

U.S. Nuclear Regulatory Commission

Privacy Impact Assessment

Designed to collect the information necessary to make relevant determinations regarding the applicability of the Privacy Act, the Paperwork Reduction Act information collection requirements, and records management requirements.

Financial Management Systems (FMS)

Date: February 9, 2022

A. GENERAL SYSTEM INFORMATION

- 1. Provide a detailed description of the system:** *(Use plain language, no technical terms.)*

FMS is owned and managed by the Office of the Chief Financial Officer (OCFO). FMS provides the framework for managing cybersecurity compliance for OCFO financial services and systems used by the Nuclear Regulatory Commission (NRC). FMS is an umbrella system that is comprised of subsystems that support mission and business functions that OCFO provides for the agency. FMS consists of six subsystems: Cost Activity Code System (CACCS), Financial Account and Integrated Management Information System (FAIMIS), eBilling (EB), Human Resources Management System (HRMS), Human Resources Management System Cloud (HRMS-C), and Oracle Planning and Budgeting Cloud (OPBC). Each subsystem is described below.

In addition to the above mentioned subsystems, under the FMS Main boundary, OCFO operates five servers as services:

- Four servers which have been repurposed from the Budget Formulation System (BFS) for Financial Management Data Mart (FMDM, previously known as the “Financial Management Data Warehouse”) activities (ML21140A238). BFS was previously a subsystem under the FMS boundary; however, OCFO migrated BFS applications to the cloud in OPBC. The FMDM serves as a centralized repository of integrated data from the NRC's financial management systems (i.e., FAIMIS, BFS, etc.). Its primary purpose is to provide timely, accurate financial data from authoritative data sources for the purpose of reporting and data analytics. The FMDM will also feed data to the NRC Enterprise Data Warehouse.
- A Secure File Transfer Protocol (SFTP) server which is used to facilitate file transfer between NRC and Oracle Human Capital Management (HCM) Cloud for the HRMS-C (ML21022A387).

Cost Activity Code System (CACCS)

CACCS is the modernized system for work planning and authorization, scheduling, conducting, reporting, and analyzing agency activities executed by NRC staff. CACCS Labor and Assignment related reports provide agency users with easy to launch reporting products with multiple criteria to choose from. NRC staff access CACCS through an internal web portal.

CACCS replaced Task Assignment Control System (TACS) that was deployed in 1998 as part of the NRC's Reactor Program System to support the agency's license fee billing process. The primary function of TACS was to create and maintain distinct codes that are used by all NRC employees to enter time spent on various work activities, projects or services, both billable and non-billable, across all business lines.

Financial Accounting and Integrated Management Information System (FAIMIS)

FAIMIS is a multi-tier, distributed, financial management system supporting dynamic interoperability with other federal systems and providing both financial planning capabilities and the means to record financial transactions. FAIMIS is the NRC's official repository for the agency's financial records and is used to produce official agency financial reports. FAIMIS is based upon the CGI Momentum™ Enterprise Resource Planning commercial off-the-shelf (COTS) suite. FAIMIS records purchasing, accounts receivable, accounts payable, disbursements, and other budget activities that are integrated so the transactions, when processed, can update budgets, financial plans, and the general ledger. FAIMIS also offers the functions needed to consolidate financial reports and controls.

Using FAIMIS, NRC staff is able to:

- Track and manage the budget;
- Compute and track performance data;
- Distribute project costs to appropriate offices;
- Provide user-defined queries;
- Perform online analytical processing to enhance decision processing;
- Program spending alerts for key budget items;
- Provide real-time and ad hoc reporting capabilities; and
- Bill and collect NRC License Fee Billing costs/fees.

eBilling (EB)

The eBilling system is a modern and user-friendly web-based electronic billing solution, providing the NRC's licensees with the ability to view and pay their invoices online. eBilling automates and improves several billing processes that NRC handled manually. Licensees can maintain their own account details, such as their official billing address, within the eBilling tool, "publish" invoices to the eBilling application through a cohesive integration within FAIMIS, and receive the status of their invoices as well as their invoice details and export them to Microsoft Excel for analysis.

Human Resources Management System (HRMS)

Note: OCFO is currently in the process of migrating the HRMS subsystem from on-premise components to the Oracle HCM Cloud. HRMS-C received its full authority to operate as a subsystem of FMS on December 15, 2021.

HRMS is used to capture time, attendance, and labor data. HRMS contains a customized COTS product from Oracle PeopleSoft (PS). The PS product provides four modules: human resources (HR), time and labor (T&L), training administration, and payroll. HRMS only uses the T&L module and provides historical HR and payroll information. The T&L module requires all employees to be self-reporters and to enter time taken for vacation, sick leave, jury duty, etc. It also tracks monthly leave accrual (vacation and sick hours earned each month vs. hours taken) and tracks positive pay and leave (exception) time.

