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.

Master Data Management Services (MDMS) System

Date: October 26, 2020

A. GENERAL SYSTEM INFORMATION

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

The U.S. Nuclear Regulatory Commission (NRC) has established the Master Data Management Services (MDMS) system to address both short and long-term enterprise data management needs. The MDMS is a major agency-wide initiative to support the processes and decisions of NRC through:

- Improving data quality
- Improving re-use and exchange of information
- Reducing or eliminating the storage of duplicate information
- Providing an enterprise-wide foundation for information sharing
- Establishing a data governance structure

The MDMS provides an overall vision for, and leadership focused on, an enterprise solution that establishes authoritative data owners, delivers quality data in an efficient manner to the systems that require it, and effectively meets business needs. The MDMS is also focused on data architecture and includes projects that will identify and define data elements across the agency.

The MDMS system is a web-based application accessible to representatives from every NRC office—that provides standardized and validated dockets and data records that support dockets, including licenses, contact and billing information, to all downstream NRC systems that require that data. The NRC collects digital identification data for individuals to support the agency core business operations, issue credentials, and administer access to agency‘s physical and logical resources. To support this need, the MDMS system also serves as a centralized repository for the accessibility of organization and personnel data.

MDMS resides on the Business Application Support System (BASS) General Support System (Enterprise Architecture (EA) #: 20070047)) operated by the Office of the Chief Information Officer (OCIO). In general, the support services provided to the MDMS by BASS for operations and compliance with relevant security controls is the same for other applications in the BASS environment.

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

The MDMS system is the authoritative source for dockets, docket contact and docket licensee information. MDMS receives dockets information created under 10 *Code of Federal Regulations* (CFR) Parts 30, 40, 70, 71, 72, 110 and 150 from the Web Based Licensing (WBL) system on a nightly basis. The MDMS is also the source of creation for all new power reactor (050, 052) and vendor / non-vendor (999) dockets.

In addition, MDMS passes Employee and Organization data received from Enterprise Information Hub (EIH) and Federal Personnel/Payroll System (FPPS), respectively, to subscriber systems.

MDMS data is provided to the following subscriber systems:

- Replacement Reactor Program System (R-RPS)
- Enforcement Action Tracking System (EATS)
- Allegation Management System (AMS)
- Case Management System (CMS)
- Agency-wide Documents Access and Management Systems (ADAMS)
- Cost Activity Code System (CACS)
- Financial Accounting and Integrated Management Information System (FAIMIS)
- Public Meeting Notice System (PMNS)
- System of Ticketing and Reporting (STAR)
- Enterprise Project Management (EPM)
- Operator Digitized Dockets (ODD)
- Federal IT Portfolio Management System (FEDPASS)

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

N/A.

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.*)

The collection of billing data is required in order to recover fees in accordance with OBRA-90. 10 CFR 15 Debt Collection Procedures touches on billing data.

For the collection and maintenance of Tax Identification Number (TIN) (Employee Identification Number or Social Security Number (SSN) data in MDMS: The Debt Collection Improvement Act 1996 (Public Law 104-134) "The head of each Federal agency shall require each person doing business with that agency to furnish to that agency such person's taxpayer identifying number".

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

MDMS is used by representatives from every NRC office to access—and with specific permissions to generate—standardized and validated dockets and data records that support dockets, including licensee and facility information. MDMS has been modified to also store the TIN of docket licensees as part of the billing information.

In addition, MDMS also stores the employee/contractor data from the agency's EIH system and organization data from FPPS and provides the same source data downstream to multiple NRC information systems to support their business functions.

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.*)

Program Manager	**Office/Division/Branch**	**Telephone**
Melissa Ash	OCIO/ITSDOD/ADSB	301-415-7251
Project Manager	**Office/Division/Branch**	**Telephone**
Sandra Valencia	OCIO/GEMSD/APIB	301-415-8701
Business Project Manager	**Office/Division/Branch**	**Telephone**
N/A	N/A	N/A
Technical Project Manager	**Office/Division/Branch**	**Telephone**
Jun Lee	OCIO/GEMSD/APIB	301-415-1337

Executive Sponsor	**Office/Division/Branch**	**Telephone**
John Moses	OCIO/GEMSD	301-415-1276
ISSO	**Office/Division/Branch**	**Telephone**
N/A	N/A	N/A
System Owner/User	**Office/Division/Branch**	**Telephone**
N/A	N/A	N/A

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

a. ____ New System

__X__ Modify Existing System

____ Other

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

Yes.

