

---

U.S. Nuclear Regulatory Commission

---



**Privacy Impact Assessment  
Financial Management Systems (FMS) -  
Financial Management Data Mart (FMDM)  
Office of the Chief Financial Officer (OCFO)**

**Version 1.0**

**7/13/2023**

Financial Management Systems (FMS) – Financial Management Data Mart (FMDM)	Version 1.0
Privacy Impact Assessment	7/13/2023

## Document Revision History

Date	Version	PIA Name/Description	Author
7/13/2023	1.0	FMS FMDM PIA Initial Release.	OCFO Oasis Systems, LLC
6/23/2023	DRAFT	FMS FMDM PIA Draft Release.	OCFO Oasis Systems, LLC

Financial Management Systems (FMS) – Financial Management Data Mart (FMDM)	Version 1.0
Privacy Impact Assessment	7/13/2023

## Table of Contents

1	Description	1
2	Authorities and Other Requirements	3
3	Characterization of the Information	4
4	Data Security	6
5	Privacy Act Determination	8
6	Records and Information Management-Retention and Disposal	9
7	Paperwork Reduction Act	11
8	Privacy Act Determination	13
9	OMB Clearance Determination	14
10	Records Retention and Disposal Schedule Determination	15
11	Branch Chief Review and Concurrence	16

Financial Management Systems (FMS) – Financial Management Data Mart (FMDM)	Version 1.0
Privacy Impact Assessment	7/13/2023

*The agency is subject to the requirements of the E-Government Act and is committed to identifying and addressing privacy risks whenever it develops or makes changes to its information systems. The questions below help determine any privacy risks related to the E-Government Act or later guidance by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST).*

**Name/System/Subsystem/Service Name:** Financial Management Systems (FMS) – Financial Management Data Mart (FMDM).

**Data Storage Location (i.e., Database Server, SharePoint, Cloud, Other Government Agency, Power Platform):** Database Server.

**Date Submitted for review/approval:** August 29, 2023.

## 1 Description

**1.1 Provide the description of the system/subsystem, technology (i.e., Microsoft Products), program, or other data collections (hereinafter referred to as “project”). Explain the reason the project is being created.**

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 and services that support mission and business functions that OCFO provides for the agency. FMDM is a service under FMS that serves as a centralized repository of integrated data from the NRC's financial management systems. Its primary purpose is to provide timely, accurate financial data from authoritative data sources for the purpose of reporting and data analytics. The FMDM also feeds data to the NRC Enterprise Data Warehouse.

Information in the FMDM contains employee name, ID, location, position, and position ID; as well as pay amounts (salary and benefits), hours charged, and time codes used. Only the Legacy PAYPERS database (DB) contains personally identifiable information (PII). The 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 Payroll Historical Database (PHDB) for historical purposes and later was migrated to the FMS Human Resources Management System (HRMS) subsystem. In 2021, the PAYPERS DB was moved to the servers repurposed for FMDM activities. The data originally stored in the PAYPERS DB has not been modified since the data was originally collected.

The FMDM environment currently consists of on-premises Windows components; however, FMDM is planning on migrating to the NRC OCIO Azure Cloud Services (ACS) tenant.

Financial Management Systems (FMS) – Financial Management Data Mart (FMDM)	Version 1.0
Privacy Impact Assessment	7/13/2023

Please mark appropriate response below if your project/system will involve the following:

<input checked="" type="checkbox"/> PowerApps	<input type="checkbox"/> Public Website
<input checked="" type="checkbox"/> Dashboard	<input type="checkbox"/> Internal Website
<input type="checkbox"/> SharePoint	<input type="checkbox"/> None
<input type="checkbox"/> Other:	

**1.2 Does this privacy impact assessment (PIA) support a proposed new project, proposed modification to an existing project, or other situation? Select options that best apply in table below.**

Mark appropriate response.

