
U.S. Nuclear Regulatory Commission



Privacy Impact Assessment Case Management System Web (CMS-W) Subsystem of Business Application Support System (BASS)

Office of the Chief Information Officer (OCIO)

Version 1.0

08/30/2023

Instruction Notes:

Please do not enter the PIA document into ADAMS. An ADAMS accession number will be assigned through the e-Concurrence system which will be handled by the Privacy Team

Template Version 2.0 (03/2023)

Case Management System Web (CMS-W)	Version 1.0
Privacy Impact Assessment	08/30/2023

Document Revision History

Date	Version	PIA Name/Description	Author
08/30/2023	1.0	Case Management System Web (CMS-W) - Initial Release	OCIO Oasis Systems, LLC
08/10/2023	DRAFT	Case Management System Web (CMS-W) - Draft Release	OCIO Oasis Systems, LLC

Case Management System Web (CMS-W)	Version 1.0
Privacy Impact Assessment	08/30/2023

Table of Contents

1	Description	1
2	Authorities and Other Requirements	2
3	Characterization of the Information	3
4	Data Security	5
5	Privacy Act Determination	7
6	Records and Information Management-Retention and Disposal	8
7	Paperwork Reduction Act	14
8	Privacy Act Determination	17
9	OMB Clearance Determination	18
10	Records Retention and Disposal Schedule Determination	19
11	Branch Chief Review and Concurrence	20

Case Management System Web (CMS-W)	Version 1.0
Privacy Impact Assessment	08/30/2023

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: Case Management System Web (CMS-W).

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

Date Submitted for review/approval: September 1, 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.

The Case Management System (CMS-W) is an overarching subsystem hosted within BASS that provides an integrated methodology for planning, scheduling, conducting, reposting, and analyzing allegations programs for the NRC. CMS-W is the umbrella title given to three separate applications. The following are the 3 applications within CMS-W.

Enforcement Action Tracking System (EATS) - web application that allows authorized users to enter new or updated case information, query enforcement case information, report on enforcement case information, and update validation tables and user logon information.

Allegation Management System (AMS) – database web application that is used to assist in the timely collection, storage, and retrieval of key information on allegations received by the NRC related to NRC regulated facilities. AMS was developed so that individual offices of the NRC could manage information regarding allegations related to NRC regulated facilities more effectively.

Case Management System (CMS) - designed to assist the Office of Investigations (OI) in meeting their objectives by tracking all the different entities required for NRC investigations.

CMS-W tracks enforcement activities, allegations, individuals, and entities referred to in potential or actual investigations and matters of concern to the Office of Investigations.

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

<input type="checkbox"/> PowerApps	<input type="checkbox"/> Public Website
<input type="checkbox"/> Dashboard	<input type="checkbox"/> Internal Website
<input type="checkbox"/> SharePoint	<input type="checkbox"/> None
<input checked="" type="checkbox"/> Other: Data resides on the CMS-W servers.	

Case Management System Web (CMS-W)	Version 1.0
Privacy Impact Assessment	08/30/2023

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> Applying the new PIA template.
<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
Name	Elena Greynolds	David Pelton (AMS and EATS), Thomas Ashley (CMS)	Consuella Debnam	N/A	N/A	N/A
Office /Division /Branch	Office of the Chief Information Officer (OCIO)	Office of Enforcement (OE), Office of Investigations (OI)	Office of the Chief Information Officer (OCIO)			
Telephone	301-287-0794	301-415-1492 301-415-0771	301-287-0834			

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"/>	Statute	<ul style="list-style-type: none"> • Privacy Act of 1974, as amended, 5 U.S.C. §552a • Paperwork Reduction Act, as amended, 44 U.S.C. § 3501 et seq • E-Government Act of 2002, Section 208 (Public Law 107-347)

Case Management System Web (CMS-W)	Version 1.0
Privacy Impact Assessment	08/30/2023

		• Records Management by Federal Agencies, 44 U.S.C. Chapter 31
<input type="checkbox"/>	Executive Order	
<input type="checkbox"/>	Federal Regulation	
<input type="checkbox"/>	Memorandum of Understanding/Agreement	
<input type="checkbox"/>	Other (summarize and provide a copy of relevant portion)	

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).