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

April 16, 2019, Main Library ML19121A465.

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

The following areas of MDMS were implemented as part of the redesign efforts on October 31, 2019:

1. Data-driven architecture improves system performance and maintainability
2. Localized user permissions streamline visibility, accountability, and management of user permissions
3. User-focused design improves system usability and data quality
4. Clearly identifiable data available for subscribing systems identifies the data source and purpose to ensure data integrity
5. Modern and backfit interface options are available for subscribing systems

The MDMS application is in the Operations and Maintenance (O&M) phase with a quarterly release maintenance cycle. The O&M phase include routine maintenance or enhancements such as routine patching, service packs related upgrades, and implementing change requests to support agency's Master Data Management program functions.

Please note that no changes have been made to the MDMS application recently that effect or create new privacy risks.

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

Yes.

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

20160006.

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.)).

Individuals may be Federal employees, Federal contractors or commercial vendors who are NRC's licensees.

(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)?

NRC Employees / Contractor Data:
The MDMS system contains data for both current and past individual NRC employees and contractors supplied through an interface with EIH. The Employee entity has the following fields: Code (10 character unique ID for each digital identity), Name, LAN ID, Email ID, First Name, Middle Name, Last Name, Name Suffix, Status (Active or Inactive), Affiliation (Employee or Contractor), Position, Employee ID, Effective Date, Termination Date and Organization, Region Name, Building, Floor, Location, Entry on Duty Date. This data is not modifiable in MDMS; any changes made to the data are applied at the source and pushed to MDMS daily. An amalgam of the employee First Name and Last Name is used as the Name for each record in the Employee entity. These Name values are utilized in MDMS to establish points-of-contact for Dockets. Docket contacts are individual records (hereafter "Contact records") created in MDMS and linked to one or more dockets. Contact records connect the Name value with email, phone and physical address information for that individual. This data is entered and maintained by MDMS users with specific permissions. Contact records are not currently utilized outside of MDMS and are not passed to subscriber systems. Employee data in MDMS is not linked to TINs or other licensee data.

NRC Employees' Organization Data:
The MDMS system contains NRC employees' organization data supplied from FPPS system via CSV file. The Organization data has the following fields - Code, Organization Name, Organization Abbreviation, Level 1 Abbreviation (Office), Level 2 Abbreviation (Division), Level 3 Abbreviation (Branch), Level 4 Abbreviation (Team), Active (Organization status).

Licensees:
Required fields are Name (of license holder entity, which could be an individual), Legal Contact Name (person representing license holder entity), and the Street Address, City, could be a State (if U.S.), Country and Zip of that legal contact. Optional information: legal contact phone and email address. The license holder entity will now be required to also provide the TIN associated with the entity. In the case of some small businesses this TIN may actually be the SSN of the business owner who is likely named as the legal contact.

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

No, MDMS does not collect the information directly from the individuals. Employee data is being passed to MDMS system from the EIH.

For the 030, 040, 070, 071, 110 and 150 dockets, the licensee information is being passed to the MDMS system from WBL or is being added/maintained by NRC employees with specific user roles in MDMS that are restricted to data relevant to their NRC office.

A business applying for a license (050 / 052 (power reactors) and 999 (vendor and non-vendor dockets), submits an application to NRC that includes the information name of an applicant, business telephone number, business cell phone number, business email address and address where licensed material will be used or possessed. In MDMS, TINs/SSNs may only be viewed, added and modified by users with appropriate roles and permissions.

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

N/A.

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

Yes.

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

Yes.

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

OMB clearance No. 3150-0188 provides authority to the NRC, specifically the Office of the Chief Financial Officer (OCFO) for NRC Form 531 "Request for Taxpayer Identification Number".

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

Yes and no.

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

MDMS receives NRC employee and contractor data (personal/work contact and location information) from EIH via database connection.

MDMS receives NRC employees' organization information from FPPS via CSV file in the shared drop box.

The Office of Nuclear Material Safety and Safeguards (NMSS) WBL application is the authoritative source for material dockets (30, 40, 70, 71, 72, 110, 150) as well as sealed source devices and general licenses. MDMS receives updated docket and corresponding license information from WBL on a nightly basis via flat file.

