ADAMS ML20150A436

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.

Office of the Inspector General Management Information System (OIGMIS)

Date: May 29, 2020

A. GENERAL SYSTEM INFORMATION

1. Provide a detailed description of the system:

OIGMIS is an automated collaborative computing and workflow tracking system that supports the ongoing tracking of the NRC Office of the Inspector General (OIG) audit, investigation, and resource management operations. The system contains reports of OIG's audit and investigative activities including most documents used to formulate OIG findings, observations and recommendations. OIGMIS also supports the Defense National Facilities Safety Board (DNFSB) audits and investigations which are performed by NRC OIG staff.

Working documents for activities deemed by OIG management to be particularly sensitive are not contained in the OIGMIS but are processed, stored, and managed separately. Such activities typically include audit work papers prepared by contractors conducting Information Technology (IT) security audits and reports of interviews prepared by OIG criminal investigators in conjunction with sensitive OIG investigations. The OIGMIS contains sufficient information about these activities for completion of statistical reports for OIG's Semiannual Report to Congress but identifies the hard copy file as the repository for more detailed information.

Most audit reports and all investigative event inquiries are publicly available and published on the Nuclear Regulatory Commission's (NRC) external web site. Reports contained in the OIGMIS that are not publicly available are considered For Official Use Only (FOUO). The system does not contain any SAFEGUARDS or classified information.

Commercial-Off-The-Shelf (COTS) and custom databases on a Domino application server are utilized to meet business requirements. Built-in security features of the platform, such as database encryption and digital certificates,

restrict access to authorized users. The Windows 2012 R2 virtual server hosting the Domino application server is configured according to NRC standards and resides in NRC's Three White Flint North (3WFN) data center. OIGMIS is accessed by IBM Domino client software which is installed on standard NRC desktop or mobile desktop computers connected to the NRC network. Network port encryption is enabled at the server and allows unencrypted data to be encrypted at the port level for safe transport through the network. The Domino application server is password protected and requires an OIGMIS administrator to enter the password whenever the server is rebooted or the application service is restarted.

2. What agency function does it support?

The OIGMIS supports audits and investigations performed by the OIG.

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

- Windows 2012 R2 server – Hosts IBM Domino server which supports OIGMIS.
- IBM Domino server – Application server that hosts the IBM Domino databases comprising the OIGMIS. The system provides users and managers with instant data access, workflow, document control, standard formats and reports all within a controlled, multi-user environment. The OIGMIS contains the following databases:
    - AutoAudit – A customized COTS audit management database that stores OIG audit data. AutoAudit automates the audit process, including risk assessment, audit management, work papers and reporting, and managing audit recommendations. It also tracks progress in meeting performance objectives, training requirements, and resource utilization.
    - DNFSB AutoAudit – Same purpose as AutoAudit but for the Defense Nuclear Facilities Safety Board.
    - Magnum – A customized COTS case management database that stores OIG allegation and investigative data. Magnum automates the investigative process, including allegation disposition, case management and referrals and follow-up. It also tracks progress in meeting performance objectives, training requirements, and resource utilization.
    - DNFSB Magnum – Same purpose as Magnum but for the Defense Nuclear Facilities Safety Board.
    - Assistant Inspector General for Investigations (AIGI) Legacy Data – Database that contains information about allegations and cases received and processed by OIG and its predecessor, the Office of Inspector and Auditor (OIA), between 1985 and April 2005. It also includes electronic copies of case closing reports.
    - Operations Support Database - Stores administration and support procedures, and maintenance records for the OIGMIS.

- Correspondence Control Log (CCL) – Database used to log OIG incoming and outgoing correspondence. It is also used to track and manage Yellow Ticket correspondence requiring action by the office.

4. What legal authority authorizes the purchase or development of this system?

Inspector General Act of 1978 (as amended). *Pursuant to the Consolidated Approporation Act for Fiscal Year 2014 (H.R. 3547).*

What law, regulation, or Executive Order authorizes the collection and maintenance of the information necessary to meet an official program mission or goal?

Inspector General Act of 1978 (as amended*). Pursuant to the Consolidated Approporation Act for Fiscal Year 2014 (H.R. 3547).*

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

Information is collected to support the OIG's mission to (1) independently and objectively conduct and supervise audits and investigations relating to NRC's programs and operations; (2) prevent and detect fraud, waste, and abuse, and (3) promote economy, efficiency, and effectiveness in NRC's programs and operations.