CMS-W tracks enforcement activities, allegations, individuals, and entities referred to in potential or actual investigations and matters of concern to the Office of Investigations. CMS contains sensitive allegation, enforcement action, and investigation data involving actual or alleged criminal and civil/regulatory violations. CMS may include witness and subject names and personal identifiers as well as personal background information with address and phone numbers. These systems will contain detailed information on current and completed allegations, enforcement actions, and investigations with pre-decisional information for enforcement actions.

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

The SSN is used to conduct investigations. CMS-W tracks enforcement activities, allegations, individuals, and entities referred to in potential or actual investigations and matters of concern to the Office of Investigations.

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

Case Management System Web (CMS-W)	Version 1.0
Privacy Impact Assessment	08/30/2023

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 checked="" type="checkbox"/>	Resume or curriculum vitae
<input checked="" type="checkbox"/>	Date of Birth	<input checked="" 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 checked="" 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 checked="" type="checkbox"/>	Personal Mobile Number	<input type="checkbox"/>	Accommodation/disabilities information
<input type="checkbox"/>	Marital Status	<input type="checkbox"/>	Other: Organization, Education, Training, Certifications, Experience, License type, Height, Weight, Eye Color, Scars/Tattoo's, Title.
<input type="checkbox"/>	Children Information		
<input type="checkbox"/>	Mother's Maiden Name		

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).

The license information, witness/subject names, addresses, phone numbers, social security numbers, and physical attributes collected by the CMS-W application will come from existing hardcopy files (the information will be manually entered into the system).

The background information collected about individuals by CMS-W, including criminal history and individual business information, is from a background investigation with information obtained through the National Crime Information Center (NCIC). In addition, the background information is also collected through public records such as credit checks, property records, investment records, and Dun and Bradstreet Reports. These databases, however, do originally collect their information from the subject individual and require periodic updates to verify the accuracy of the information.

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

N/A.

Case Management System Web (CMS-W)	Version 1.0
Privacy Impact Assessment	08/30/2023

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

The individual’s information will be pulled from other NRC databases and files, and through public records such as credit checks, property records, investment records, and Dun and Bradstreet Reports

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

This information will be validated for relevancy and accuracy by the cross-reference of the current data provided by the CMS-W applications.

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

No.

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

The application user with the correct permissions can open an existing case, locate the individual’s information, and complete the update.

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).

CMS-W is accessed by user account and password verification as assigned by the application administrators. Additionally, access to varying features of CMS-W is restricted by user roles. The BASS administrators and database administrators have high-level access to the CMS-W. Appropriate access must be requested by the user through project managers and application owners and then be granted by CMS-W administrators to ensure access is limited to authorized users only.

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.

No. Only CMS-W will share data between the three applications (EATS, AMS and CMS).

Case Management System Web (CMS-W)	Version 1.0
Privacy Impact Assessment	08/30/2023

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.

Access to CMS-W is limited to authorized personnel only. This is also enforced through access controls. The applications track users (by LAN ID and date) who add or update data. Audit trails will be reviewed periodically to minimize the impact of misuse.

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 will be transmitted electronically on the NRC networks behind the NRC firewall. All data transfer will be internal, and on the infrastructure only.

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

Some of the PII data stored in CMS-W will be encrypted in the database. Yes, the data may be used by OI personnel (or NRC personnel) for investigation purposes and when printed as a report which is classified as an aggregation of data. This information will be stored in locked cabinets if/when it is created as a report.

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

Yes, the CMS-W environment is located at NRC HQ. All users using CMS-W are behind the NRC firewall and on the NRC network. Consistent use will be maintained from all sites via agency approved methods (e.g., VPN, mobility platforms). Because users will need to be on the NRC LAN to access CMS, access authorization enforcement is facilitated.

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

No, only authorized personnel. OI has access to CMS-W.

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

Auditing measures in place include record keeping of system access, application logs of sign-on and sign-off activities, records of additions and deletions to databases, and Unix/Linux logs for administrator access. Technical safeguards include access authorization enforcement, periodic password changes, and account reviews.