See detailed description in section B.1.b.

For all other dockets that existed prior to MDMS becoming the authoritative source for such information, docket licensee data was imported from the Legacy (L)-RPS system. New docket licensee data is now entered directly into MDMS. OCFO already maintained some TINs in FAIMIS, collected using NRC Form 531. As a first step regarding the inclusion of TINs in MDMS, FAIMIS (in a one-time transfer) provided to MDMS those TINs that were already on-hand. Thereafter, any new applicants or licensees applying for an amendment, who have not yet provided their TINs to NRC, will provide that information using NRC Form 531 and OCFO staff with the specific MDMS user role of OCFO Contributor will input the TIN in MDMS. MDMS will then transfer the TINs and other licensee data to FAIMIS on a nightly basis along with the data being passed from WBL.

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

Yes – Current license holders and applicants.

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

Licensee applicants must submit an application (via NRC Form 313), which includes the business information of the licensee as well as contact information for the licensee representative.

Applicants are also required to submit the TIN and billing information using NRC Form 531.

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

This information is verified during the business process of reviewing licensee applications, which is conducted by NMSS and Regions I, III, & IV for all materials dockets coming from WBL, by the Office of Nuclear Reactor Regulation (NRR) for 050 docket information, and by the Office of New Reactors for 052 and 999 docket information. OCFO is responsible for the accuracy of the TIN and other billing information for all dockets.

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

Licensees and applicants can send the information via the license application paper form (NRC Form 313).

2. INFORMATION NOT ABOUT INDIVIDUALS

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

Yes.

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

Licensee information: License holder entity name (if not an individual), type of docket licensee (applicant, certificate holder or licensee), legal contact address and phone number (if not associated with an individual), TIN and billing address (if not associated with an individual), From and To dates of the license holder entity's relationship with the docket;

License Information: License number, operational phase covered by the license, From and To dates that the license is in effect;

Docket information: Docket Name, Docket Number, 10 CFR Part Number, Docket Type, Docket Category, Owner Office, Operational Phase (of docket), Region, Active or Historical status (of docket);

Organization Data: Levels 1-5 Abbreviation & Description fields, Active, Effective Date, Organization Name, Organization Abbreviation. Organization data is used to direct Enterprise Project Identifier requests to appropriate approvers. It is not associated with TINs or Licensee data.

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

The licensee information comes from the license application (NRC Form 313), the TIN paper form (NRC Form 531), and from NRC (reviewers in each Region and Headquarters).

Organization data is transmitted to MDMS from FPPS.

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.

The purpose of MDMS system is to standardize and validate docket and license information so that all recipient systems downstream of MDMS get uniform, accurate and complete data for fee billing, time accounting, record keeping, reporting, etc. The information related to fee billing is used by OCFO for issuing invoices, refunds, and collections. The TINs and all other fee billing related information are routinely passed to FAIMIS for fee billing purposes.

MDMS also provides NRC's employees and contractors (personal/work contact and location information) and employees' organization data it receives from EIH and FPPS to its subscriber systems R-RPS and FEDPASS via Application Programming Interface (API) / webservices, and to CACS, EATS, AMS, CMS, ODD, EPM, and STAR systems via database connection.

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

Yes.

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

Staff in the offices of NRR, NMSS, OCFO and OCIO.

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

Yes.

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

MDMS Data Inputs and Outputs and MDMS Data Mapping documents are located under Enterprise Data Management System (EDMS) System Data Folder and the MDMS designs are located in the EDMS Diagrams folder.

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

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?

N/A.

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

N/A.

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

N/A.

5. 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.)

Within the Application
An application user can access NRC's Employees, Organization, Docket, and Licensee information in the MDMS application via search queries or by paging through the summary/listing screens for each entity. Search results and entity summary/listing pages in MDMS may be exported into a CSV file. TIN data for Licensees may be accessed and viewed only by MDMS application users with the TIN Administrator role. Users with this role may also modify the data if the source system is MDMS.

Via Interface with MDMS
NRC systems that receive docket, licensee, employee, and related data from MDMS do so either via an API Webservice connection or through scheduled data retrievals from the Master Data Management (MDM) database.

The API Webservice connection allows read access to EDMS authenticated users, and the ability to modify data if 1) The user has an appropriate role that allows them to edit the data and the source system is MDM, or 2) The user owns the source system for that data. Any interface with the MDM database will have access controls implemented at the database level.