Status Options	
<input type="checkbox"/>	New system/project
<input type="checkbox"/>	Modification to an existing system/project. <i>If modifying or making other updates to an existing system/project, provide the ADAMS ML of the existing PIA and describe the modification.</i>
<input checked="" type="checkbox"/>	Annual Review <i>If making minor edits to an existing system/project, briefly describe the changes below.</i>
<input type="checkbox"/>	Other (explain)

**1.3 Points of Contact:**

	Project Manager	System Owner/Data Owner/Steward	ISSO	Business Project Manager	Technical Project Manager	Executive Sponsor
<b>Name</b>	Abby Olarte	Howard Osborne	John Howerton	Susan Hayden	Daniel Klein	Howard Osborne
<b>Office/Division /Branch</b>	OCFO/DOC/FSB	OCFO	OCFO/DOC/FSB	OCFO/DOC/FSB	OCFO	OCFO
<b>Telephone</b>	301-415-6288	N/A	301-415-8170	301-415-6206	N/A	N/A

Financial Management Systems (FMS) – Financial Management Data Mart (FMDM)	Version 1.0
Privacy Impact Assessment	7/13/2023

## 2 Authorities and Other Requirements

### 2.1 What specific legal authorities and/or agreements permit the collection of information for the project?

*Provide all statutory and regulatory authorities for operating the project, including the authority to collect the information; NRC internal policy is not a legal authority. Please mark appropriate response in table below.*

Mark with an "X" on all that apply.	Authority	Citation/Reference
<input checked="" type="checkbox"/>	<b>Statute</b>	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; and Public Law 104-193, "Personal Responsibility and Work Opportunity Reconciliation Act of 1996"
<input checked="" type="checkbox"/>	<b>Executive Order</b>	Executive Order (E.O.) 9397, "Numbering System for Federal Accounts Relating to Individual Persons" (Nov. 22, 1943)
<input type="checkbox"/>	<b>Federal Regulation</b>	
<input type="checkbox"/>	<b>Memorandum of Understanding/Agreement</b>	
<input type="checkbox"/>	<b>Other (summarize and provide a copy of relevant portion)</b>	

### 2.2 Explain how the information will be used under the authority listed above (i.e., *enroll employees in a subsidies program to provide subsidy payment*).

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

Information stored in the FMDM is used for future funding considerations and decisions, financial reporting, and Tableau dashboard reporting.

### **If the project collects Social Security numbers, state why this is necessary and how it will be used.**

The Legacy PAYPERS DB contains 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.

Financial Management Systems (FMS) – Financial Management Data Mart (FMDM)	Version 1.0
Privacy Impact Assessment	7/13/2023

### 3 Characterization of the Information

In the table below, mark the categories of individuals for whom information is collected.

Category of individual	
<input checked="" type="checkbox"/>	Federal employees
<input type="checkbox"/>	Contractors
<input type="checkbox"/>	Members of the Public (any individual other than a federal employee, consultant, or contractor)
<input type="checkbox"/>	Licensees
<input type="checkbox"/>	<b>Other:</b>

In the table below, is a list of the most common types of PII collected. Mark all PII that is collected and stored by the project/system. If there is additional PII not defined in the table below, a comprehensive listing of PII is provided for further reference in ADAMS at the following link: [PII Reference Table 2023](#).