Case Management System Web (CMS-W)	Version 1.0
Privacy Impact Assessment	08/30/2023

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

Yes. Monitoring information will be provided by the CMS-W applications. The applications will store information that will include individual licenses, licensees, radioactive material, and allegation data, witnesses, and subjects. This data will provide monitoring support, allowing authorized application users to monitor and track individuals.

4.11 Define which FISMA boundary this project is part of.

BASS.

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.

20050012.

5 Privacy Act Determination

5.1 Is the data collected retrieved by a personal identifier?

Data will be retrieved from the CMS-W databases using queries and data output created by CMS applications. Data can be retrieved by an individual's name or personal identifier and will be viewed on the system or printed out by authorized personnel.

Mark the appropriate response.

Response	
<input checked="" type="checkbox"/>	Yes, the PII is retrieved by a personal identifier (i.e., individual's name, address, SSN, etc.)
<input type="checkbox"/>	List the identifiers that will be used to retrieve the information on the individual.
<input type="checkbox"/>	No, the PII is not retrieved by a personal identifier. If no, explain how the data is retrieved from the project.

Case Management System Web (CMS-W)	Version 1.0
Privacy Impact Assessment	08/30/2023

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"/>	Yes, this system is covered by an existing SORN. (See existing SORNs: https://www.nrc.gov/reading-rm/foia/privacy-systems.html) Provide the SORN name, number, (List all SORNs that apply): CMS-W is covered under the Privacy Act system of records NRC 23, Case Management System – Indices, Files, and Associated Records
<input type="checkbox"/>	SORN is in progress
<input type="checkbox"/>	SORN needs to be created
<input type="checkbox"/>	Unaware of an existing SORN
<input type="checkbox"/>	No, this system is not a system of records and a SORN is not applicable.

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

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

Mandatory.

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 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

Case Management System Web (CMS-W)	Version 1.0
Privacy Impact Assessment	08/30/2023

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 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 checked="" type="checkbox"/>	NUREG-0910, "NRC Comprehensive Records Disposition Schedule"
<input type="checkbox"/>	NARA's General Records Schedules
<input checked="" type="checkbox"/>	Unscheduled

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

System Name (include sub-systems, platforms, or other locations where the same data resides)	Regardless of the format or location of data/records such as hardcopy, electronic format in CMS-W, ADAMS or another authoritative source, all records should be disposed of according to the NUREG 0910 or GRS. There are 3 separate applications: EATS; AMS; and CMS. Most of the data/information in the system is covered by several schedules for these applications. However, some records/data in the system may need to be scheduled as they may not follow under any identified schedule; therefore, NRC records personnel will need to work
---	--

Case Management System Web (CMS-W)	Version 1.0
Privacy Impact Assessment	08/30/2023

	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.
Records Retention Schedule Number(s)	NUREG 2.16.1- Allegation and Inquiry Files
Approved Disposition Instructions	Official case files located at HQ documenting allegations of possible wrongdoing
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
Disposition of Temporary Records Will the records/data or a composite be automatically or manually deleted once they reach their approved retention?	Temporary. Hold closed allegation case files in office for 2 years.
Disposition of Permanent Records 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? NRC Transfer Guidance (Information and Records Management Guideline - IRMG)	Destroy 10 years after cases are closed.
Records Retention Schedule Number(s)	NUREG 2.16.4.a (N1-431-01-1 item 1a)- Investigation Case Files. Official case files created by field investigators

Case Management System Web (CMS-W)	Version 1.0
Privacy Impact Assessment	08/30/2023

	and maintained at regional field offices
Approved Disposition Instructions	<p>Cases which meet the following criteria-wide attention from media:</p> <ul style="list-style-type: none"> - Significant interest to Congress or White House or the Commissioners - Extensive litigation - Major policy discussion or change <p>Significant changes to designs or procedures relating to the nuclear industry</p>
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
Disposition of Temporary Records Will the records/data or a composite be automatically or manually deleted once they reach their approved retention?	N/A
Disposition of Permanent Records 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? NRC Transfer Guidance (Information and Records Management Guideline - IRMG)	Permanent. Cut off files when case is closed. Hold in field office for 6 months, then forward to HQ for processing. Hold for 2 years, and then transfer to NARA in 10-year blocks at 10-year intervals.
Records Retention Schedule Number(s)	NUREG 2.16.4.b - Investigation Case Files which do not meet permanent criteria
Approved Disposition Instructions	Files created by field investigators and maintained in regional offices that do not meet the criteria for permanent retention
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	N/A