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

See details above in C.6.

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

Yes.

a. If "Yes," provide name of SORN and location in the Federal Register.

NRC 32 Office of the Chief Financial Officer Financial Transactions and Debt Collection Management Records.

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

N/A.

8. 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.

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

There are no reports produced directly from/by the MDMS system. Any reports utilizing data received from MDMS are produced from interfacing systems and are solely controlled by those systems.

a. What are the reports used for?

N/A.

b. Who has access to these reports?

N/A.

D. ACCESS TO DATA

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

NRR, NMSS, OCIO, OCFO, Office of Nuclear Security and Incident Response, and Office of the Chief Human Capital Officer (OCHCO).

(1) For what purpose?

- To create, modify and view Contacts and Contacts information
- specific to Reactor, Vendor and non-Vendor Dockets
- To create, modify and view Dockets, Docket Licensees information associated with Reactor, Vendor and non-Vendor dockets
- To create, modify and view TIN data for Docket and Vendor Docket Licensees
- To view 030, 040, 070, 071, 110 and 150 dockets and the licensee information
- To view organization and NRC's personnel data

(2) Will access be limited?

Yes, the MDMS system access will be limited based on the roles and responsibilities with need to know 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).

MDMS will receive data from the following systems –

WBL, EIH and FPPS.

The following systems will receive data from the MDMS system –

- R-RPS
- EATS
- AMS
- CMS
- ADAMS
- CACS
- FAIMIS
- PMNS
- STAR
- EPM
- ODD
- FEDPASS

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

Disclosure of Data within the Application
An application user can access NRC's Employees, Organization, Docket, and Licensee information in the MDMS application via search queries or by paging through the summary/listing screens for each entity. Search results and entity summary/listing pages in MDMS may be exported into a CSV file. TIN data for Licensees may be accessed and viewed only by MDMS application users with an appropriate application role. Users with that role may also modify data if the source system is MDMS.

Transmission of Data via Interface with MDMS
NRC systems that receive docket, licensee, employee, and related data from MDMS do so either via an API Webservice connection or through scheduled data retrievals from the MDM database.

The API Webservice connection allows read access to MDMS authenticated users, and the ability to modify data if 1) The user has an appropriate role that allows them to edit the data and the source system is MDMS, or 2) The user owns the source system for that data. Any interface with the MDMS database will have access controls implemented at the database level.

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

No.

(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)?

Yes. See table in section a.

However, further assessment is needed to ensure all data is represented according to NARA policies; therefore, NRC records personnel will need to work with staff to develop a records retention and disposition schedule for records and 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.

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?**

MDMS Operations and Maintenance (O&M) Records	GRS 3.1 item 020	Temporary. Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use.

Financial Data / Contract Data	GRS 1.1 item 011 All other copies (for administrative or reference purposes)	Temporary. Destroy when business use ceases.
Financial Data / Contract Data	GRS 1.1 item 010 Official record held in the office of record	Temporary. Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use.
Docket 030 Byproduct Licensing	NUREG 0910 2.17 item 6.b	Permanent. Cut off upon license or certification termination following completion of decommissioning procedure. Transfer to NARA 20 years after termination.
Docket 040 Source Material Licensing	NUREG 0910 2.17 item 6.b	Permanent. Cut off upon license or certification termination following completion of decommissioning procedure. Transfer to NARA 20 years after termination.
Docket 070 Special Nuclear Material Licensing	NUREG 0910 2.17 item 6.b	Permanent. Cut off upon license or certification termination following completion of decommissioning procedure. Transfer to NARA 20 years after termination.
Docket 071 Packaging and transportation of Radioactive Material	NUREG 0910 2.17 item 6.b	Permanent. Cut off upon license or certification termination following completion of decommissioning procedure. Transfer to NARA 20 years after termination.
Docket 110 Export and Import Licensing	NUREG 0910 2.15 item 4.a	Permanent. Cut off files upon license termination. Transfer to NARA 10 years license termination.
Docket 150 Exemptions and regulatory authority in Agreement States	NUREG 0910 2.17 item 6.a	Transfer to Agreement States
Docket 050 Production and Utilization Facilities Licensing	NUREG 0910 2.17 item 6.b	Permanent. Cut off upon license or certification termination following completion of decommissioning procedure. Transfer to NARA 20 years after termination.
Docket 052 Nuclear Power Plant Licensing	NUREG 0910 2.17 item 6.b	Permanent. Cut off upon license or certification termination following completion of decommissioning procedure. Transfer to NARA 20 years after termination.
Docket 999 Vendor/Nonvendor Dockets	NUREG 0910 2.20 item 20.a	Temporary. Cut off files at close of fiscal year. Destroy 60 years after cutoff.