Categories of Information			
<input checked="" type="checkbox"/>	Name	<input type="checkbox"/>	Resume or curriculum vitae
<input checked="" type="checkbox"/>	Date of Birth	<input type="checkbox"/>	Driver's License Number
<input type="checkbox"/>	Country of Birth	<input type="checkbox"/>	License Plate Number
<input type="checkbox"/>	Citizenship	<input type="checkbox"/>	Passport number
<input type="checkbox"/>	Nationality	<input type="checkbox"/>	Relatives Information
<input type="checkbox"/>	Race	<input type="checkbox"/>	Taxpayer Identification Number
<input checked="" type="checkbox"/>	Home Address	<input type="checkbox"/>	Credit/Debit Card Number
<input checked="" type="checkbox"/>	Social Security number (Truncated or Partial)	<input type="checkbox"/>	Medical/health information
<input type="checkbox"/>	Gender	<input type="checkbox"/>	Alien Registration Number
<input type="checkbox"/>	Ethnicity	<input type="checkbox"/>	Professional/personal references
<input type="checkbox"/>	Spouse Information	<input type="checkbox"/>	Criminal History
<input type="checkbox"/>	Personal e-mail address	<input type="checkbox"/>	Biometric identifiers (facial images, fingerprints, iris scans)
<input type="checkbox"/>	Personal Bank Account Number	<input type="checkbox"/>	Emergency contact (e.g., a third party to contact in case of an emergency)
<input type="checkbox"/>	Personal Mobile Number	<input type="checkbox"/>	Accommodation/disabilities information
<input type="checkbox"/>	Marital Status	<input type="checkbox"/>	<b>Other:</b>
<input type="checkbox"/>	Children Information		
<input type="checkbox"/>	Mother's Maiden Name		

Financial Management Systems (FMS) – Financial Management Data Mart (FMDM)	Version 1.0
Privacy Impact Assessment	7/13/2023

**3.1 Describe how the data is collected for the project. (i.e., NRC Form, survey, questionnaire, existing NRC files/databases, response to a background check).**

Data in the FMDM is not collected directly from the subject individual. Information is collected from existing NRC files/databases via direct connection (linked server, JDBC connections), or flat file:

- HCM Cloud for Time and Labor System (HCMTL) & Office of the Chief Human Capital Officer (OCHCO) / Federal Personnel Payroll System (FPPS) – Salary/benefit amounts, employee duty location, employee pay grade/step, position title, employee and position ID, hours worked, and time codes charged.
- Budget Formulation System (BFS) – Procurement spend planning, budget formulation, commitment planning.
- Financial Accounting and Integrated Management Information System (FAIMIS) – General financial information (commitments, obligations, expenditures).
- Strategic Acquisition System (STAQS) – Contract information (ceiling, period of performance, COR) used for procurement spend planning.
- Federal Planning and Architecture Support System (FEDPASS) – Transmission of pending IT changes between approvers and financial planners within BFS's commitment planning module.

As it relates to the data from the Legacy PAYPERS DB, data was transferred from the PAYPERS system to the PHDB in 2002, and from HRMS in 2021.

**3.2 If using a form to collect the information, provide the form number, title and/or a link.**

N/A.

**3.3 Who provides the information? Is it provided directly from the individual or a third party.**

Information in FMDM is not collected directly from subject individuals. Refer to section 3.1 regarding data sources (HCMTL, OCHCO/FPPS, BFS, FAIMIS, STAQS, FEDPASS, and Legacy PAYPERS DB).

**3.4 Explain how the accuracy of the data collection is validated. If the project does not check for accuracy, please explain why.**

Data is sourced from the respective systems of record at NRC. Data accuracy is verified by the respective systems in which the data is originally collected from the individual.

As it relates to the data from the 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.

**3.5 Will PII data be used in a test environment? If so, explain the rationale.**

No.



Financial Management Systems (FMS) – Financial Management Data Mart (FMDM)	Version 1.0
Privacy Impact Assessment	7/13/2023

**3.6 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?**

No data used or maintained by the FMDM is collected from the subject individual. All information maintained by the service is from data transfers from other systems/services, as discussed in section 3.1 (HCMTL, OCHCO/FPPS, BFS, FAIMIS, STAQS, FEDPASS, and Legacy PAYPERS DB). If the individual wants to correct inaccurate PII, they must correct the PII in the source system/service.

**4 Data Security**

**4.1 Describe who has access to the data in the project (i.e., internal NRC, system administrators, external agencies, contractors, public).**

Access to the server hosting the FMDM is restricted to OCFO administrators. However, data stored on the servers for the purpose of the FMDM is available to NRC personnel with roles and responsibilities related to budget planning and reporting who have requested access to the budget formulation data set. Request forms must be reviewed and approved by OCFO.

