

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.

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.

NSIR Federal Information Security Management Act (FISMA) System (NFS)

Date: March 1, 2023.

A. GENERAL SYSTEM INFORMATION

1. Provide a detailed description of the system:

NFS is owned and managed by the Office of Nuclear Security and Incident Response (NSIR). NFS relies upon the agency Information Technology Infrastructure (ITI) network for enterprise cybersecurity and IT services, including managing the workstations used to support NFS components. Under an existing service level agreement (SLA), NFS receives continuous visibility of services and inherits enterprise cybersecurity controls from this relationship.

2. What agency function does it support?

The NSIR FISMA boundary includes the systems required to ensure the physical safety and security of agency facilities. The systems operate under U.S. NRC Privacy Act systems of records NRC-39, "Personnel Security Files and Associated Records," NRC-40, "Facility Security Access Controls Records," and NRC-45, "Digital Certificates for Personal Identity Verification Records." The systems in the NSIR FISMA boundary are support-systems and do not directly drive the agency mission. They ensure the physical safety and security of personnel, property, information, infrastructure, and assets.

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

The NFS FISMA boundary includes the following subsystems and components:

1) Criminal History System (CH): Licensees use the criminal history system to request criminal history background checks from the Federal Bureau of Investigation (FBI).

2) Operations Center Information Management System: (OCIMS): is comprised of the following components:

Data Component

Incident Response Management System (IRMS) – facilitates the creation of all documents and briefing materials used during incidence response in the NRC Operations Center.

Headquarters Operations Officer (HOO) system – used for managing information pertaining to the daily operational status of nuclear facilities and nuclear events. Includes the following modules:

- **HOO Event Database** – log of events reported by licensees under the Code of Federal Regulations (CFR) Parts 50 and 73. Also maintains a list of NRC personnel to be contacted in case of an emergency.
- **HOO Logbook** – daily log of HOO activities.
- **RAMQC** – tracks the transportation of radioactive materials with significant levels of consequence.

Geographic Information System (GIS) – commercial off the shelf (COTS) application used to provide maps and population information.

Protected Web Server (PWS) system – log of suspicious activity reported to the HOO by the licensees under CFR 10 part 73.125 or other law enforcement officials. This information is distributed through a website to authorized users, including NRC employees, licensees, federal agencies, and law enforcement agencies.

Government-supplied utilities (e.g., Aloha, Cameo, ERAD, Hurrevac, Marplot, RASCAL, and MATLABS) (scientific code).

Display Component – displays information on monitors in the Headquarters Operations Center (HOC).

- Display controllers.
- Display switches.
- Display monitors.
- Paging system.
- Audio Conferencing.
- Video conferencing.
- Cable TV.

Voice Component – used for voice communications in the HOC.

- Private branch exchange (PBX).
- Voice Conferencing system.
- Digital recorders.

- Automatic Notification System (ANS).
- Emergency Telecommunications System (ETS) phones.
- Iridium phones.

This Privacy Impact Assessment will focus on the modules that contain privacy related data which are:

- **HOO Event Database** (Emergency Contacts).
- **PWS** (Personally Identifiable Information (PII) related to Suspicious Activity).
- **ANS** (Emergency Contacts).
- **Voice Conferencing System** (Emergency Contacts).

3) Emergency Response Data System (ERDS): is to provide emergency responders with real-time environmental and operational conditions of U.S. nuclear power plants. This information includes current weather conditions, various plant metrics, and operational statuses. If an incident occurs, this information can be used to help predict the possible impact of an emergency at one of the sites. ERDS supports the NRC's role in assessing the overall adequacy of the licensee actions and makes recommendations for mitigating the consequences of accidents to protect the public. The NRC's role in protecting the health and safety of the public requires access to certain data from plants during emergencies that are as timely and accurate as it is to the licensee.

a. Provide ADAMS ML numbers for all Privacy Impact Assessments or Privacy Threshold Analysis for each subsystem.

CH: ADAMS ML19253A041, ML16229A481.

OCIMS: ADAMS ML20063L302, ML16020A286.

ERDS: ADAMS MLML19183A474.