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).

Roles are managed within the MDMS application by users with the Administrator (Admin) role.

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

The MDMS administrators in communication with NRC offices supply individuals with appropriate roles that control view and modification permissions.

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

There are three roles within EDMS (front-end), each of which grants a specific set of permissions and functionality execution within the application. A user may be assigned multiple roles, and they are as follows:

- **Administrator**: Grants a user access to all functions within the application.
- **Data Steward**: Ability to create/edit/modify Docket and Licensee data within the application.
- **TIN Administrator**: Ability to view tax identification number data within the user interface.

The EDMS System Administrators (back-end/infrastructure) roles and responsibilities are documented in the BASS Operations Guide.

(1) If yes, where?

The MDMS users access controls, procedures and responsibilities are documented in the MDMS Technical Operations Guide (application (non-privileged) users)) and BASS Operations Guide (system administrators/privileged users).

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

Yes, access is through a web browser.

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

N/A.

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

See Section D.1.

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

Yes, in system logs.

a. If yes, what will be collected?

LAN ID and date/time stamp.

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

Yes.

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?

All access to the MDMS system is captured in system log files and audit records.

Auditing - Every modification to specified database tables are logged.
Safeguards – Access is controlled via system administrators, and access changes are logged.

The security controls recommended by NIST 800-53 Rev 4 will be implemented based on the MDMS system categorization to prevent misuse of data. The MDMS is residing under the BASS boundary, so the BASS infrastructure support team may use the Splunk tool for auditing purposes.

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?

June 26, 2020.

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

System Name: Master Data Management Services (MDMS) System

Submitting Office: Office of the Chief Information Officer (OCIO)

A. PRIVACY ACT APPLICABILITY REVIEW

____ Privacy Act is not applicable.

__X__ Privacy Act is applicable.

Comments:

Since collecting TINs (which could occasionally be Social Security Number (SSN)) and SSNs are considered PII information this system would be considered a Privacy Act System of Records. This system would be covered by NRC 32 Office of the Chief Financial Officer Financial Transactions and Debt Collection Management Records.

Reviewer's Name	Title
Signed by Hardy, Sally on 11/13/20	Privacy Officer

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

____ No OMB clearance is needed.

____ OMB clearance is needed.

__X__ Currently has OMB Clearance. Clearance No. 3150-0120 (NRC Form 313) and 3150-0188 (NRC Form 531)

Comments:

MDMS does not need an OMB clearance as it does not directly collect any information. If this changes then the need for a clearance will be revisited.

Reviewer's Name	Title
Signed by Cullison, David on 11/13/20	Agency Clearance Officer

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

____ No record schedule required.

__X__ Additional information is needed to complete assessment.

____ Needs to be scheduled.

____ Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:

Further assessment is needed to ensure all data is represented according to NARA policies; therefore, NRC records personnel will need to work with staff to develop a records retention and disposition schedule for records and 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.

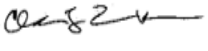
Reviewer's Name	Title
Signed by Dove, Marna on 11/13/20	Sr. Program Analyst, Electronic Records Manager

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.

__X__ 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 Brown, Cris
on 11/27/20

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: Thomas G. Ashley, Jr., ITSDOD Director, Office of the Chief Information Officer (OCIO)	
Name of System: Master Data Management Services (MDMS) System	
Date CSB received PIA for review: October 26, 2020	**Date CSB completed PIA review:** November 13, 2020
Noted Issues:	
Chief Cyber Security Branch Governance and Enterprise Management Services Division Office of the Chief Information Officer	Signature/Date: Signed by Brown, Cris on 11/27/20
Copies of this PIA will be provided to: *Thomas G. Ashley, Jr.* *Director* *IT Services Development and Operations Division* *Office of the Chief Information Officer* *Jonathan R. Feibus* *Chief Information Security Officer (CISO)* *Office of the Chief Information Officer*	