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

**4.2 If the project/system shares information with any other NRC systems, identify the system, what information is being shared and the method of sharing.**

Data in the FMDM is collected from existing NRC files/databases via direct connection (linked server, JDBC connections), or flat file:

- HCMTL provides general employee information, employee salaries, as well as benefits, payroll, time and attendance, and activity-based work hour data via flat file 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.
- FEDPASS provides a view of all transactions received and their processing status via SQL server link BFS CPM module.

Financial Management Systems (FMS) – Financial Management Data Mart (FMDM)	Version 1.0
Privacy Impact Assessment	7/13/2023

**4.3 If the project/system connects, receives, or shares information with any external non-NRC partners or systems, identify what is being shared.**

Identify what agreements are in place with the external non-NRC partner or system in the table below.

Agreement Type	
<input type="checkbox"/>	Contract Provide Contract Number:
<input type="checkbox"/>	License Provide License Information:
<input type="checkbox"/>	Memorandum of Understanding Provide ADAMS ML number for MOU:
<input type="checkbox"/>	Other:
<input checked="" type="checkbox"/>	None

**4.4 Describe how the data is accessed and describe the access control mechanisms that prevent misuse.**

Accounts for BFS administrators and FMDM users viewing budgeting data are restricted to NRC personnel with a LAN ID and a need-to-know. Accounts are integrated with the NRC Information Technology Infrastructure (ITI) Identity, Credential, and Access Management (ICAM) for Single Sign-On (SSO).

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

**4.5 Explain how the data is transmitted and how confidentiality is protected (i.e., encrypting the communication or by encrypting the information before it is transmitted).**

Data in the FMDM is collected from existing NRC files/databases via direct connection (linked server, JDBC connections), or flat file, as discussed above in section 4.2. Communications are encrypted and transmitted within the NRC firewall.

**4.6 Describe where the data is being stored (i.e., NRC, Cloud, Contractor Site).**

Data is being stored on servers located at NRC HQ. FMDM is planning to migrate to the cloud in the NRC ACS tenant.

**4.7 Explain if the project can be accessed or operated at more than one location.**

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

**4.8 Can the project be accessed by a contractor? If so, do they possess an NRC badge?**

Yes, all contractors supporting FMDM are, at minimum, NRC IT-I cleared, possessing NRC badges.

Financial Management Systems (FMS) – Financial Management Data Mart (FMDM)	Version 1.0
Privacy Impact Assessment	7/13/2023

**4.9 Explain the auditing measures and technical safeguards in place to prevent misuse of data.**

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

**4.10 Describe if the project has the capability to identify, locate, and monitor (i.e., trace/track/observe) individuals.**

N/A.

**4.11 Define which FISMA boundary this project is part of.**

FMDM operates as a service under the FMS FISMA boundary.

**4.12 Is there an Authority to Operate (ATO) associated with this project/system?**

Authorization Status	
<input type="checkbox"/>	Unknown
<input type="checkbox"/>	No <i>If no, please note that the authorization status must be reported to the Chief Information Security Officer (CISO) and Computer Security Organization (CSO's) Point of Contact (POC) via e-mail quarterly to ensure the authorization remains on track.</i>
<input type="checkbox"/>	In Progress provide the estimated date to receive an ATO. Estimated date:
<input checked="" type="checkbox"/>	Yes Indicate the data impact levels (Low, Moderate, High, Undefined) approved by the Chief Information Security Officer (CISO) Confidentiality – Moderate Integrity – Moderate Availability – Moderate

**4.13 Provide the NRC system Enterprise Architecture (EA)/Inventory number. If unknown, contact [EA Service Desk](#) to get the EA/Inventory number.**

EA Number: 20190012.

## 5 Privacy Act Determination

**5.1 Is the data collected retrieved by a personal identifier?**

Mark the appropriate response.