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

The systems in the NFS FISMA Boundary are authorized through several legal authorities:

CH:

- 10 CFR parts 10, 11, 14, 25, 50, 73, 95.
- 42 United States Code (U.S.C.) 2011 et seq.
- 42 U.S.C. 2165 and 2201(i).
- 42 U.S.C. 2165–2169, 2201, 2201a, and 2284 et seq.
- 42 U.S.C. 5801 et seq.
- 44 U.S.C. 3501, 3504, and 3541.
- 44 U.S.C. 36.

- 5 CFR parts 731, 732.
- 5 U.S.C. 301E-Government Act of 2002 (Pub. L. 107-347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803).
- Electronic Government Act of 2002, 44 U.S.C. 36.
- Executive Order 10450, as amended.
- Executive Order 10865, as amended.
- Executive Order 13462, as amended by Executive Order 13516.
- Executive Order 13467.
- Executive Order 13526.
- Executive Order 9397, as amended by Executive Order 13478.
- Federal Information Security Management Act of 2002 (Pub. L. 107-296, Sec. 3544).
- Homeland Security Presidential Directive 12 (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004.
- Interagency security committee standards "Physical Security Criteria for Federal Facilities," April 2010.
- Office of Management and Budget (OMB) Circular No. A-130, Revised.

OCIMS:

- **HOO Event Database** – Federal Register: 44 U.S.C. 3101, 3301; Executive Order (E.O.) 9397, as amended by E.O. 13478; and E.O. 12656.
- **ANS** – Federal Register: 44 U.S.C. 3101, 3301; E.O. 9397, as amended by E.O. 13478; and E.O. 12656.
- **Voice Conferencing System** – Federal Register: 44 U.S.C. 3101, 3301; E.O. 9397, as amended by E.O. 13478; and E.O. 12656.
- **PWS** – The Enhanced Weapons rule (10 CFR part 73.1215 requires the reporting of any suspicious activity to the HOC).

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

The purpose of the systems in the NSIR FISMA boundary, and for the data they maintain, is to ensure the physical safety and security of personnel, property, information, infrastructure, and assets.

6. Points of Contact:

Project Manager	Office/Division/Branch	Telephone
Dan Warner	NSIR/DPCP/CSB	301-287-3642
Technical Project Manager	Office/Division/Branch	Telephone
CH: Dan Warner	NSIR/DPCP/CSB	301-287-3642
OCIMS: Omar Khan	NSIR/DPR/OB	301-287-3725
PWS: Nick Ballam	NSIR/DSO/ISB	301-415-1504
ERDS: Bezakulu Alemu	NSIR/DPR/OB	301-287-3731
ISSO	Office/Division/Branch	Telephone
NFS: Dan Warner	NSIR/DPCP/CSB	301-287-3642
OCIMS: Omar Khan	NSIR/DPR/OB	301-287-3725
ERDS: Beza Alemu	NSIR/DPR/OB	301-287-3731
System Owner/User	Office/Division/Branch	Telephone
Mirela Gavrilas	NSIR	301-415-1270

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
 Other

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

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

Yes, ML21127A213.

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

Updated to combine ERDS, OCIMS, and CH under the NFS boundary.

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

YES.

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

EA Number 20210002.

- 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?**

CH: Yes.

OCIMS: has four modules that contain information about individuals:

- **HOO Event Database** (Emergency Contacts)
- **PWS** (PII related to Suspicious Activity)
- **ANS** (Emergency Contacts)
- **Voice Conferencing System** (Emergency Contacts)

ERDS: N/A.

- (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.)).**

CH: The criminal history system has information about applicants in the criminal history program.

OCIMS:

- **HOO Event Database** – Contains emergency contact information for NRC Employees and contractors for OCIMS.
- **PWS** – Contains information about people involved in suspicious activity (general public) as well as names and contact information for licensees or law enforcement officials that report the incidents to the NRC.
- **Voice Conferencing System**– Contains emergency contact information for NRC Employees and contractors for OCIMS.
- **ANS**– Contains emergency contact information for NRC Employees and contractors for OCIMS.

ERDS: N/A.