6. Points of Contact:

Information System Owner	**Office/Division/Branch**	**Telephone**
Robert J. Feitel	OIG	301-415-5930
Information System Security Officer (ISSO)	**Office/Division/Branch**	**Telephone**
Consuella Debnam	OCIO/SDOB/SOB	301-287-0834
Project Manager/System Administrator	**Office/Division/Branch**	**Telephone**
Rick Grancorvitz	OIG	301-287-0805
Alternate System Administrator	**Office/Division/Branch**	**Telephone**
Ziad Buhaissi Kristean Marchant	OIG	301-415-1983 301-415-5890
Subsystem Information System Security Officer (ISSO)	**Office/Division/Branch**	**Telephone**
Eric Rivera Malion Bartley	OIG	301-415-7032 301-415-5962

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

a. ___ New System ___Modify Existing System _X_ Other (Explain)

This is an updated PIA prepared for an existing system.

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

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

April 1, 2019 – ML19092A059

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

The OIGMIS application now resides on a Windows 2012 R2 virtual server and is now a subsystem of the Business Application Support System (BASS).

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).

Investigation information includes individuals and entities referred in complaints or actual investigative cases, reports, accompanying documents, and correspondence prepared by, compiled by, or referred to the OIG. Subjects of the complaints and investigative cases include Federal employees and contractors. Information about the persons making the complaints could include Federal employees and contractors, licensees, interveners, or the general public.

Audit information includes names, titles, and work contact information for NRC employees and contractors associated with the NRC activities being audited.

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

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

OIGMIS could include the following information about an individual: first name, last name, home and work address, home and work phone number, employer, and email address.

Optional fields are Other Names Used, Date of birth, Place of Birth, Height, Weight, Social security number, Personal Telephone Number (Home, Mobile), Sex, Race, Marital Status, Scar/Marks/Tattoos, Prior Criminal Record and Picture.

c. Is information being collected from the subject individual?

Yes, the information is obtained from a variety of sources including, but not limited to, the individual record subject; NRC officials and employees; employees of Federal, State, local, and foreign agencies; and other persons.

To the greatest extent possible, collect information about an individual directly from the individual.

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

OIGMIS information could include correspondence, cases, matters, memoranda, materials, legal papers, evidence, exhibits, and data about a case and/or audit. An individual's first name, last name, address, phone number, and email address could also be collected should it concern the specifics of an investigation or audit.

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?

No, the Paperwork Reduction Act does not apply to the conduct of a Federal criminal investigation or during the conduct of an Administrative action, investigation, or audit involving an agency against specific individuals or entities.

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

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 information is obtained from a variety of sources including, but not limited to, the individual record subject; NRC officials and employees; and NRC contractors. It could contain information obtained from any NRC sensitive but unclassified files or systems. It does not contain Classified or Safeguards information.

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 information is obtained from a variety of sources including, but not limited to, the individual record subject; NRC officials and employees; employees of Federal, State, local, or foreign agencies; licensees; interveners, advocacy groups, and the general public.

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

OIG staff that input and update information in the system are responsible for ensuring that the data entered is current, accurate, and complete. The OIGMIS also utilizes a variety of automated mechanisms to verify the information, including:

- Mandatory fields that must be completed before a document can be saved
- Pick lists for selecting values for key fields to ensure data consistency
- Required management review and approval of documents, and record locking to prevent changes once documents are approved
- Validation checks to verify that prerequisite activities were completed, for example:
    - In AutoAudit, the status of an audit cannot be changed to complete unless all associated documents are approved

- In Magnum, a case cannot be closed with a disposition of Referred to NRC Management unless a referral form exists in the system

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

Information is input into the OIGMIS by authorized users via IBM Domino forms. Reference documents in electronic format are attached to forms using built-in electronic data transfer mechanisms of Windows and IBM Domino software.

2. INFORMATION NOT ABOUT INDIVIDUALS

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

Yes. Based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 and as documented in the OIGMIS Security Categorization, the OIGMIS processes the following types of Information:

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

Information Type	NIST SP 800-60 Description
Program Evaluation Information Type	Program Evaluation Information is used to document, analyze and report information related to investigations, allegations and audit work.
Program Monitoring Information Type	Program Monitoring Information is used to document, analyze and report information related to internal and external programs and the extent to which they comply with related laws, regulations, and policies.
Lifecycle/Change Management Information Type	Lifecycle/Change Management Information is used to document, track and approve information system modifications.
IT Security Information Type	IT Security Information is used to configure and monitor security configurations and to restrict access to data and functions.
Criminal Investigation and Surveillance Information Type	Criminal investigation and surveillance includes the collection of evidence required to determine responsibility for a crime and the monitoring and questioning of affected parties.
Legal Investigation Information Type	Legal Investigation Information is used to document, track and support activities

	associated with gathering information about a given party (government agency, citizen, and corporation) that would be admissible in a court of law, in an attempt to prove guilt or innocence.