Response	
<input checked="" type="checkbox"/>	<b>Yes, the PII is retrieved by a personal identifier (i.e., individual's name, address, SSN, etc.)</b>
<input checked="" type="checkbox"/>	<b>List the identifiers that will be used to retrieve the information on the individual.</b> Users will not typically view data in this manner, but employee name/ID can be used to pull data for a specific individual.
<input type="checkbox"/>	<b>No, the PII is not retrieved by a personal identifier.</b> <b>If no, explain how the data is retrieved from the project.</b>

Financial Management Systems (FMS) – Financial Management Data Mart (FMDM)	Version 1.0
Privacy Impact Assessment	7/13/2023

**5.2 For all collections where the information is retrieved by a personal identifier, the Privacy Act requires that the agency publish a System of Record Notice (SORN) in the Federal Register.** *As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some other personal identifier assigned to the individual.*

Mark the appropriate response in the table below.

Response	
<input checked="" type="checkbox"/>	<b>Yes, this system is covered by an existing SORN. (See existing SORNs: <a href="https://www.nrc.gov/reading-rm/foia/privacy-systems.html">https://www.nrc.gov/reading-rm/foia/privacy-systems.html</a>)</b> <b>Provide the SORN name, number, (List all SORNs that apply):</b> Legacy PAYPERS DB – NRC-21, “Payroll Accounting Records”
<input type="checkbox"/>	<b>SORN is in progress</b>
<input type="checkbox"/>	<b>SORN needs to be created</b>
<input type="checkbox"/>	<b>Unaware of an existing SORN</b>
<input type="checkbox"/>	<b>No, this system is not a system of records and a SORN is not applicable</b>

**5.3 When an individual is asked to provide personal data (i.e., form, webpage, survey), is a Privacy Act Statement (PAS) provided?** *A Privacy Act Statement is a disclosure statement required to appear on documents used by agencies when an individual is asked to provide personal data. It is required for any forms, surveys, or other documents, including electronic forms, used to solicit personal information from individuals that will be maintained in a system of records.*

Mark the appropriate response.

Options	
<input type="checkbox"/>	<b>Privacy Act Statement:</b>
<input checked="" type="checkbox"/>	<b>Not Applicable</b>
<input type="checkbox"/>	<b>Unknown</b>

**5.4 Is providing the PII mandatory or voluntary? What is the effect on the individual by not providing the information?**

FMDM does not collect PII directly from the subject individuals, it is the responsibility of the source system/service to inform individuals whether or not PII disclosure is mandatory or voluntary.

## 6 Records and Information Management-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

Financial Management Systems (FMS) – Financial Management Data Mart (FMDM)	Version 1.0
Privacy Impact Assessment	7/13/2023

significance). Records/data and information with historical value, identified as having a “permanent” disposition, are transferred to the National Archives of the United States at the end of their retention period. All other records identified as having a “temporary” disposition are destroyed at the end of their retention period in accordance with the NARA Records Schedule or the General Records Schedule.

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, agencies are required to establish procedures for addressing Records and Information Management (RIM) requirements. This includes strategies for establishing and managing recordkeeping requirements and disposition instructions before approving new electronic information systems or enhancements to existing systems.

The following questions are intended to determine whether the records/data and information in the system have approved records retention schedules and disposition instructions, whether the system incorporates RIM strategies including support for [NARA’s Universal Electronic Records Management \(ERM\) requirements](#), and if a mitigation strategy is needed to ensure compliance.

**If the project/system:**

- Does not have an approved records retention schedule and/or
- Does not have an *automated* RIM functionality,
- Involves a cloud solution,
- And/or if there are additional questions regarding Records and Information Management - Retention and Disposal, please contact the NRC Records staff at [ITIMPolicy.Resource@nrc.gov](mailto:ITIMPolicy.Resource@nrc.gov) for further guidance.