Human Resources Management System Cloud (HRMS-C)

HRMS-C is NRC's instance of the FedRAMP authorized Software-as-a-Service (SaaS) for HCM product from Oracle that complies with federal systems standards and security requirements for major financial systems. The Oracle SaaS HCM product consists of numerous components comprising their Human Capital Management System. The HRMS-C uses only the T&L module and includes historical human resources and payroll information. The Oracle HCM T&L module requires all employees, as self-reporters, to enter time taken for vacation, sick leave, jury duty, etc. The system also tracks monthly leave accruals (how many vacation and sick hours earned each month vs. how many hours taken) and tracks positive pay and leave (exception) time.

The HRMS-C system processes, stores, and contains personal identity, human resource, revenue collection, income, debt collection, entitlements, accounting, and benefit management information.

Oracle Planning and Budgeting Cloud (OPBC)

OPBC is used for simplifying and improving the formulation, development, operation, and maintenance of the agency's planning, budgeting, and forecasting processes. OCFO procured the cloud service from Oracle as a SaaS solution hosted in a community cloud infrastructure designed by Oracle for federal agencies. OPBC assists staff involved in planning and forecasting efforts to:

1. Reduce the administrative burden (e.g., eliminate excessive staff time and the duplication of data entry of financial information into multiple systems);
2. Improve quality, timelines, and confidence in the budget formulation outcome; increase credibility by producing accurate and concise financial forecasting and budget data and produce “what if” scenarios; and
3. Reduce large amounts of paper used to produce the financial planning reporting, enable the end-user to access the budget and forecasting information electronically, and improve the security of the system by enabling electronic authentication and authorization to read, write, view, etc.

Separate Privacy Impact Assessments (PIAs) and/or Privacy Threshold Analyses (PTAs) have been performed on the individual subsystems. No further information/discussion of the FMS subsystems is contained in this FMS PIA.

2. **What agency function does it support?** *(How will this support the U.S. Nuclear Regulatory Commission’s (NRC’s) mission, which strategic goal?)*

BFS servers in the FMDM

The repurposed BFS servers in the FMDM assist in the effort to provide reporting and analysis of financial data at the NRC.

HRMS-C SFTP server

The SFTP server facilitates data transfer with NRC systems (HRMS, FAIMIS, BFS, and CACS), the Department of the Interior’s (DOI) Federal Personnel Payroll System (FPPS), and Oracle HCM Cloud in order to support HRMS-C employee activity-based hour recording, payroll management, and fee billing.

3. **Describe any modules or subsystems, where relevant, and their functions.**

Refer to section A.1.

- a. **Provide ADAMS ML numbers for all Privacy Impact Assessments or Privacy Threshold Analysis for each subsystem.**

- CACS PTA – ML20197A209.
- FAIMIS PIA – ML18303A105.
- eBilling PTA – ML19066A224
- HRMS PIA – ML18305A362.
- HRMS-C PIA – ML21025A267.
- OPBC PTA – ML18163A026.

4. **What legal authority authorizes the purchase or development of this system?** *(What law, regulation, or Executive Order authorizes the collection and maintenance of the information necessary to meet an official program mission or goal? NRC internal policy is not a legal authority.)*

BFS servers in the FMDM

Legacy PAYPERS DB – 5 United States Code (U.S.C.) 5101 et seq., 5501 et seq., 5 U.S.C. 5701 et seq., 5525 et seq., 6301 et seq.; 31 U.S.C. 716, 1104, 1105, 1108, 3325, 3511, 3512, 3701, 3711, 3717, 3718; Executive Order 9397 (Nov. 22, 1943); Public Law 104-193, Personal Responsibility and Work Opportunity Reconciliation Act of 1996.

HRMS-C SFTP server

26 Code of Federation Regulations (CFR) 31.6011(b)(2), 31.6109–1; 5 U.S.C. 6334; 5 U.S.C. Part III, Subpart D; 31 U.S.C. 716; 31 U.S.C. Chapters 35 and 37.

5. **What is the purpose of the system and the data to be collected?**

BFS servers in the FMDM

Support budget formulation and forecasting needs for the NRC across procurement spending, commitment planning, salaries, and benefits, Full Time Equivalent (FTE), and funding for employees.

HRMS-C SFTP server

Refer to sections A.1 and A.2.