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

The information is obtained from internal and external sources including but not limited to, the individual record subject, NRC officials and employees, employees of Federal, State, local, and foreign agencies and other persons.

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.

- Conducting, managing, and tracking the status and outcome of allegations, investigations, and audits
- References for aiding current OIG projects
- Routine uses identified in the Privacy Act System of Records Notices, NRC-18, Office of the Inspector General (OIG) Investigative Records

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 System Administrator, BASS Information System Security Officer(s) (ISSO) and the OIG Subsystem Information System Security Officer(s) (ISSO) are responsible for ensuring that the policies and procedures of the system are followed by users. The Assistant Inspector General for Investigations is responsible for ensuring that investigative records are used in accordance with the Privacy Act System of Records Notices, NRC-18, Office of the Inspector General (OIG) Investigative Records.

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?

Data elements are defined and characterized in the FY19_BASS_Security_Categorization_Report_v5.1_20190821, April 21, 2019 (EA Number 20070047). This information is maintained in the BASS Security Categorization Report as OIGMIS is a subsystem of BASS. Additional information about the data elements is maintained in the OIGMIS Operations Support Database.

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

No

Derived data is obtained from a source for one purpose and then the original information is used to deduce/infer a separate and distinct bit of information that is aggregated to form information that is usually different from the source information.

Aggregation of data is the taking of various data elements and then turning it into a composite of all the data to form another type of data (i.e. tables or data arrays).

a. If yes, how will aggregated data be maintained, filed, and utilized?

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

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

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

Investigative information is retrieved by the name of an individual, by allegation/case number, fiscal year, assigned investigative team/agent, NRC program office, status, or by subject matter. Audit information is retrieved by audit name/number, fiscal year, audit team, NRC program office, status, or assigned auditor name. CCL information is retrieved by fiscal year, NRC program office/external organization name, correspondence type, person assigned (OIG staff only), or status. Operations Support information is retrieved by subject matter(s).

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

No

a. If yes, explain.

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

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

A variety of reports are available to authorized users, such as:

- Performance measure reports
- Issue Area Monitoring activity reports
- Audit recommendation reports
- Hotline activity reports
- Allegation and Case reports
- Pending follow-up reports
- Referral reports
- Legal outcome and prosecution reports
- Law Enforcement Availability Pay (LEAP) reports
- Time and Expense by Activity reports

a. What are the reports used for?

Reports are used to track and manage investigation and audit activities, to assess progress in meeting OIG performance measures, to provide statistics for inclusion in OIG's Semi-Annual Report to Congress, and to respond to requests for information from external entities such as the Federal Bureau of Investigation.

b. Who has access to these reports?

Authorized OIGMIS users.

D. ACCESS TO DATA

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

OIG

(1) For what purpose?

Daily work activities that support OIG investigations and audits.

(2) Will access be limited?

Yes, access to information is limited to OIG through least privilege and separation of duties principles.

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).

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

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

No

If yes, who?

(1) Will access be limited?

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

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

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 ?

Yes.

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?

A records retention and disposition schedule (N1-431-10-002) for OIG records,

including OIGMIS, was approved by the Archivist of the United States on September 16, 2014. Additional information is scheduled under the General Records Schedules (GRS) below:

Lifecycle/Change Management Information Type (found under PIA Section B.2.a(1)	GRS 3.1 item 030	Configuration and Change Management Records	Temporary. Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use.
IT Security Information Type (found under PIA Section B.2.a(1)	GRS 3.2 item 010	Systems and data security records	Temporary. Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system.

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 <u>cannot</u> 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.

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?

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?

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?

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

F. <u>TECHNICAL ACCESS AND SECURITY</u>

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

In order to access the OIGMIS, users must have IBM Domino client software installed on their machine and be logged in to the NRC LAN. An OIGMIS digital certificate and password is then used to login to access OIG's Domino application server. If the user's certificate is a member of the Allowed Users group authentication to the Domino server is permitted, however the user is not able to access any OIGMIS data. Each database has its own Access Control List (ACL) and roles to limit what users can see and do within the database. The default access level for all OIGMIS databases is No Access. Once users successfully access a database, Reader and Editor permission fields on each document further restrict capabilities to specified roles and/or named users.