(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)?**

CH: The criminal history system has information about applicants' names, addresses, dates of birth, places of birth, social security numbers, citizenships, fingerprints, and criminal history records.

OCIMS:

- **HOO Event Database** – Contains emergency contact information (name and office, cell and home phone numbers) for NRC Employees and contractors for OCIMS.
- **PWS** – Contains the name, address, phone number, license plate number, Vehicle Identification Number (VIN), passport number of people involved in suspicious activity as reported by the licensee or law enforcement official. Not every report has PII, and not every report has all of the fields described above. In all instances, suspicious incidents will never contain SSNs. PWS also contains the name and phone number of the licensee or law enforcement official that reported the incident to the NRC.
- **Voice Conferencing System** – Contains emergency contact information (name and office, cell and home phone numbers) for NRC Employees and contractors for OCIMS.
- **ANS** – Contains emergency contact information (name and office, cell and home phone numbers) for NRC Employees and contractors for OCIMS.

ERDS: N/A.

c. Is information being collected from the subject individual?

CH: No. The information is collected and submitted by the electronic submissions from NRC Licensees (EIE “Submissions”) for criminal history checks performed by the FBI for personnel requesting unrestricted access at nuclear facilities (i.e. Applicants).

OCIMS:

- **HOO Event Database** – Yes, the NRC collects the contact information of emergency response personnel.
- **PWS** – No. The NRC does not collect information directly from the subject individual. The NRC only receives information as reported by the licensee or law enforcement official.
- **Voice Conferencing System** - No. The information is transferred from the HOO Event Database.
- **ANS** – No. The information is transferred from the HOO Event Database.

ERDS: N/A

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

OCIMS:

- **HOO Event Database** – Name and office, cell, and home phone numbers.

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

CH: Yes. Licensees use the CH system to request criminal history background checks from the FBI. The Licensees collect this information from the individuals directly then submit it, not the NRC staff.

OCIMS:

- **HOO Event Database** – Yes. Contractors supporting ERDS, OCIMS, and PWS.
- **ANS** – Yes. Contractors supporting ERDS, OCIMS, and PWS.
- **Voice Conferencing System** – Yes. Contractors supporting ERDS, OCIMS, and PWS.
- **PWS** – Yes. However, the NRC does not collect information directly from the subject individual. The NRC only receives information as reported by the licensee or law enforcement official.

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

YES.

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

CH: Yes.

OMB control number 3150-0002(Part 73)**OCIMS:**

• **PWS:**

- OMB 3150-0219
- The NRC has the legal authority to share this information with the FBI under Section 221.b. of the Atomic Energy Act, codified at 42 U.S. Code 2271

ERDS: N/A.

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

CH: No.

OCIMS

- **HOO Event Database** – No. The information is collected directly from the individual.
- **ANS** – Yes. Information is transferred from the HOO Event Database.
- **Voice Conferencing System** – Yes. Information is transferred from the HOO Event Database.
- **PWS** – No. Information is collected as reported by the licensee or law enforcement official.

ERDS: N/A

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

CH: N/A.

OCIMS:

- **ANS** – ANS receives information from the HOO Event Database.
- **Voice Conferencing System** – The Voice Conferencing System receives information from the HOO Event Database.

ERDS: N/A.

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

CH: Yes.

OCIMS:

- **HOO Event Database** – No.
- **ANS** – No.
- **Voice Conferencing System** – No.
- **PWS** – Yes.

ERDS: N/A.

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

CH: Licensees. (see B.1.b).

OCIMS:

- **PWS** – The licensee or law enforcement official reporting the suspicious incident. They report their name and phone number as well as information about individuals involved in the suspicious incident as described above in section B.1.b. For example, information may relate to identifying an individual or vehicle involved in a suspicious incident, such as: name, address, date of birth, vehicle make and model, license plate, Vehicle Identification Number, etc.

ERDS: N/A.

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

CH: The NRC does not verify the accuracy of the information. The operators of the criminal history system rely on the third parties that collected the information to verify the accuracy and completeness of the information.

