ADAMS ML13358A187

# 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:** 12/23/13

## A. GENERAL SYSTEM INFORMATION

1. Provide a detailed description of the system:

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;

- 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) meet their objectives by tracking all the different entities required for NRC investigations. This was previously called the Office of Investigations Management Information System (OIMIS). It has been renamed CMS.

***This PIA was revised to update the CMS-W application with new PII.

2. What agency function does it support?

CMS-W supports the Office of Investigations (OI). OI uses CMS-W to track enforcement activities, allegations individuals and entities referred to in potential or actual investigations and matters of concern to the Office of Investigations.

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?

   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:

| **Project Manager** | **Office/Division/Branch** | **Telephone** |
|---|---|---|
| Claire Robb | Office of Information Services (OIS)/Operations Division (OD)/Applications Operations Branch (AOB) | (301) 287-0779 |
| **Business Project Manager** | **Office/Division/Branch** | **Telephone** |
| Benjamin Partlow | OIS/OD/AOB | (301) 287-0817 |
| **Technical Project Manager** | **Office/Division/Branch** | **Telephone** |
| Claire Robb | OIS/OD/AOB | (301) 287-0779 |
| **Executive Sponsor** | **Office/Division/Branch** | **Telephone** |
| Robert Webber | OIS/OD | (301) 287-0763 |

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 (Explain)

   b. If modifying an existing system, has a PIA been prepared before? Yes

(1) If yes, provide the date approved and ADAMS accession number.

CMS-W: ML061180261, approved on May 25, 2006

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

Added additional data that is considered PII (i.e., driver's license number) and physical attributes of entities (witnesses and subjects).

- Height
- Weight
- Hair color
- Eye color
- Ethnicity
- Scars or tattoos
- Title

## 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?

(1) If yes, identify the group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public).

Yes. CMS maintains personal information about Federal employees, licensees, and Federal contractors that work with nuclear materials inside and outside of NRC.

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

b. What information is being maintained in the system about an individual (be specific)?

The information that resides within the three CMS-W applications (AMS, EATS and CMS) includes: Name, organization, Human Resources Management System (HRMS)-ID, 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?

Yes. All of the information listed above is collected from the subject individual.

(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 10 or more individuals who are **not** Federal employees?

Yes.

(1) If yes, does the information collection have OMB approval?
(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, 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 (NCIC). 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?

Information not collected by the individual will be pulled from other NRC databases and files. Through public records such as credit checks, property records, investment records, and Dun and Bradstreet Reports.

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

CMS-W will pull information from License files and the Reactor Program System (RPS) which resides within BASS.

2. **INFORMATION NOT ABOUT INDIVIDUALS**

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

No.

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

Not applicable

## 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 (AMS, EATS and CMS) will be used for the following activities:

- Track individuals
- Track licensees and licensed materials
- 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?
   a. If yes, what is the name of the document that contains this information and where is it located?

      Yes. Privacy data elements collected by BASS applications are described at a high level in the BASS System Security Plan (SSP) and in more detail in the respective BASS administrator guides and user documentation for each application. These documents include the following:

      - 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 PII data stored in CMS-W will be encrypted in the database. 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.

   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?

      Aggregated data will be created on an as-needed basis; this data will also be stored in locked file cabinets and will only be accessible to authorized personnel who have signed the necessary rules of behavior (ROB) documentation or have the appropriate clearance. 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?

The applications track users by LAN ID and date who added or modified data. Audit trails are reviewed periodically to minimize the impact of misuse.

Consolidated data that is output in a report from CMS-W applications are protected by physical access controls. This data is stored in locked file cabinets and only accessible to authorized individuals.

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

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

a. If yes, explain.

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.

(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 rules of behavior acknowledgement documentation, to prevent unauthorized monitoring of personal information.

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

CMS-W applications produce reports.

a. What are the reports used for?

CMS stores PII data and physical attributes on entities (i.e., witnesses and other subjects) for investigation purposes. These entities may also be referenced for historical purposes of newer investigations.

b. Who has access to these reports?

CMS administrators, OI directors, field office directors and assistant directors, investigation assistants, senior agents, and agents may have access to CMS information.

**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 OI and OI offices in the regions.

(1) For what purpose?

OI offices will access PII data and physical attributes on entities for investigation purposes.

(2) Will access be limited?

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.

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

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

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

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

Data will be transmitted electronically on the NRC network 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?

Not applicable.

(2) Will access be limited?

Not applicable.

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

Not applicable.

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

Not applicable.

## E. RECORDS 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 are required under 36 CFR 1234.10. The following questions are intended to determine whether the records in the system have an approved records retention schedule or if one will be needed.*

1. Can you map this system to an applicable retention schedule in NUREG-0910, or the General Records Schedules at http://www.archives.gov/records-mgmt/grs ?

   No.

   a. If yes, please cite the schedule number, approved disposition, and describe how this is accomplished. For example, will the records or a composite thereof be deleted once they reach their approved retention or exported to a file for transfer based on their approved disposition?

      Please see question E.1.

   b. If the answer to question E.1 is yes, skip to F.1. If the response is no, complete question E.2 through question E.7.