6. **Points of Contact:** *(Do not adjust or change table fields. Annotate N/A if unknown. If multiple individuals need to be added in a certain field, please add lines where necessary.)*

Project Manager	Office/Division/Branch	Telephone
Abby Olarte	OCFO/DOC/FSB	301-415-6288
Sharon Clarkson	OCFO/DOC/FSB	301-415-8483
Business Project Manager	Office/Division/Branch	Telephone
Susan Hayden	OCFO/DOC/FSB	301-415-6206
Erikka Legrand	OCFO/DOC/FSOB	301-415-7748
Technical Project Manager	Office/Division/Branch	Telephone
Samuel Momotiuk	OCFO	N/A
Daniel Klein	OCFO	N/A

Rei-Mei Shieh	OCIO/ITSDOD	301-287-0517
Executive Sponsor	Office/Division/Branch	Telephone
Cherish Johnson	OCFO	301-415-7322
ISSO	Office/Division/Branch	Telephone
Tung Truong	OCFO/DOC/FSB	301-415-8490
System Owner/User	Office/Division/Branch	Telephone
Cherish Johnson	OCFO	301-415-7322

7. Does this privacy impact assessment (PIA) support a proposed new system or a proposed modification to an existing system?

- a. New System
 Modify Existing System
 Other

b. If modifying or making other updates to an existing system, has a PIA been prepared before?

BFS servers in the FMDM
Legacy PAYPERS DB – Yes, Payroll Historical Database (PHDB).

HRMS-C SFTP server
No.

(1) If yes, provide the date approved and the Agencywide Documents Access and Management System (ADAMS) accession number.

BFS servers in the FMDM
August 17, 2006 – ML062140244.

HRMS-C SFTP server
N/A.

- (2) **If yes, provide a summary of modifications or other changes to the existing system.**

BFS servers in the FMDM

The Legacy PAYPERS DB stored and maintained Time & Attendance records and Earnings & Leave Statements for NRC employees between November 1998 and November 2001. After the frontend application was retired in 2002, the data collected by PAYPERS was put into the new PHDB for historical purposes and later was migrated to the HRMS subsystem. In 2021, the PAYPERS DB was moved to the BFS servers repurposed for FMDM activities.

Please note that the data originally stored in the PAYPER DB has not been modified since the data was originally collected.

HRMS-C SFTP server

N/A.

8. **Do you have an NRC system Enterprise Architecture (EA)/Inventory number?**

Yes.

- a. **If yes, please provide the EA/Inventory number.**

20190012.

- b. **If no, please contact [EA Service Desk](#) to get the EA/Inventory number.**

B. INFORMATION COLLECTED AND MAINTAINED

These questions are intended to define the scope of the information requested as well as the reasons for its collection. Section 1 should be completed only if information is being collected about individuals. Section 2 should be completed for information being collected that is not about individuals.

1. INFORMATION ABOUT INDIVIDUALS

- a. **Does this system maintain information about individuals?**

Yes.

- (1) **If yes, identify the group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public (provide description for general public (non-licensee workers, applicants before they are licenses etc.)).**

Federal – NRC employees.

(2) IF NO, SKIP TO QUESTION B.2.

- b. What information is being maintained in the system about an individual (be specific – e.g. Social Security Number (SSN), Place of Birth, Name, Address)?**

BFS servers in the FMDM

Employee name, ID, location, position, and position ID; as well as pay amounts (salary and benefits), hours charged, and time codes used.

Legacy PAYPERS DB – employee name, date of birth, SSN, and address. Please note, this information was collected from November 1998 through November 2001. The PAYPERS front end application has since been retired, and no further information was collected. This information is available based on need and in read-only view.

HRMS-C SFTP server

General employee information (first name, last name, SSN), salaries, and benefits, leave balances, payroll data, time and attendance data, and activity-based work hours.

- c. Is information being collected from the subject individual? (*To the greatest extent possible, collect information about an individual directly from the individual.*)**

BFS servers in the FMDM

No.

HRMS-C SFTP server

No – All data in the SFTP server comes from files delivered to the server via interface.

- (1) If yes, what information is being collected?**

N/A.

- d. Will the information be collected from individuals who are not Federal employees?**

No.

- (1) If yes, does the information collection have the Office of Management and Budget's (OMB) approval?**

N/A.

- (a) If yes, indicate the OMB approval number:**

N/A.

e. Is the information being collected from existing NRC files, databases, or systems?

Yes.

(1) If yes, identify the files/databases/systems and the information being collected.

BFS servers in the FMDM

HRMS (will become HCM in the future) & FPPS/OCHCO – Salary/benefit amounts, employee duty location, employee pay grade/step, position title, employee and position ID, hours worked, and time codes charged.

Legacy PAYPERS DB – Refer to section B.1.b.

HRMS-C SFTP server

All data in the SFTP server comes from files delivered to the server via interface. The SFTP server maintains files from the following NRC systems:

- CACS – employee CAC/Docket/EPID assignments.
- HRMS – timesheet information.

f. Is the information being collected from external sources (any source outside of the NRC)?

BFS servers in the FMDM

No.

HRMS-C SFTP server

Yes.

(1) If yes, identify the source and what type of information is being collected?