OCIMS

- **HOO Event Database** – The HOO collects the information directly from the subject individuals and verifies it with them.
- **ANS** – The HOO transfers the information from the HOO Event Database.
- **Voice Conferencing System** – The HOO transfers the information from the HOO Event Database.

- **PWS** – The NRC does not verify or investigate any of the information. They simply record it as reported by the licensee or law enforcement official.

ERDS: N/A.

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

CH: Data transfer.

OCIMS:

- **HOO Event Database** – The HOO collects the information directly from the subject individual.
- **ANS** – Data transfer from the HOO Event Database.
- **Voice Conferencing System** – Data transfer from the HOO Event Database.
- **PWS** – The NRC receives information as reported by the licensee or law enforcement official over the phone.

ERDS: N/A.

2. INFORMATION NOT ABOUT INDIVIDUALS

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

CH: No.

OCIMS:

- **HOO Event Database** –Yes.
- **ANS** – Yes.
- **Voice Conferencing System** – Yes.
- **PWS** – Yes.

ERDS: N/A.

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

OCIMS:

- **HOO Event Database** –The system is a repository of reports of reactor events, materials events, and information pertaining to the daily operational status of nuclear facilities. It also includes emergency contact information for responders.
- **ANS** – N/A.
- **Voice Conferencing System** – N/A.
- **PWS** - The system contains reports of suspicious activity occurring at NRC licensed facilities throughout the United

States as reported by licensees. Suspicious activity reports may contain other sensitive but unclassified information about the facility, security posture, security countermeasures, and other potential vulnerabilities. In addition, it reposts unclassified security bulletins from the FBI, Department of Homeland Security (DHS), and alerts from the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and the United States Computer Emergency Readiness Team (US-CERT). PWS also reposts NRC information notices, security advisories, and bulletins.

ERDS: N/A.

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

CH: N/A.

OCIMS:

- **HOO Event Database** –External NRC licensees provide reports of reactor events, materials events and information pertaining to the daily operational status of nuclear facilities. Emergency contact information is provided directly from the individual.
- **ANS** – Internal transferred from the HOO Event Database.
- **Voice Conferencing System** – Internal transferred from the HOO Event Database.
- **PWS** – As provided in 10 CFR part 73.1215 suspicious information is provided via email, phone, or fax from external agencies and licensees. The information is received and entered into the system by the HOO. The communications documents originate from NRC, FBI, DHS, ICS-CERT, and US-CERT.

ERDS: 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.

CH:

The FBI uses the information the licensees obtain from personnel through the criminal history system to conduct criminal history background checks. The licensees use the information the FBI passes back to them through the criminal history system to assess personnel.

OCIMS:

- **HOO Event Database** – The purpose of the emergency contact information is to alert personnel in the event of an emergency. This line of communication aids the NRC in their ability to respond effectively to emergency situations.
- **ANS** - The purpose of the emergency contact information is to alert personnel in the event of an emergency.
- **Voice Conferencing System** - The purpose of the emergency contact information is to alert personnel in the event of an emergency.
- **PWS** – This information is collected to help ensure the security of NRC licensed nuclear facilities.

ERDS: N/A

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

CH: Yes.

OCIMS:

- **HOO Event Database** – Yes.
- **ANS** – Yes.
- **Voice Conferencing System** –Yes.
- **PWS** –Yes.

ERDS: N/A.

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

CH:

The administrators of the criminal history system protect the privacy rights of the individuals whose information is held and transferred by the criminal history system. They sign a “notification of responsibilities regarding the use, disclosure, and protection of privacy act information.”

The information is protected under:

- Privacy Act Systems of Records,
- SORN NRC-39, “Personnel Security Files and Associated Records.”

