MOA restrictions. FRA does not involve user-based collaboration or information sharing.
	Access Control for Mobile Devices: access to PII is prohibited on mobile devices or limited so that data can only be accessed on mobile devices that are properly secured and regularly scanned for malware. FRA has not authorized access through mobile devices.

Audit controls

X	Auditable Events: access to PII is audited for unauthorized access
X	Audit Review, Analysis, and Reporting: Audit records are regularly reviewed on a weekly basis by the Information System Security Officer (ISSO) for any inappropriate or unusual activity, including activity that affects PII. Any such activity is investigated. Any findings from the investigation are reported to the system lead/designee, who will undertake any necessary responsive action(s) and appropriate mitigation.

Identification and Authentication controls

X	Identification and Authentication: users are uniquely identified and authenticated before accessing PII; remote access requires 2-factor authentication and 30-minute “time-out” functionality.

Media controls

	Media Access: access to system media containing PII (CDs, USB flash drives, backup tapes) is restricted.
	Media Marking: media containing PII is labeled with distribution/handling caveats.
	Media Storage: media containing PII is securely stored.
	Media Transport: media is encrypted and stored in a locked container during transport.
	Media Sanitation: media is sanitized prior to re-use
Once data is downloaded from the FRA to another location, the FRA user then is responsible for where the data is stored and how long the data is retained.	

Data Confidentiality controls

X	Transmission Confidentiality: information is encrypted prior to transmission or encrypted transmission is used. The communication channels used by the WebFocus client and the WFRS use AES 128.
	Protection of Information at Rest: information stored on a secondary storage device (e.g., hard drive or backup tape is encrypted.

Information System Monitoring

X	Information System Monitoring: network boundaries are automatically monitored for unusual or suspicious transfers or events

FRA contains classified information and operates at the System Moderate Mode of Operation within the FBISE. The FRA does not transmit data into or out of the FBISE.

FRA is primarily used to process, rather than store, data; most of the data it processes is not stored within FRA. The FRA has a temporary holding area, used only while processing the data transfers. However, Travel W-2 data that is input directly into FRA is currently stored in a FOCUS format database, but in the future, they will be moved to DAS-FIRE, one of the interconnecting systems for FRA.

FRA reflects UFMS-S data, which contains classified information. The unauthorized release of this information, or unauthorized user access, could seriously damage criminal or terrorist investigations, jeopardize legal outcomes, or put the lives of FBI personnel at risk. The need for maintaining the confidentiality is Moderate. Inaccurate, corrupted, or missing data could seriously damage the FBI's ability to function, or be detrimental to the overall mission. As a result, the protection level for integrity is rated as Moderate. Outages of days or weeks will not endanger the FBI operational mission. The need for maintaining availability of FRA is rated as Medium.

FRA users are able to view the FRA reports or have them sent to another FRA format and location of their choice, within the limited options available, as discussed below. The FRA transfer of data from UFMS-S to other locations, such as Excel spreadsheets on an individual drive, is direct, with no permanent holding area in the FRA. The FRA has a temporary holding area, used only while processing the data transfers. Once UFMS-S data is downloaded from the FRA to another location, the FRA user then has control over where the data is stored and how long the data is retained.

In order to help reduce the risk of inappropriate access to or use of the information, FRA users must have approved access for the FRA submitted through EPAS before they can view any data. Authentication of all users is provided through an Active Directory group which is assigned through EPAS. Once the user has had positive authentication and positive authorization, they will be allowed to view the data presented in the FRA. All users have Basic User access, but can gain additional access to data and reporting features by requesting one or more additional user roles (see list below). Users requesting additional reporting features must submit a request through the EPAS system with the appropriate justification and approvals in order to receive less restrictive access to the application which provides role-based access that limits access to PII to only those users authorized to view it. User roles for FRA include the following seven privileges:

1. **Administrator** has all privileges of the WebFOCUS software and the reporting application. These select users perform install, configuration, and management of the system as well as for the reporting application. These users will have access to the PII information in order to build and troubleshoot reports containing PII.
2. **Developers** create WebFOCUS objects (e.g. reports, reporting objects/templates, HTML frontends). These users have select configuration and management access to the application. These users have access to the PII information in order to build and troubleshoot reports containing PII.
3. **Program Manager** has the ability to use Standard Reporting, Monitoring Portal, Ad Hoc Reporting, Scheduling and Distribution.

4. **Advanced User** has the ability to use Standard Reporting, Ad Hoc Reporting, and Scheduling and Distribution.
5. **Basic User** has the ability to use Standard Reporting and Scheduling and Distribution.
6. **Executive User** has the ability to use Run only Executive Portal reports.
7. **PII User** will have this role added to their Active Directory Group.

The FBISE Active Directory security will ensure that unique user ID and passwords are entered successfully before access to the data. Passwords are authenticated using software tools within the FBISE domain. All users are required to have signed the FBI Rules of Behavior, which contain procedures for passwords, compromise, and required training.

Annually, FRA participates in Access Removal Certification (ARC), referred to as the annual recertification process, via EPAS. During this process, each user with access to FRA will receive a notification through EPAS to either remove or keep their access to FRA. The request is then routed to the user's supervisor, who approves or disapproves their selection based on the user's business need and justification. Any time a user changes positions, access will be deactivated once the employer submits a SAR to remove access.