BFS servers in the FMDM

N/A.

HRMS-C SFTP server

All data in the SFTP server comes from files delivered to the server via interface. The SFTP server maintains files from the following systems:

- Oracle HCM Cloud - hours information with missing PA codes, payroll information for GL postings, cost accounting information, NRC employee addresses and bank account data for travel reimbursement (for FAIMIS), time and absence information (for DOI FPPS); salary and benefits information (for BFS); and employee CAC/Docket/EPID

assignments, time data, reported hours, and approvers' data and pay period dates information (for CACS).

- DOI FPPS – department, grade, and position data; employee demographic, employment, and supervisory information; salary data (base salary); payroll assigned to each employee to drive pay period information; leave balances, and cost data.

g. How will information not collected directly from the subject individual be verified as current, accurate, and complete?

BFS servers in the FMDM

Data is sourced from the respective systems of record at NRC, such as FAIMIS or HRMS.

Legacy PAYPERS DB – the information was verified in 2002 when the PHDB was tested and compared to the PAYPERS system from which it was derived.

HRMS-C SFTP server

Data accuracy is verified on the respective systems on which the data is originally collected from the individual (Oracle HCM Cloud; FPPS via Employee Express, Monster, or the Entrance on Duty System). Subsequent verification can be done via Employee Express by reviewing the biweekly Earning and Leave Statement.

h. How will the information be collected (e.g. form, data transfer)?

BFS servers in the FMDM

Direct connection (linked server, JDBC connections), or flat file.

Legacy PAYPERS DB – data was transferred from the PAYPERS system to the PHDB in 2002.

HRMS-C SFTP server

All data in the SFTP server is collected from the respective system (HRMS-C, FAIMIS, FPPS, etc.) and their corresponding files are uploaded to the server. After which point, the files are transported to their respective applications, servers, or file locations.

2. INFORMATION NOT ABOUT INDIVIDUALS

a. Will information not about individuals be maintained in this system?

BFS servers in the FMDM

Yes.

HRMS-C SFTP server

No.

(1) If yes, identify the type of information (be specific).

BFS servers in the FMDM

- BFS – Procurement spend planning, budget formulation, commitment planning.
- FMDM – Accounts Payable, Budget Execution Reporting, forward funding, Part 170 data.
- FAIMIS – General financial information (commitments, obligations, expenditures).
- STAQS – Contract information (ceiling, period of performance, COR) used for procurement spend planning.
- FedPass – Transmission of pending IT changes between approvers and financial planners within BFS's commitment planning module.

Legacy PAYPERS DB – N/A, all data is about individuals.

HRMS-C SFTP server

N/A.

b. What is the source of this information? Will it come from internal agency sources and/or external sources? Explain in detail.

BFS servers in the FMDM

Internal NRC sources – FAIMIS, STAQS, FedPass, PAYPERS DB.

HRMS-C SFTP server

N/A.

C. USES OF SYSTEM AND INFORMATION

These questions will identify the use of the information and the accuracy of the data being used.

1. Describe all uses made of the data in this system.

BFS servers in the FMDM

Future funding considerations and decisions, Financial reporting, Tableau dashboard reporting.

HRMS-C SFTP server

All files on the SFTP server will be used for HRMS-C purposes. As per the HRMS-C PIA (ML21025A267), "uses of the data are as follows: data transmissions to DOI for paycheck and leave balances calculations, license fees billings, updates to the agency's core financial system, financial reporting, project

management, salary and benefits modeling, cost accounting modeling, and strategic workforce planning.”

Future uses include sharing HR data from FPPS with a variety of internal subscribing systems (Personnel Security Adjudication Tracking System [PSATS], Space and Property Management System [SPMS], Ethics, Talent Management System [TMS], and Active Directory) to automate the generation and distribution of files currently produced manually.

2. Is the use of the data both relevant and necessary for the purpose for which the system is designed?

Yes.

3. Who will ensure the proper use of the data in this system?

BFS servers in the FMDM
OCFO and the BFS Team.

HRMS-C SFTP server
The system administrator (OCIO) and the application administrators (OCHCO) will ensure proper use of the data.

4. Are the data elements described in detail and documented?

BFS servers in the FMDM
Yes – Some data sets do have detailed field listings.

HRMS-C SFTP server
No – Documentation is still in development.

a. If yes, what is the name of the document that contains this information and where is it located?

BFS servers in the FMDM
Please refer to the [FMDM SharePoint site](#) for data set-specific [Quick Reference Guides](#).

HRMS-C SFTP server
Documentation will be housed in the HCM Cloud Project SharePoint site.

5. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

BFS servers in the FMDM
Yes – Data is aggregated for individuals for salary and benefits to provide a comprehensive agency view.

HRMS-C SFTP server
No.