Case Management System Web (CMS-W)	Version 1.0
Privacy Impact Assessment	08/30/2023

records accessibility, reliability, integrity, and disposition.	
<p>Disposition of Temporary Records</p> <p>Will the records/data or a composite be automatically or manually deleted once they reach their approved retention?</p>	<p>Temporary. Cut off files when case is closed. Hold in field office for 6 months, and then forward to HQ. Hold for 2 years.</p>
<p>Records Retention Schedule Number(s)</p>	<p>NUREG 2.10.2. a -Enforcement Action Case Files.</p> <p>Significant Enforcement Actions</p>
<p>Approved Disposition Instructions</p>	<p>Case files located in OE and the Regions documenting enforcement actions and violations.</p> <p>Enforcement actions that have exceptional value because of the historical significance of their contents or their uniqueness:</p> <ul style="list-style-type: none"> - Significant judicial decisions or legislation that affect the functions and activities of NRC - Significant changes in regulatory activities and procedures - Subject of congressional investigation or great public interest <p>Substantive information supporting docket files identified for permanent retention</p>
<p>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.</p>	N/A
<p>Disposition of Temporary Records</p> <p>Will the records/data or a composite be automatically or manually deleted once they reach their approved retention?</p>	N/A
<p>Records Retention Schedule Number(s)</p>	<p>NUREG 2.10.2.b - Enforcement Action Case Files. (Routine)</p>
<p>Approved Disposition Instructions</p>	<p>All other enforcement actions and</p>

Case Management System Web (CMS-W)	Version 1.0
Privacy Impact Assessment	08/30/2023

	violations
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
Disposition of Temporary Records Will the records/data or a composite be automatically or manually deleted once they reach their approved retention?	Temporary. Cut off files when case is closed. Hold 2 years. Destroy 10 years after enforcement actions are cut off.
Disposition of Permanent Records 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? NRC Transfer Guidance (Information and Records Management Guideline - IRMG)	N/A
Records Retention Schedule Number(s)	GRS 5.2 item 020` - Intermediary records* *This schedule is generally used to dispose of those records (paper or electronic) which are used to create a subsequent record, such as those manually input into a system
Approved Disposition Instructions	Records of an intermediary nature, meaning that they are created or used in the process of creating a subsequent record
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
Disposition of Temporary Records Will the records/data or a composite be automatically or manually deleted once they reach their approved retention?	Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

Case Management System Web (CMS-W)	Version 1.0
Privacy Impact Assessment	08/30/2023

<p>Disposition of Permanent Records</p> <p>Will the records be exported to an approved format and transferred to the National Archives based on approved retention and disposition instructions?</p> <p>If so, what formats will be used?</p> <p>NRC Transfer Guidance (Information and Records Management Guideline - IRMG)</p>	<p>N/A</p>
---	------------

SUMMARY OF RECORDS RETENTION SCHEDULES AND DISPOSITIONS (SAME AS ABOVE)		
SCHEDULE NUMBER	SCHEDULE TITLE	DISPOSTION
<p>NR4-2.10.2.A(1) N1-431-00-5 item 1a</p>	<p>Enforcement Action Case Files. Significant Enforcement Actions</p>	<p>Permanent. Cut off files when case is closed. Transfer to NARA with indexes when 20 years old.</p> <p>(Same retention for the Regions)</p>
<p>NR4-2.10.2.B(1) N1-431-00-5 item 3.b(1)(a)</p>	<p>Enforcement Action Case Files. All Other Enforcement Actions and Violations</p>	<p>Temporary. Cut off files when case is closed. Hold 2 years. Destroy 10 years after enforcement actions are cutoff.</p> <p>(Same retention for the Regions)</p>
<p>NR4-2.16.1 NC1-431-83-6 item 1</p>	<p>Allegation and Inquiry Files</p>	<p>Temporary. Hold closed allegation case files in office 2 years. Destroy 10 years after cases are closed.</p> <p>(Allegation files will be bucketed to cover multiple offices in the agency)</p>
<p>NR4-2.17.1 N1-43-00-13 item 1.a NR4-2.18.1 N1-431-00-8 item 1.a</p>	<p>Allegation Case Files</p>	<p>Temporary. Cut off files upon final resolution of allegation. Retain in office for 2 years or until no longer needed for current activities. Destroy 10 years after cutoff.</p> <p>(Covers NMSS and NRR)</p>