OIGMIS data is available only to authorized personnel who have a need to know and whose duties require access to the information. The OIGMIS application utilizes separation of duties to determine login abilities. Separate login accounts with different access privileges are used by personnel who have multiple roles within the OIGMIS, such as an auditor who also serves as a backup system administrator. Administrative access to the OIGMIS Domino application server is restricted to authorized OIGMIS administrators.

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

Access to data within the OIGMIS is restricted to authorized personnel who have a need to know and whose duties require access to the information. ACLs, roles, and document level Reader/Editor fields are used to prevent misuse. The default access level for all OIGMIS databases is No Access. Access permissions are independently assigned for each OIGMIS database, so authorized users of one database must be specifically granted access privileges to other databases in order to view the information it contains. Access permissions are promptly removed when users leave the OIG.

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

Yes

(1) If yes, where?

The "OIGMIS Technical Guidelines" is maintained by the OIG within the OIGMIS.

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

Users who have an NRC mobile desktop computer can access the OIGMIS remotely through NRC's Virtual Private Network (VPN).

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

Security controls implemented within the OIGMIS apply to all users and sessions regardless of their location.

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

- OIG criminal investigators
- OIG investigative analysts
- OIG auditors and management analysts
- OIG team leaders and managers
- OIG General Counsel
- OIG administrative support staff
- OIGMIS system administrators

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

Yes

a. If yes, what will be collected?

The OIGMIS username and date/time of successful login is recorded. OIGMIS also logs user activity including the username, and the date/time records were created or modified.

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

Yes, one contractor has authorized access to OIGMIS.

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?

Logical access controls have been implemented to prevent misuse of data (i.e., unique username and password requirements). OIGMIS logs user activity

including the username and the date/time records were created or modified. Access logs are reviewed by the system administrators and Subsystem ISSOs for anomalies. Attempts to access the OIGMIS by unauthorized users and attempts by OIGMIS users to access databases for which they are not authorized are logged as security events.

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

Yes, FIPS 140-2 compliant encryption and the other required FISMA security controls have been implemented.

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

FY19 Q3 Periodic System Cybersecurity Assessment PSCA) Report on May 13, 2019. This PSCA was for Public Meeting Feedback System (PMFS), Drupal Web Content Management System (DWCMS), Replacement Reactor Program System (RRPS), Office of the Inspector General Management Information System (OIGMIS)

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

System Name: Office of the Inspector General Management Information System (OIGMIS)

Submitting Office: Office of the Inspector General

A. PRIVACY ACT APPLICABILITY REVIEW

____ Privacy Act is not applicable.

_X_ Privacy Act is applicable.

Comments:
OIGMIS maintains personally identifiable information. The OIGMIS meets the criteria for a Privacy Act system of records and is currently covered under NRC's Privacy Act System of Records, NRC-18, Office of the Inspector General (OIG) Investigative Records.

Reviewer's Name	Title	Date
Sally A. Hardy	Privacy Officer	06/19/2020

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

_X_ No OMB clearance is needed.

____ OMB clearance is needed.

____ Currently has OMB Clearance. Clearance No.____

Comments:
The Inspector General Empowerment Act of 2016 states that "Subchapter I of chapter 35 of title 44, United States Code (Federal Information Policy), shall not apply to the collection of information during the conduct of an audit, investigation, inspection, evaluation, or other review conducted by the Council of the Inspectors General on Integrity and Efficiency or any Office of Inspector General, including any Office of Special Inspector General.''.

Reviewer's Name	Title	Date
David Cullison	Agency Clearance Officer	5/29/20

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	Date
Marna B. Dove	Sr. Program Analyst, Electronic Records Manager	6/22/2020

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 June 26, 2020

Clarissa L Evans Brown, Chief
Computer Security Branch
Governance & Enterprise Management
Services Division
Office of the Chief Information Officer

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

TO: **Office of the Inspector General**	
Name of System: **Office of the Inspector General Management Information System (OIGMIS)**	
Date CSB received PIA for review: **May 28, 2020**	Date CSB completed PIA review: **06/23/2020**
Noted Issues:	
Clarissa L Evans Brown, Chief Computer Security Branch Governance & Enterprise Management Services Division Office of the Chief Information Officer	Signature/Date: **/RA/ June 26, 2020**
Copies of this PIA will be provided to: *Tom Ashley, Director* *IT Services Development & Operation Division* *Office of the Chief Information Officer* *Jonathan Feibus* *Chief Information Security Officer (CISO)* *Governance & Enterprise Management Services Division* *Office of the Chief Information Officer*	