Derived data is obtained from a source for one purpose and then the original information is used to deduce/infer a separate and distinct bit of information that is aggregated to form information that is usually different from the source information.

Aggregation of data is the taking of various data elements and then turning it into a composite of all the data to form another type of data (i.e. tables or data arrays).

a. If yes, how will aggregated data be maintained, filed, and utilized?

BFS servers in the FMDM

Aggregated data is maintained through the use of standardized metadata hierarchies that ensure control and accuracy.

HRMS-C SFTP server

N/A.

b. How will aggregated data be validated for relevance and accuracy?

BFS servers in the FMDM

Refer to section C.5.a.

HRMS-C SFTP server

N/A.

c. If data are consolidated, what controls protect it from unauthorized access, use, or modification?

BFS servers in the FMDM

Access controls exist on the application and associated Tableau data sets to ensure that only allowed individuals can access this data.

HRMS-C SFTP server

N/A.

6. How will data be *retrieved* from the system? Will data be retrieved by an individual's name or personal identifier (name, unique number or symbol)? (Be specific.)

BFS servers in the FMDM

Users will not typically view data in this manner, but employee name/ID can be used to pull data for a specific individual.

HRMS-C SFTP server

Data will not generally be retrieved at the individual employee level except in cases of data quality assurance (QA) or troubleshooting. In those cases, Employee ID will usually be used.

- a. **If yes, explain, and list the identifiers that will be used to retrieve information on the individual.**

BFS servers in the FMDM

Refer to section C.6.

HRMS-C SFTP server

For QA/troubleshooting purposes, any relevant identifier may be used, including name, employee ID, SSN, bank account number, etc.

7. **Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register?**

BFS servers in the FMDM

Legacy PAYPERS DB – Yes.

HRMS-C SFTP server

Yes.

- a. **If “Yes,” provide name of SORN and location in the Federal Register.**

BFS servers in the FMDM

NRC-21 – Payroll Accounting Records.

HRMS-C SFTP server

US Federal Government-wide SORN.

8. **If the information system is being modified, will the SORN(s) require amendment or revision?**

No.

9. **Will this system provide the capability to identify, locate, and monitor (e.g., track, observe) individuals?**

No.

- a. **If yes, explain.**

N/A.

- (1) **What controls will be used to prevent unauthorized monitoring?**

N/A.

10. **List the report(s) that will be produced from this system.**

BFS servers in the FMDM

Various reports related to budget formulation and forecasting needs for the NRC across procurement spending, commitment planning, salaries and benefits, FTE,

and funding for employees. Custom reports can also be created by users themselves in Tableau.

HRMS-C SFTP server

Only log files of transfer and file preparation activities will be produced. The reports will contain no data records from the files being transferred or created.

a. What are the reports used for?

BFS servers in the FMDM

Insights related to procurement spending, commitment planning, salaries and benefits, FTE, and funding for employees.

HRMS-C SFTP server

Reporting status (success or failure) of file transfer and preparation processes.

b. Who has access to these reports?

BFS servers in the FMDM

Access depends on the specific report in question, but access is generally controlled by provisioning models in both BFS and Tableau.

HRMS-C SFTP server

They system administrator, application administrator, computer operator, and select e-mail recipients will have access to the reports.

D. ACCESS TO DATA

1. Which NRC office(s) will have access to the data in the system?

BFS servers in the FMDM

Server access is restricted to OCFO BFS administrators.

However, data stored on the BFS servers for the purpose of the FMDM is available to NRC personnel who have requested access to the budget formulation data set. Request forms must be reviewed and approved by OCFO.

HRMS-C SFTP server

Sever access is restricted to OCIO administrators a limited number of OCHCO personnel.

(1) For what purpose?

BFS servers in the FMDM

Server administration.

Access to the budget formulation data set in the FMDM is permitted for NRC personnel who have roles/responsibilities related to budget planning/reporting.

HRMS-C SFTP server
Server administration and HR related activities.

(2) Will access be limited?

BFS servers in the FMDM
Yes.

HRMS-C SFTP server
Yes – only individuals from the above mentioned groups are granted access to perform official duties.

2. Will other NRC systems share data with or have access to the data in the system?

Yes.

(1) If yes, identify the system(s).

BFS servers in the FMDM
HRMS, FAIMIS, STAQS, and FedPass.

HRMS-C SFTP server
CACs, FAIMIS, HRMS, and BFS.

(2) How will the data be transmitted or disclosed?

BFS servers in the FMDM

- HRMS provides general employee information, employee salaries, as well as benefits, payroll, time and attendance, and activity-based work hour data via SQL server link for the BFS SALARY module.
- FAIMIS provides financial transaction activity data via JDBC connection for BFS BUDGET and SPENDPLN module.
- STAQS provides procurement contractual activity data via SQL server link for the BFS SPENDPLN module.