Section 4: Information Sharing

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

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component	x	x	x	
DOJ components				
Federal entities				
State, local, tribal gov't entities				
Public				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an

unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.) [In answering the question, you should discuss the relevant NIST Confidentiality Safeguard Security Controls.]

The use of any information in FRA must comply with FBI policies and procedures, which incorporate privacy and civil liberty protections to minimize the threats to privacy that may occur when information is disclosed. The FRA is a reporting application. No data is shared outside of the FBI by the application.

The information used in the FRA comes from FMS and UFMS-S directly, and both have implemented the National Institute of Standards and Technology (NIST) 800-53 controls, which are referenced in NIST 800-122. The FRA incorporates security protections into the system to minimize the risk that information is disclosed or accessed in an unauthorized manner. For example, all authorized users must be authenticated through EPAS. System security logs are configured to keep track of successful and unsuccessful login. The ISSO will report all failed attempts to the business owner so that appropriate action can be taken.

Since FFD is the business owner of both FRA and UFMS-S, an internal memorandum of understanding (MOU) between these systems is not required and does not exist. Data connections are not shared or distributed to any external system from FRA. FRA has an internal MOU with the FBI's Human Resource Division (HRD) regarding consumption of human resource and payroll data from HR Source, the FBI's official human resources system. HR Source data is combined with UFMS data via FRA for use in Travel W-2 Forms and Vendor Reports. These reports are limited to a subset of authorized users.

Section 5: Notice, Consent, and Redress

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

x	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

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

	Yes, individuals have the opportunity to	Specify how:

	decline to provide information.	
x	No, individuals do not have the opportunity to decline to provide information.	Specify why not: FRA does not collect PII directly from individuals. FRA uses already collected PII from UFMS-S and other systems.

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

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:
x	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: FRA does not collect PII directly from individuals. FRA uses already collected PII from UFMS-S and other systems.

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

FRA does not collect PII directly from individuals, so does not provide specific notice in a Privacy Act Statement. FRA uses UFMS-S data that includes already collected PII from other Federal IT systems. The Federal IT systems that collect PII directly from individuals provide specific notice and opportunity to consent to particular uses including financial management and procurement operations, which the FRA supports. For more information, see the DOJ/JMD "Unified Financial Management System" PIA posted at https://www.justice.gov/opcl/doj-privacy-impact-assessments.

Section 6: Information Security

6.1 Indicate all that apply.

X	A security risk assessment has been conducted.

X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: FRA contains classified information and operates at the System Moderate Mode of Operation. Its Levels of Concern are Moderate for Confidentiality, Moderate for Integrity, and Moderate for Availability. Applicable security controls can be found in the System Security Plan located in the RiskVision system.	
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: Annual User Audits are conducted to determine if individuals still require access to the FRA. The ISSO has server scans scheduled regularly. Privileged users to the FRA take the Annual Privileged User Training on Virtual Academy.	
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: FRA has an Authorization to Operate (ATO) with an expiration date of January 10, 2026.	
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: Resource Management is the tool used to monitor all system access. Activity is maintained for audit for one year.	
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.	
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.	
X	The following training is required for authorized users to access or receive information in the system:	
	X	General information security training
		Training specific to the system for authorized users within the Department.
		Training specific to the system for authorized users outside of the component.
	X	Other (specify): Annual Privileged User Training

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure. [In answering the question, you should discuss the relevant NIST Confidentiality Safeguard Security Controls.]

SSNs and other PII used by FRA are authorized for use by a limited number of FBI personnel who have the responsibility for downloading data onto the Travel W-2 forms and vendor studies and reports on vendor activities. System access controls are enforced to ensure that only the FBI personnel with such responsibility have access to the SSNs. All users are required to be vetted, authorized, and authenticated to access FRA. Once authenticated, access to the system is limited based on a user's role. Access information is audited and reviewed by the system's staff. Users are required to take training to further mitigate any unintentional information disclosure. Each time they access the FRA, users are required to acknowledge the system Warning banner as follows:

> **WARNING!** You are accessing a U.S. Government information system, which includes this computer, this computer network, all computers connected to this network, and all devices and/or storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only. Unauthorized or improper use of this system may result in disciplinary action, and civil and criminal penalties. By using this information system, you understand and consent to the following: You have no reasonable expectation of privacy regarding any communications transmitted through or data stored on this information system. At any time, the government may monitor, intercept, search and/or seize data transiting or stored on this information system. Any communications transmitted through or data stored on this information system may be disclosed or used for any U.S. Government-authorized purpose.

Section 7: Privacy Act

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

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: Accounting Systems for the Department of Justice, **DOJ-001**, 69 Fed. Reg. 31406 (June 3, 2004); DOJ Computer Systems Activity and Access Records, **DOJ-002**, 64 Fed. Reg. 73585 (Dec. 30, 1999); DOJ Payroll System, **JMD-003**, 69 Fed. Reg. 107 (Jan. 2, 2004).
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

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

The FRA is a financial and procurement management reporting tool. Users choose the report format or create a custom report format and then choose the information to load into that report. The information chosen from the underlying source systems (i.e., UFMS-S, FIT, AMS, Phoenix, HR Source, and EPAS/TRIP) will depend on the type of report format and the role-based access authorizations and restrictions assigned to the user. The information retrieved can be either in the aggregate at various organizational levels (such as FBI unit or section) or for a specific individual (such as name or credit card number).