**If the project/system has a record retention schedule or an automated RIM functionality, please complete the questions below.**

**6.1 Does this project map to an applicable retention schedule in NRC’s Comprehensive Records Disposition Schedule (NUREG-0910), or NARA’s General Records Schedules?**

<input type="checkbox"/>	<a href="#">NUREG-0910, “NRC Comprehensive Records Disposition Schedule”</a>
<input type="checkbox"/>	<a href="#">NARA’s General Records Schedules</a>
<input checked="" type="checkbox"/>	Unscheduled

**6.2 If so, cite the schedule number, approved disposition, and describe how this is accomplished.**

<b>System Name (include sub-systems, platforms, or other locations where the same data resides)</b>	N/A – 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.
<b>Records Retention Schedule Number(s)</b>	<b>FMDM is Unscheduled; <i>suggested disposition instruction for records in Masterfile:</i></b> <b><i>Temporary. Delete data when superseded by next scheduled update or when system is discontinued or obsolete.</i></b>  Additional information/data/records kept in this

Financial Management Systems (FMS) – Financial Management Data Mart (FMDM)	Version 1.0
Privacy Impact Assessment	7/13/2023

	system may need to be scheduled; therefore, NRC records personnel will need to work with staff to develop a records retention and disposition schedule for records/data created or maintained. Until the approval of such schedule, these records and information are Permanent. Their willful disposal or concealment (and related offenses) is punishable by fine or imprisonment, according to 18 U.S.C., Chapter 101, and Section 2071. Implementation of retention schedules is mandatory under 44 U.S. 3303a (d), and although this does not prevent further development of the project, retention functionality or a manual process must be incorporated to meet this requirement.
<b>Approved Disposition Instructions</b>	N/A
Is there a current automated functionality or a manual process to support RIM requirements? This includes the ability to apply records retention and disposition policies in the system(s) to support records accessibility, reliability, integrity, and disposition.	N/A
<b>Disposition of Temporary Records</b> Will the records/data or a composite be automatically or manually deleted once they reach their approved retention?	N/A
<b>Disposition of Permanent Records</b> Will the records be exported to an approved format and transferred to the National Archives based on approved retention and disposition instructions? If so, what formats will be used? <a href="#">NRC Transfer Guidance (Information and Records Management Guideline - IRMG)</a>	N/A

## 7 Paperwork Reduction Act

The Paperwork Reduction Act (PRA) of 1995 requires that agencies obtain an Office of Management and Budget (OMB) approval in the form of a "control number"—before promulgating a paper form, website, surveys, questionnaires, or electronic submission from 10 or members of the public. If the data collection is from federal employees regarding work-related duties, then a PRA clearance is not necessary.

### 7.1 Will the project be collecting any information from 10 or more persons who are not Federal employees?

No.

Financial Management Systems (FMS) – Financial Management Data Mart (FMDM)	Version 1.0
Privacy Impact Assessment	7/13/2023

**7.2 Is there any collection of information addressed to all or a substantial majority of an industry (i.e., Fuel Fabrication Facilities or Fuel Cycle Facilities)?**

No.

**7.3 Is the collection of information required by a rule of general applicability?**

No.

*Note: For information collection (OMB clearances) questions: contact the NRC's Clearance Officer. Additional guidance can be found on the NRC's internal Information Collections Web page at: <https://intranet.nrc.gov/ocio/33456>.*

Financial Management Systems (FMS) – Financial Management Data Mart (FMDM)	Version 1.0
Privacy Impact Assessment	7/13/2023

## 8 Privacy Act Determination

**Project/System Name:** Financial Management Systems (FMS) – Financial Management Data Mart (FMDM).

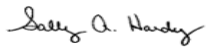
**Submitting Office:** Office of the Chief Financial Officer (OCFO).

### Privacy Officer Review

Review Results		Action Items
<input type="checkbox"/>	This project/system <b>does not contain PII.</b>	<b>No further action</b> is necessary for Privacy.
<input type="checkbox"/>	This project/system <b>does contain PII</b> ; the Privacy Act does <b>NOT</b> apply, since information is NOT retrieved by a personal identifier.	<b>Must be protected with restricted access</b> to those with a valid need-to-know.
<input checked="" type="checkbox"/>	This project/system <b>does contain PII</b> ; the <b>Privacy Act does apply.</b>	<b>SORN is required-</b> Information is <b>retrieved</b> by a personal identifier.