HRMS-C SFTP server
The data is transferred via batch file interfaces. All file transfers between Oracle HCM Cloud and the SFTP server occur through a VPN tunnel.

3. Will external agencies/organizations/public have access to the data in the system?

BFS servers in the FMDM
No.

HRMS-C SFTP server
No – Only NRC personnel can access the SFTP server directly.

(1) **If yes, who?**

N/A.

(2) **Will access be limited?**

N/A.

(3) **What data will be accessible and for what purpose/use?**

N/A.

(4) **How will the data be transmitted or disclosed?**

N/A.

E. RECORDS AND INFORMATION MANAGEMENT (RIM) - RETENTION AND DISPOSAL

The National Archives and Records Administration (NARA), in collaboration with federal agencies, approves whether records are temporary (eligible at some point for destruction/deletion because they no longer have business value) or permanent (eligible at some point to be transferred to the National Archives because of historical or evidential significance). These determinations are made through records retention schedules and NARA statutes (44 United States Code (U.S.C.), 36 Code of Federation Regulations (CFR)). Under 36 CFR 1234.10, agencies are required to establish procedures for addressing records management requirements, including recordkeeping requirements and disposition, before approving new electronic information systems or enhancements to existing systems. The following question is intended to determine whether the records and data/information in the system have approved records retention schedule and disposition instructions, whether the system incorporates Records and Information Management and NARA's Universal Electronic Records Management requirements, and if a strategy is needed to ensure compliance.

1) **Can you map this system to an applicable retention schedule in [NRC's Comprehensive Records Disposition Schedule \(NUREG-0910\)](#), or NARA's [General Records Schedules \(GRS\)](#)?**

BFS servers in the FMDM

No – There is no specific retention period for this data. The data is helpful to the agency in resolving HR and payroll issues, so it should be kept as long as possible.

HRMS-C SFTP server

Yes – Leveraging from HRMS-C PIA (ML21025A267) and provided in the table below.

a. **If yes, please cite the schedule number, approved disposition, and describe how this is accomplished (then move to F.1).**

- **For example, will the records or a composite thereof be deleted once they reach their approved retention or exported to an approved file format for transfer to the National Archives based on their approved disposition?**

BFS servers in the FMDM

N/A.

HRMS-C SFTP server

<u>System (or module)</u>	<u>Schedule Number/ NARA Disposition Authority Number</u>	<u>Schedule Title</u>	<u>Disposition Instruction</u>
CACS (formerly TACS)	NUREG 2.6 item 18 / NC1- 431-81-2 Item 12.F	Technical Assignment Control System (TACS)	Retain until it has been determined by a competent NRC Official that data are no longer needed; erase and reuse tape, etc.
FAIMIS Masterfile	N1-431-10-001 item 2	Financial Accounting and Integrated Management Information System	Temporary. Cut off at the fiscal year and transfer to inactive storage within FAIMIS data storage. Destroy/delete 10 years after cutoff.
FAIMIS Documentation			Temporary. Destroy 5 years after the project/activity/transaction is completed or superseded, or the associated system is terminated, or the associated data is migrated to a successor system, but longer retention is authorized if required for business use.
eBilling	(follow schedule and disposition for FAIMIS)		
OPBC (migration from BFS on- premises)	GRS 1.3 – Budgeting Records	Oracle Planning and Budgeting Cloud	(See the NARA link for schedule items and disposition instructions)

HRMS-C	GRS 2.4 item 010	Records used to calculate payroll, arrange paycheck deposit, and change previously issued paychecks.	Temporary. Destroy 2 years after employee separation or retirement, but longer retention is authorized if required for business use.
HRMS-C	GRS 2.4 item 030	Time and attendance records.	Temporary. Destroy after Government Accountability Office (GAO) audit or when 3 years old, whichever is sooner.
HRMS-C	GRS 2.4 item 040	Agency payroll record for each pay period.	Temporary. Destroy when 56 years old.
HRMS-C	GRS 2.4 item 050	Wage and tax statements.	Temporary. Destroy when 4 years old, but longer retention is authorized if required for business use.
HRMS-C	GRS 2.4 item 060	Payroll program administrative records. Administrative correspondence between agency and payroll processor, and system reports used for agency workload and or personnel management purposes.	Temporary. Destroy when 2 years old, but longer retention is authorized if required for business use.
HRMS-C	GRS 2.4 item 061	Payroll program administrative records. Payroll system reports providing fiscal information on agency payroll.	Temporary. Destroy when 3 years old or after GAO audit, but longer retention is authorized if required for business use.
HRMS	GRS 2.2 item 040	OPF/eOPF Long-term records	Temporary. Destroy when survivor or retirement claims are adjudicated or when records are 129 years old, whichever is sooner, but longer retention is authorized if required for business use.
HRMS	GRS 2.2 item 041	OPF/eOPF Short-term records	Temporary. Destroy when superseded or obsolete, or upon separation or transfer of employee, whichever is earlier.
HRMS	GRS 2.2 item 060	Employee eligibility verification records	Temporary. Destroy 3 years after employee separates from service or transfers to another agency.

