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.

Case Management System Web (CMS-W)

Date: May 28, 2021

A. GENERAL SYSTEM INFORMATION

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

The Case Management System Web (CMS-W) is an overarching subsystem hosted within the Business Application Support System (BASS) that provides an integrated methodology for planning, scheduling, conducting, reposting, and analyzing allegation programs for the U.S. Nuclear Regulatory Commission (NRC). CMS-W is the umbrella title given to three separate applications.

- 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) - Application that allows authorized users to store and retrieve key information on allegations related to NRC-regulated facilities. AMS was developed so that Headquarters and Regional 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) meet their objectives by tracking all the different entities required for NRC investigations. This was previously called the Office of Investigations Management Information System. It has been renamed CMS.

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

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

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

There are no other modules or subsystems.

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 Privacy Information by applications hosted in the CMS-W environment has been authorized by the following statues:

- 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)
- Records Management by Federal Agencies, 44 U.S.C. Chapter 31

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

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.

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*.)

Technical Project Manager	**Office/Division/Branch**	**Telephone**
Natasha Harris - CMS	OI	301-415-2374
Dori Willis - AMS	OE	301-287-9423
Lisamarie Jarriel - AMS	OE	301-287-9006
Robert Fretz - EATS	OE	301-287-9235
ISSO	**Office/Division/Branch**	**Telephone**
Consuella Debnam	OCIO	301-287-0834
Luc Phuong	OCIO	301-415-1103
System Owner/User	**Office/Division/Branch**	**Telephone**
Thomas Ashley	OCIO	301-415-0771

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.

ML20148M353 June 17, 2020.

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

The CMS will integrate the Office of Enforcement (OE's) and OI's databases (AMS, EATS, and CMS).

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

Yes.

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

EA 20050012.

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.)).

CMS maintains personal information about Federal employees, licensees, and Federal contractors that work with nuclear materials inside and outside of NRC. It will also contain the personal information about concerned individuals that report allegations to the Agency.

(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)?

The information that resides within the three CMS-W applications (AMS, EATS and CMS) includes: Name, organization, witness and subject names, addresses, phone number, license type, certifications, title, Social Security Number, driver's license number, physical attributes (i.e., height, weight, hair color, eye color, ethnicity, scars or tattoos), citizenship, education, experience, training, and birth date.

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

Yes.

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

- Name
- Organization
- Education
- Training
- Certifications
- Experience
- Addresses
- Phone number
- License type
- Birth date
- Social Security Number
- Driver's license number
- Height
- Weight
- Hair Color
- Eye color
- Ethnicity
- Scars or tattoos
- Title

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?

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. There is no OMB clearance needed

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

N/A.

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

Yes.

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

The license information, alleger names, 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).

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

Yes.

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

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. Also, 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.

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

The individual will be pulled from other NRC databases and files. Information will also be pulled through public records such as credit checks, property records, investment records, and Dun and Bradstreet Report.

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

CMS will pull information from License files and from Replacement Reactor Program System which resides in BASS.

2. INFORMATION NOT ABOUT INDIVIDUALS

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

No.

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

N/A.

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

N/A.

C. USES OF SYSTEM AND INFORMATION

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

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

The system data collected by CMS-W applications will be used for the following activities:

- Track individuals
- Track licensees and licensed materials
- Track vendors and the materials they build/sell
- Track websites and the materials they sell
- Contact NRC personnel, as well as external personnel, involved in the use of nuclear materials
- Perform background checks and verification of personnel qualifications
- Verify employer information and personnel certifications
- Create, edit, track, and resolve allegations in the CMS-W application

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

Yes.

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

The BASS Information System Security Officer (ISSO) and the Application ISSO for each application in the BASS environment will be individually responsible for ensuring that the data collected by each application is used appropriately.

4. 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?

Privacy data elements collected by BASS applications are described at a high level in the BASS CMS-W System Security Plan (SSP) and in more detail in respective BASS Application administrator guides and user documentation for each application. These documents include the Case Management User Manual.

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

Some of the Personally Identifiable Information (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, classified as aggregation of data. This information will be stored in locked cabinets if/when it is created as a report.

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?

All output from CMS-W applications will be stored in locked file cabinets and available to authorized personnel only.

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

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

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

Consolidated data that is output in a report from the CMS-W applications are protected by physical access controls. This data is stored in locked file cabinets and only accessible to authorized individuals. Aggregated data will be created on an as-needed basis and will only be accessible to authorized personnel who have signed the necessary Rules of Behavior (ROB) documentation and have the appropriate clearance.