Case Management System Web (CMS-W)	Version 1.0
Privacy Impact Assessment	08/30/2023

NR4-2.16.4.a N1-431-01-1 item 1a	Investigation Case Files (Significant)	Permanent. Cut off files when case is closed. Hold in field 6 months then forward to HQ. Hold for 2 years, Transfer in 10-year blocks which will be transferred at 10-year intervals.
NR4-2.16.4.b.4 N1-431-01-1 item 1.b	Investigation Case Files. Files that do not meet criteria for permanent retention	Temporary. Cut off files when case is closed. Hold in field office for 6 months then forward to HQ. Hold for 2 years. Destroy 20 years after cases are closed.
GRS 5.2 item 020	Intermediary Records. This schedule is generally used to dispose of those records which are used to create a subsequent record, such as those manually input into a system.	Temporary. Destroy upon creation or update of the final record, or when no longer needed for business use, which is later.

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?

Yes, however, OMB approval is not required for information collections during a Federal criminal investigation or prosecution, during a civil action to which the United States is a party, or during the conduct of intelligence activities.

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)?

N/A.

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

OMB approval is not needed for information collections made:

- During the conduct of a federal criminal investigation or prosecution, or during the disposition of a particular criminal matter.
- During the conduct of a civil action to which the United States or any official or agency

Case Management System Web (CMS-W)	Version 1.0
Privacy Impact Assessment	08/30/2023

thereof is a party, or during the conduct of an administrative action, investigation, or audit involving an agency against specific individuals or entities. However, the requirements of the Paperwork Reduction would apply during the conduct of general investigations or audits undertaken with reference to a category of individuals or entities such as a class of licensees or an entire industry.

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>.

Case Management System Web (CMS-W)	Version 1.0
Privacy Impact Assessment	08/30/2023

8 Privacy Act Determination

Project/System Name: Case Management System Web (CMS-W).

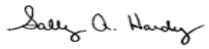
Submitting Office: Office of the Chief Information Officer (OCIO).

Privacy Officer Review

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

Comments:

Covered by NRC 23 – Case Management System – Indices, Files, and Associated Records.

Reviewer's Name	Title
 Signed by Hardy, Sally on 09/22/23	Privacy Officer

Case Management System Web (CMS-W)	Version 1.0
Privacy Impact Assessment	08/30/2023


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:

See Section 7.

Reviewer's Name	Title
 Signed by Cullison, David on 09/12/23	Agency Clearance Officer


Case Management System Web (CMS-W)	Version 1.0
Privacy Impact Assessment	08/30/2023

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 checked="" type="checkbox"/>	Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:

Regardless of the format or location of data/records such as hardcopy, electronic format in CMS-W, ADAMS or another authoritative source, all records should be disposed of according to the NUREG 0910 or GRS. There are 3 separate applications: EATS; AMS; and CMS. Most of the data/information in the system is covered by several schedules for these applications. However, some records/data in the system may need to be scheduled as they may not follow under any identified schedule; 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 09/14/23	Sr. Program Analyst, Electronic Records Manager

Case Management System Web (CMS-W)	Version 1.0
Privacy Impact Assessment	08/30/2023

11 Branch Chief Review and Concurrence

Review Results	
<input type="checkbox"/>	This project/system does not collect, maintain, or disseminate information in identifiable form.
<input checked="" type="checkbox"/>	This project/system does 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 09/28/23

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

Case Management System Web (CMS-W)	Version 1.0
Privacy Impact Assessment	08/30/2023

ADDITIONAL ACTION ITEMS/CONCERNS

Name of Project/System: Case Management System Web	
Date CSB received PIA for review: September 1, 2023	Date CSB completed PIA review: September 20, 2023
Action Items/Concerns: 	
<p><i>Copies of this PIA will be provided to:</i></p> <p><i>Ledetria Beaudoin</i> <i>Director (Acting)</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>	