HRMS	GRS 2.2 item 070	Employee performance file system records. Acceptable performance appraisals of non-senior executive service employees	Temporary. Destroy no sooner than 4 years after date of appraisal, but longer retention is authorized if required for business use.
HRMS	GRS 2.2 item 072	Employee performance file system records. Records of senior executive service employees	Temporary. Destroy no sooner than 5 years after date of appraisal, but longer retention is authorized if required for business use.
HRMS	GRS 2.6 item 010	Non-mission employee training program records	Temporary. Destroy when 3 years old, but 3 years after superseded or obsolete, whichever is appropriate, but longer retention is authorized if required for business use.
HRMS	GRS 2.6 item 030	Individual employee training records	Temporary. Destroy when superseded, 3 years old, or 1 year after separation, whichever comes first, but longer retention is authorized if required for business use.
HRMS	GRS 2.4 item 040	Agency payroll record for each pay period	Temporary. Destroy when 56 years old.
HRMS	GRS 2.4 item 030	Time and attendance records	Temporary. Destroy after GAO audit or when 3 years old, whichever is sooner.
HRMS	GRS 2.5 item 020	Individual employee separation case files	Temporary. Destroy 1 year after date of separation or transfer, but longer retention is authorized if required for business use.
HRMS	GRS 2.4 item 020	Tax withholding and adjustment documents	Temporary. Destroy 4 years after superseded or obsolete, but longer retention is authorized if required for business use.
HRMS	GRS 2.4 item 050	Wage and tax statements	Temporary. Destroy when 4 years old, but longer retention is authorized if required for business use.
HRMS	GRS 2.4 item 010	Records used to calculate payroll, arrange paycheck deposit, and change	Temporary. Destroy 2 years after employee separation or retirement, but longer retention is authorized if required for business use.

		previously issued paychecks	
HRMS	GRS 2.4 061	Payroll program administrative records. Payroll system reports providing fiscal information on agency payroll.	Temporary. Destroy when 3-year-old or after GAO audit, but longer retention is authorized if required for business use.
HRMS	GRS 2.4 item 060	Payroll program administrative records. Administrative correspondence between agency and payroll processor, and system reports used for agency workload and or personnel management purposes.	Temporary. Destroy when 2 years old, but longer retention is authorized if required for business use.

b. If no, please contact the [RIM](#) staff at ITIMPolicy.Resource@nrc.gov.

F. TECHNICAL ACCESS AND SECURITY

1. Describe the security controls used to limit access to the system (e.g., passwords).

BFS servers in the FMDM

Accounts for BFS administrators and FMDM users viewing budgeting data are restricted to NRC personnel with a LAN ID and a need-to-know.

HRMS-C SFTP server

Authorized users are granted SSH/SFTP access. PIV cards are used to authenticate to the NRC network, then username and password authentication is used to access accounts on the server.

2. What controls will prevent the misuse (e.g., unauthorized browsing) of system data by those having access?

BFS servers in the FMDM

Users only have access to the data for which they have a need-to-know. Data sources themselves cannot be edited without stepped up access provisions, such as administrator provisions.

HRMS-C SFTP server

Sessions time out after 5 minutes of inactivity, and user accounts expire every 60 days. Role-based training is required for privileged accounts.

3. Are the criteria, procedures, controls, and responsibilities regarding access to the system documented?

BFS servers in the FMDM

Yes.

HRMS-C SFTP server

No – Documentation is under development.

(1) If yes, where?

BFS servers in the FMDM

[There is a standardized access request form workflow.](#)

HRMS-C SFTP server

Documentation will be housed in the HCM Cloud Project SharePoint site.

4. Will the system be accessed or operated at more than one location (site)?

BFS servers in the FMDM

Some of the BFS applications reside in separate URLs.

HRMS-C SFTP server

No.

a. If yes, how will consistent use be maintained at all sites?

BFS servers in the FMDM

Access control is governed by URL; therefore, control can be consistently applied even across the different BFS URL links.

HRMS-C SFTP server

N/A.

5. Which user groups (e.g., system administrators, project managers, etc.) have access to the system?

BFS servers in the FMDM

Only system administrators have server access, but various analysts and employees throughout the NRC have access to the BFS applications.

HRMS-C SFTP server

System administrators and a limited number of OCHCO personnel.

6. Will a record of their access to the system be captured?

Yes.

a. If yes, what will be collected?