OCIMS:

- **HOO Event Database** – NSIR staff and management will ensure the proper use of the information.
- **ANS** – NSIR staff and management will ensure the proper use of the information.
- **Voice Conferencing System** – NSIR staff and management will ensure the proper use of the information.
- **PWS** – NSIR staff and management will ensure the proper use of the information at the NRC. PWS administrators will limit access to users based on role and need to know. Users are also required to accept terms of service before being granted an account in PWS. The NRC will not be able to ensure proper use of information by external users beyond limiting access based on need to know. Access to PII and other sensitive but unclassified information is limited to selected individuals within the NRC and FBI and is redacted for all other PWS users. The only searchable fields for suspicious incidents are as follows: incident ID, date, region, reporting organization, site/licensee name, report category, current phase, status and last updated (date). SSNs are no longer captured in suspicious incidents and all existing SSNs have been purged from the system. In order to avoid any potential issues with searching on PII, the full-text search feature is limited to the Communication Documents and Cyber Related Documents Views.

ERDS: N/A.

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

CH: Yes. The administrators of the criminal history system protect the privacy rights of the individuals whose information is held and transferred by the criminal history system. They sign a “notification of responsibilities regarding the use, disclosure, and protection of privacy act information.”

The information is protected under:

- Privacy Act Systems of Records,
- SORN NRC-39, “Personnel Security Files and Associated Records.”

OCIMS:

- **HOO Event Database** – Yes, a data dictionary of the HOO Event Database exists.
- **ANS** – Yes, the data elements are documented.
- **Voice Conferencing System** – Yes, the data elements are documented.
- **PWS** – Yes, a data dictionary of the PWS.

ERDS: N/A.

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

CH:

The NFS Security Categorization Report (ADAMS accession number ML TBD, version 1.1, October 14, 2021) describes the data elements of the systems in the NFS FISMA boundary.

OCIMS:

The HOO Event Database data dictionary is located within the Operations Center Information Management System (OCIMS) documentation. The ANS and Voice Conferencing System are documented in manuals located within the OCIMS documentation.

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

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).

CH: No.

OCIMS:

- **HOO Event Database** – No.
- **ANS** – No.
- **Voice Conferencing System** – No.
- **PWS** – No.

ERDS: N/A.

- a. **If yes, how will aggregated data be maintained, filed, and utilized?**
N/A.
- b. **How will aggregated data be validated for relevance and accuracy?**
N/A.
- c. **If data are consolidated, what *controls* protect it from unauthorized access, use, or modification?**
N/A.

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.

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

CH:

Information about individuals is not retrievable by any personal identifier in the criminal history system.

OCIMS:

- **HOO Event Database** – The information can be accessed through Microsoft Access forms, using the name of the emergency contact person.
- **ANS** – The information can be accessed from the ANS client program by the name of the emergency contact person. The system is used to make phone calls to individuals on call lists to alert them of emergencies.
- **Voice Conferencing System** – The information can be accessed from the Voice Conferencing System client. The information is stored in emergency call lists. The system is used to make phone calls to individuals on call lists to alert them of emergencies.
- **PWS** – By default, the records are sorted by last update. The only searchable fields for Suspicious Incidents are as follows: incident ID, date, region, reporting organization, site/licensee name, report category, current phase, status, and last updated (date). In order to avoid any potential issues with search on PII, the full-text search feature is limited to the Communication Documents and Cyber Related Documents Views.

ERDS: Does not maintain information about individuals

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

CH: Yes.

OCIMS: Yes.

ERDS: N/A.

a. **If “Yes,” provide name of SORN and location in the Federal Register.**

CH:

- Privacy Act Systems of Records,
- SORN NRC-39, “Personnel Security Files and Associated Records.”

OCIMS

- NRC-2019-0191 Employee Locator Records—NRC 36.
<https://www.govinfo.gov/content/pkg/FR-2019-12-27/pdf/2019-27584.pdf>

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

N/A.

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

CH: No. This system is used to submit and receive electronic submissions (criminal history check) to a reporting agency by licensees for personnel requesting unrestricted access at nuclear facilities (i.e. Applicants).

OCIMS:

- **HOO Event Database** – No. The system is used to call individuals in case of an emergency.
- **ANS** – No. The system is used to call individuals in case of an emergency.
- **Voice Conferencing System** – No. The system is used to call individuals in case of an emergency.
- **PWS** – Yes. The system will sometimes provide the identity and address of an individual. However, the NRC does not monitor or investigate any individuals who have been involved in suspicious incidents. The data is reported to the NRC and recorded in the database. It is used for analysis purposes and eventually passed on to other agencies for further processing.