2. If the records cannot be mapped to an approved records retention schedule, how long do you need the records? Please explain.
3. Would these records be of value to another organization or entity at some point in time? Please explain.

   The licensee information and witness/subject names stored by the CMS-W may be of use to another entity for historical purposes to review the individuals involved in past cases and to track use of licensing materials in the future.

4. How are actions taken on the records? For example, is new data added or updated by replacing older data on a daily, weekly, or monthly basis?

CMS-W contains data that is continuously edited, updated, and replaced with new data when necessary.

5. What is the event or action that will serve as the trigger for updating, deleting, removing, or replacing information in the system? For example, does the information reside in the system for three years after it is created and then is it deleted?

   CMS-W will retain data in accord with appropriate retentions. keep data indefinitely until it is either edited due to a change in data or a new record is created.

6. Is any part of the record an output, such as a report, or other data placed in ADAMS or stored in any other location, such as a shared drive or MS SharePoint?

   No.

7. Does this system allow for the deletion or removal of records no longer needed and how will that be accomplished?

   CMS-W will keep data indefinitely until it is either edited due to a change in data or a new record is created.

## F. TECHNICAL ACCESS AND SECURITY

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

   CMS-W is accessed by user account and password verification 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.

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?
   (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 repository.

4. Will the system be accessed or operated at more than one location (site)?
   a. If yes, how will consistent use be maintained at all sites?

   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 Information Technology Infrastructure's (ITI's) Citrix Remote Desktop software. Because users will need to be on the NRC LAN to access CMS and access authorization enforcement will be facilitated.

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

   OI has access to CMS-W.

6. Will a record of their access to the system be captured?
   a. If yes, what will be collected?

   Yes. CMS-W will capture 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 PII contract clauses are inserted in their contracts.

   - *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 Unix/Linux logs for administrator access. Technical safeguards include access authorization enforcement, periodic password changes, and account reviews.

9. Are the data secured in accordance with FISMA requirements?

Yes.

a. If yes, when was Certification and Accreditation last completed?

CMS-W is under BASS which completed a Security Test and Evaluation and received an Authority to Operate (ATO) on January 20, 2011 (ML110100569).

**PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL**

*(For Use by OIS/FPIB Staff)*

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

**Submitting Office:** Operations Division, Office of Information Services

## A. PRIVACY ACT APPLICABILITY REVIEW

____ Privacy Act is not applicable.

__X__ Privacy Act is applicable.

**Comments:**
CMS is not a new system, but an umbrella title give to 3 separate existing systems (Enforcement Action Tracking System (EATS), Allegation Management System (AMS), Case Management System (CMS))that is web-based applications allowing data common to all 3 systems to be shared electronically. The PIA is being revised to add additional data fields in the CMS system that is considered PII (i.e., driver's license number) and physical attributes of entities (witnesses and subjects). CMS is covered under Privacy Act system of records NRC-23, "OI Indices, Files and Associated Records." No change to the system notice will be required.

| Reviewer's Name | Title | Date |
|---|---|---|
| Sally A. Hardy | Privacy Act Program Analyst | January 17, 2013 |

## 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 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.

| Reviewer's Name | Title | Date |
|---|---|---|
| Fajr Majeed | Info. Management Analyst | January 16, 2014 |

## C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

___ No record schedule required.

____ Additional information is needed to complete assessment.

_X_ Needs to be scheduled.

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

**Comments:**
Records retentions for the system (data) do not currently exist, although retentions for some of the textual files in the case management files do exist. This system will need to be scheduled; therefore, OIS will work with both OE and OI to develop retentions for these records. Until the approval of such a schedule, these records and information are permanent. Implementation of retention schedules is mandatory under 44 U.S.C. 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 | Date |
|---|---|---|
| Mary Haynes | Records Management Analyst | January 14, 2014 |

## 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:

***/RA/*** Date **1/17/2014**

Laura Pearson, Branch Chief
FOIA, Privacy, and Info Collections Branch (FPIB)
Customer Service Division
Office of Information Services

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

| | |
|---|---|
| TO: **Robert Webber, Director, Operations Division, Office of Information Services** | |
| Name of System: **Case Management System Web (CMS-W)** | |
| Date IRSD received PIA for review: **January 3, 2014** | Date IRSD completed PIA review: **January 17, 2014** |
| **Noted Issues:**<br><br>The CMS System is covered under the Privacy Act system of records NRC-23.<br><br>Records retentions for the system (data) do not currently exist, although retentions for some of the textual files in the case management files do exist. This system will need to be scheduled; therefore, OIS will work with both OE and OI to develop retentions for these records. Until the approval of such a schedule, these records and information are permanent. | |
| Laura Pearson, Branch Chief<br>FOIA, Privacy, and Info Collections Branch (FPIB)<br>Customer Service Division<br>Office of Information Services | Signature/Date: ***/RA/*** **1/17/2013** |
| *Copies of this PIA will be provided to:*<br><br>*Gwen Hayden*<br>*Solutions Develop Division*<br>*Office of Information Services*<br><br>*Paul Ricketts*<br>*Senior IT Security Officer (SITSO)*<br>*FISMA Compliance and Oversight Team*<br>*Computer Security Office* | |