BFS servers in the FMDM

Auditing tools track user/administrator actions, such as data updates, calculations runs, metadata updates, etc.

HRMS-C SFTP server

Auditing of all user accounts logon activities and cron events are enabled. Audit logs are forwarded to Splunk and reviewed daily.

7. Will contractors be involved with the design, development, or maintenance of the system?

BFS servers in the FMDM

Yes.

HRMS-C SFTP server

No.

If yes, and if this system will maintain information about individuals, ensure Privacy Act and/or Personally Identifiable Information (PII) contract clauses are inserted in their contracts.

- *Federal Acquisition Regulation (FAR) clause 52.224-1 and FAR clause 52.224-2 should be referenced in all contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function.*
- *PII clause, "Contractor Responsibility for Protecting Personally Identifiable Information" (June 2009), in all contracts, purchase orders, and orders against other agency contracts and interagency agreements that involve contractor access to NRC owned or controlled PII.*

8. What auditing measures and technical safeguards are in place to prevent misuse of data?

BFS servers in the FMDM

Access control and custom security (cell-level security) mechanisms restrict access, and auditing functionality ensures tracking of data updates.

HRMS-C SFTP server

Refer to sections F.2 and F.6.

9. Is the data secured in accordance with the Federal Information Security Management Act (FISMA) requirements?

Yes.

- a. **If yes, when was Certification and Accreditation last completed? And what FISMA system is this part of?**

FMS received Chief Information Security Officer (CISO) approval to function as an umbrella system in order to consolidate OCFO financial systems under one management framework on May 29, 2019.

The security authorization will remain in effect as long as the System Owner satisfies the Periodic System Cybersecurity Assessment requirement. The most recent assessment was performed June 16, 2021 (ML21194A418).

- b. **If no, is the Certification and Accreditation in progress and what is the expected completion date? And what FISMA system is this planned to be a part of?**

N/A.

- c. **If no, please note that the authorization status must be reported to the Chief Information Security Officer (CISO) and Computer Security Office's (CSO's) Point of Contact (POC) via e-mail quarterly to ensure the authorization remains on track.**

N/A.

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL
(For Use by OCIO/GEMSD/CSB Staff)

System Name: Financial Management Systems (FMS)

Submitting Office: OCFO

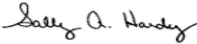
A. PRIVACY ACT APPLICABILITY REVIEW

Privacy Act is not applicable.

Privacy Act is applicable.

Comments:

FAIMIS is covered by System of Records Notice, NRC 32 Office of the Chief Financial Officer Financial Transactions and Debt Collection Management Records; HRMS and HRMSC is covered by NRC19, Official Personnel Training Records; NRC 21, Payroll Accounting Records and Government-Wide System of Records OPM/GOVT-1 General Personal Records.

Reviewer's Name	Title
 Signed by Hardy, Sally on 03/23/22	Privacy Officer

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION


No OMB clearance is needed.

OMB clearance is needed.

Currently has OMB Clearance. Clearance No. _____

Comments:


An OMB clearance is not needed as long as information will not be collected from former employees, job applicants, or new employees not yet onboarded?

Reviewer's Name	Title
 Signed by Cullison, David on 03/09/22	Agency Clearance Officer

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

- No record schedule required.
- Additional information is needed to complete assessment.
- Needs to be scheduled.
- Existing records retention and disposition schedule covers the system - no modifications needed.


Comments:

Reviewer's Name	Title
 Signed by Dove, Marna on 03/16/22	Sr. Program Analyst, Electronic Records Manager

D. BRANCH CHIEF REVIEW AND CONCURRENCE


- This IT system **does not** collect, maintain, or disseminate information in identifiable form from or about members of the public.
- This IT system **does** collect, maintain, or disseminate information in identifiable form from or about members of the public.

I concur in the Privacy Act, Information Collections, and Records Management reviews:


Signed by Nalabandian, Garo on 03/24/22

Chief
Cyber Security Branch
Governance and Enterprise Management
Services Division
Office of the Chief Information Officer

**TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS**

TO: Cherish Johnson, OCFO	
Name of System: Financial Management Systems (FMS)	
Date CSB received PIA for review: February 9, 2022	Date CSB completed PIA review: March 23, 2022
Noted Issues: 	
Chief Cyber Security Branch Governance and Enterprise Management Services Division Office of the Chief Information Officer	Signature/Date:  Signed by Nalabandian, Garo on 03/24/22
<i>Copies of this PIA will be provided to:</i> <i>Thomas G. Ashley, Jr.</i> <i>Director</i> <i>IT Services Development and Operations Division</i> <i>Office of the Chief Information Officer</i> <i>Garo Nalabandian, Acting</i> <i>Chief Information Security Officer (CISO)</i> <i>Office of the Chief Information Officer</i>	