**Comments:**

FMS-FMDM - FAIMIS is covered by System of Records Notice, NRC 32 Office of the Chief Financial Officer Financial Transactions and Debt Collection Management Records; HRMS / HRMSC is covered by NRC 19, 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 09/06/23	Privacy Officer



Financial Management Systems (FMS) – Financial Management Data Mart (FMDM)	Version 1.0
Privacy Impact Assessment	7/13/2023


## 9 OMB Clearance Determination

### NRC Clearance Officer Review

Review Results	
<input checked="" type="checkbox"/>	No OMB clearance is needed.
<input type="checkbox"/>	OMB clearance is needed.
<input type="checkbox"/>	Currently has OMB Clearance. Clearance No. _____

**Comments:**

FMS-FMDM does not collect information directly from individuals or organizations and is not subject to the requirements of the Paperwork Reduction Act.

Reviewer's Name	Title
 Signed by Cullison, David on 08/25/23	Agency Clearance Officer


Financial Management Systems (FMS) – Financial Management Data Mart (FMDM)	Version 1.0
Privacy Impact Assessment	7/13/2023

## 10 Records Retention and Disposal Schedule Determination Records Information Management Review

Review Results	
<input type="checkbox"/>	No record schedule required.
<input type="checkbox"/>	Additional information is needed to complete assessment.
<input checked="" type="checkbox"/>	Needs to be scheduled.
<input type="checkbox"/>	Existing records retention and disposition schedule covers the system - no modifications needed.

**Comments:**

The system is **Unscheduled**. Additional information/data/records kept in this system may need to be scheduled; therefore, NRC records personnel will need to work with staff to develop a records retention and disposition schedule for records created or maintained. Until the approval of such schedule, these records and information are **Permanent**. Their willful disposal or concealment (and related offenses) is punishable by fine or imprisonment, according to 18 U.S.C., Chapter 101, and Section 2071. Implementation of retention schedules is mandatory under 44 U.S. 3303a (d), and although this does not prevent further development of the project, retention functionality or a manual process must be incorporated to meet this requirement.

Reviewer's Name	Title
 Signed by Dove, Marna on 09/05/23	Sr. Program Analyst, Electronic Records Manager

Financial Management Systems (FMS) – Financial Management Data Mart (FMDM)	Version 1.0
Privacy Impact Assessment	7/13/2023

## 11 Branch Chief Review and Concurrence

Review Results	
<input type="checkbox"/>	This project/system <b>does not</b> collect, maintain, or disseminate information in identifiable form.
<input checked="" type="checkbox"/>	This project/system <b>does</b> collect, maintain, or disseminate information in identifiable form.
<input checked="" type="checkbox"/>	I concur with the Privacy Act, Information Collections, and Records Management reviews.



Signed by Harris, Kathryn  
on 09/19/23

---

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

Financial Management Systems (FMS) – Financial Management Data Mart (FMDM)	Version 1.0
Privacy Impact Assessment	7/13/2023

## ADDITIONAL ACTION ITEMS/CONCERNS

<b>Name of Project/System:</b>	
Financial Management System (FMS) – Financial Management Data Mart (FMDM)	
<b>Date CSB received PIA for review:</b>	<b>Date CSB completed PIA review:</b>
August 29, 2023	September 5, 2023
<b>Action Items/Concerns:</b>	
<p><i>Copies of this PIA will be provided to:</i></p> <p><i>Ledetria Beaudoin</i>  <i>Acting Director</i>  <i>IT Services Development and Operations Division</i>  <i>Office of the Chief Information Officer</i></p> <p><i>Garo Nalabandian</i>  <i>Chief Information Security Officer (CISO)</i>  <i>Office of the Chief Information Officer</i></p>	