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

Yes. By individual's name or personal identifier.

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

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.

7. 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.

CMS-W is covered under the Privacy Act system of records NRC 23, "Office of Investigations Indices, Files and Associated Records.

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

Not Sure – Would adding the Office of Enforcement require an amendment or revision? It currently only states "Office of Investigation".

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

Yes.

a. If yes, explain.

Monitoring information will be provided by the CMS 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.

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

CMS W applications will use access controls, including user rights and privilege enforcement through access control lists and ROBs acknowledgement documentation, to prevent unauthorized monitoring of personal information.

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

OI Reports

CASE REPORTS

- Status Report
- Cases Initiated
- Open Cases Trend Report
- Open Cases Detail Trend Report
- Closed Cases
- Investigations Referred to DOJ
- By Allegation Method
- By Allegation Source
- By Received Date
- OI Violation
- Case Statistics
- Case Status

ACTIVITY REPORTS

- Law Enforcement Tracking and Coordination Activities
- Chronology
- ISR Report
- Agent Activities
- Activity Certification

CRIMINAL REPORTS

- Referrals
- Indictments
- Convictions
- Sentencing
- Declinations

CIVIL REPORTS

- Referrals
- Filings
- Judgments
- Settlements
- Recoveries
- Declinations
- Annual Case Count Summary
- Performance Measure
- Performance Measure Annual
- Performance Measure Material
- Performance Measure High Level Waste
- Performance Measure Reactors
- Performance Measure New Reactors
- Case Count ALL
- Case Count Reactors
- Case Count Materials
- Case Count High Level Waste
- Case Count H & I Cases
- Case Count NON-H & I Cases
- OI National Performance STATS

SOL REPORT

LEAP REPORTS

- Leap Report Pay Year
- Region 1 Pay Period
- Region 2 Pay Period
- Region 3 Pay Period
- Region 4 Pay Period
- Region HQ Pay Period
- Manpower Report
- Non-Case Specific Investigative to the Mission
- Case Specific Investigative Activities
- Miscellaneous/Other Investigative Activities
- Records Retention
- Inactive Cases
- Recently Approved Docs.
- Annual Report Details
- Annual Report Statistics
- Criminal Cases
- Performance Measures - Stats
- Performance Measures – Details
- Dead files
- Summary Sheet
- Licensee History
- Regional Weekly Status
- Data Compilation Report
- Escalated Enforcement Actions Timeliness Report

- Statistical Summary Report
- Ad-Hoc Report

ALLEGATION REPORTS

Weekly Status Report – includes the following

- Initial ARBs Due
- Follow-up/6-Monthy ARBS Due
- Acknowledgment Letters Due
- Status Letters Due
- Non-Allegations and Open Actions
- Open Agreement State Actions
- Open DOL Actions
- Responses After Closure
- Technical Actions Due in 2 Weeks
- Actions Overdue
- All Open Allegations and Actions

Monthly Status Report for each HQ office – includes the following

- Monthly Activity (allegations opened, and allegations closed)
- CY Activity (Items received during the CY/FY, number of acknowledgment letters, ARBs, and closures and their related metrics, feedback measures)
- Summary of Open Allegations (separated by technical allegations and OI/DOL/ADR allegations)

Other Reports/Queries

- Quarterly VIPP Inspection Metrics
- Commissioner Drop-In Briefings
- Security Allegations
- Fitness-for-Duty Allegations
- FOIA List for Specific Sites
- Closed Case Chronology
- Index of Allegation Concerns
- Open Chilled Environment Allegations

a. What are the reports used for?

These reports provide information used for investigation and allegation purposed.

b. Who has access to these reports?

CMS administrators, OI directors. Special Agents in Charge, assistant directors, investigation assistants, senior agents, HQ Allegation Team (HQAT) and agents may have access to CMS information reports only.

D. ACCESS TO DATA

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

Data in CMS-W is accessed by OE (enforcement specialists and HQAT), Allegation staff in the regions, and OI offices at HQ and the regions.

(1) For what purpose?

All users will access PII data and physical attributes on entities for allegation, investigation, and enforcement purposes.

(2) Will access be limited?

Access to CMS is limited to authorized personnel only. This is also enforced through access controls. The applications track users by Local Area Network Identification and date who add or update data. Audit trails will be reviewed periodically to minimize the impact of misuse.

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

No.

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

N/A.

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

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

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.

Regardless of the format or location of data/records such as in hard copy, 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: Enforcement Action Tracking System (EATS; Allegation Management System (AMS; and Case Management System (CMS) - CMS-W. Most of the data/information in the system is covered by several schedules for these applications as shown in the table under (a). 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.

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?**

Schedule Number	Records Series/Title	Description	Disposition
NUREG 2.16.1	Allegation and Inquiry Files	Official case files located at HQ documenting allegations of possible wrongdoing…	Temporary. Hold closed allegation case files in office for 2 years. Destroy 10 years after cases are closed.
NUREG 2.16.4.a	Investigation Case Files. Official case files created by field investigators and maintained at regional field offices	Cases which meet the following criteria: -wide attention from media - significant interest to Congress or White House or the Commissioners -Extensive litigation -Major policy discussion or change -Significant changes to designs or procedures relating to the nuclear industry	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 then transfer to NARA in 10-year blocks at 10year intervals.
NUREG 2.16.4.b	Investigation Case Files which do not meet permanent criteria	Files created by field investigators and maintained in regional offices that do not meet the 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.
NUREG 2.10.2. a	Enforcement Action Case Files. Significant Enforcement Actions	Case files located in OE and the Regions documenting enforcement actions and violations…Enforcement actions that have exceptional value because of the historical significance of their	Permanent. Cut off files when case is closed. Hold 5 years. Transfer to NARA with related indexes when 20 years old.

		contents or their uniqueness: -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 -Substantive information supporting docket files identified for permanent retention	
NUREG 2.10.2.b	Enforcement Action Case Files. (Routine)	All other enforcement actions and violations	Temporary. Cut off files when case is closed. Hold 2 years. Destroy 10 years after enforcement actions are cutoff.
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	Records of an intermediary nature, meaning that they are created or used in the process of creating a subsequent record.	Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

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).

Access to varying features of CMSW is restricted by user roles. The application administrators and database administrators have high-level access to the

CMSW. 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.

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

Access controls and identification and authentication controls are in place. Specifically, account management and access enforcement are implemented to prevent the misuse of system data. Only authorized users who have been approved by project managers and applications owners and reviewed by CMS-W administrators are granted access. Furthermore, identification and authentication controls are used to enforce unique ID requirements and periodic password changes.

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

N/A.

(1) If yes, where?

Yes. Criteria, procedures, controls, and responsibilities for CMS-W are documented in the CMS-W SSP and in the respective application user and administrator guides found in the BASS document.

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

Yes.

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

The CMSW 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, Citrix, mobility platforms) because users will need to be on the NRC LAN to access CMS access authorization enforcement is facilitated.

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

OI, OE (enforcement HQAT), Regional allegation staff, and application administrators.

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

N/A.

a. If yes, what will be collected?

Yes. CMS-W captures time of access and what changes have been made by which user for applications.

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?

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 logs for administrator access. Technical safeguards include access authorization enforcement, and account reviews.

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

Yes.

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

December 23, 2019, (BASS).

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

N/A.

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

N/A.

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

System Name: Case Management System Web (CMS-W)

Submitting Office: OCIO

A. PRIVACY ACT APPLICABILITY REVIEW

____ Privacy Act is not applicable.

__X__ Privacy Act is applicable.

Comments:

CMS-W is covered under the Privacy Act system of records NRC 23, "Office of Investigations, Indices, Files and Associated Records".

Reviewer's Name	Title
Signed by Hardy, Sally on 07/21/21	Privacy Officer

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

__X__ No OMB clearance is needed.

____ OMB clearance is needed.

____ Currently has OMB Clearance. Clearance No._____

Comments:

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 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 Act 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. Likewise, the requirements of the

Paperwork Reduction Act would likely apply to any portal developed for interactions with the public.

Reviewer's Name	Title
 Signed by Cullison, David on 06/14/21	Agency Clearance Officer

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

____ No record schedule required.

____ Additional information is needed to complete assessment.

____ Needs to be scheduled.

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

Comments:

Reviewer's Name	Title
 Signed by Dove, Marna on 06/21/21	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 Nalabandian, Garo on 07/27/21

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 Ashley, OCIO	
Name of System: **Case Management System Web (CMS-W)**	
Date CSB received PIA for review: May 28, 2021	**Date CSB completed PIA review:** July 21, 2021
Noted Issues: SORN NRC 23 will be renamed to Case Management System and other revisions made to clarify that this SORN covers more than just OI information.	
Chief Cyber Security Branch Governance and Enterprise Management Services Division Office of the Chief Information Officer	Signature/Date: Signed by Nalabandian, Garo on 07/27/21
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*	