ERDS: N/A.

a. **If yes, explain.**

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

CH: N/A.

OCIMS:

- **HOO Event Database** – Access to contact information is limited to authorized Headquarters Operations Officers.
- **ANS** – Access to contact information is limited to authorized Headquarters Operations Officers.
- **Voice Conferencing System** – Access to contact information is limited to authorized Headquarters Operations Officers.
- **PWS** – Access to non-redacted information is limited to authorized NRC users and the FBI.

ERDS: N/A.

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

CH:

- Criminal history billing report.

OCIMS:

- **HOO Event Database** – Emergency Contact Call Lists.
- **ANS** – List of emergency responders successfully or unsuccessfully contacted.
- **Voice Conferencing System** – None.
- **PWS** – Quarterly reports are produced showing the number of users who have an account on PWS from a variety of user groups. It also indicates the total number of times PWS was accessed for that quarter. No PII is present in these reports.

ERDS: N/A.

a. **What are the reports used for?**

CH: Produce invoices for licensees.

OCIMS:

- **HOO Event Database** – Hard copy of emergency call lists in case database is not available.
- **ANS** – Determine who is reporting to the Operation Center to

ensure the Operations Center is fully staffed.

- **Voice Conferencing System** – N/A.
- **PWS** – These reports are used to assess how large our user base is, how many users have joined the system in the last quarter, and how often the system is being accessed.

ERDS: N/A.

b. Who has access to these reports?

CH: Access to the reports in the criminal history system is limited to authorized users. Persons must have a need-to-know to become authorized users and they can only access reports appropriate for their job responsibility. They undergo a rigorous background screening process and their need-to-know and access privileges are reviewed yearly.

OCIMS:

- **HOO Event Database** – Authorized NSIR users.
- **ANS** - Authorized NSIR users.
- **Voice Conferencing System** – N/A.
- **PWS** – Authorized NSIR users.

D. ACCESS TO DATA

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

CH:

- Office of Nuclear Security and Incident Response, Division of Physical & Cyber Security Policy, Reactor Security,
- Office of Chief Information Officer, IT Services Development and Operations Division.

OCIMS:

- **HOO Event Database** – Authorized NSIR Personnel (HOOs).
- **ANS** - Authorized NSIR Personnel (HOOs).
- **Voice Conferencing System** - Authorized NSIR Personnel (HOOs).
- **PWS** – Authorized NRC Personnel (NSIR, Office of Enforcement, Office of Investigations, NRR, NRO, NMSS, and personnel from other offices who have a business need).

ERDS: N/A.

(1) For what purpose?

CH:

The Office of Nuclear Security and Incident Response, Reactor Security Branch operates the criminal history system.

The Office of Chief Information Officer, IT Services Development and Operations Division maintains the infrastructure on which the criminal history system operates.

OCIMS:

- **HOO Event Database** – To rapidly inform emergency responders.
- **ANS** - To rapidly inform emergency responders.
- **Voice Conferencing System** - To rapidly inform emergency responders.
- **PWS** – Viewing, entering, and tracking status of reports on potential security threats to nuclear facilities.

ERDS: N/A.

(2) Will access be limited?

CH: Yes.

OCIMS:

- **HOO Event Database** – Yes.
- **ANS** – Yes.
- **Voice Conferencing System** – Yes.
- **PWS** – Yes.

ERDS: - N/A.

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

CH: No. Although the EIE system sends the submission information from the licensees to the criminal history system, it does not have access to the data because it is encrypted.

OCIMS: Yes.

ERDS: N/A.

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

CH: - No.

OCIMS:

- **HOO Event Database** – ANS and Voice Conferencing System.
- **ANS** – No.
- **Voice Conferencing System** – No.
- **PWS** – No.

ERDS: N/A.

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

CH: No.

OCIMS:

- **HOO Event Database** – Transmitted electronically to ANS and Voice Conferencing systems. Not disclosed.
- **ANS** – Not transmitted or disclosed.
- **Voice Conferencing System** – Not transmitted or disclosed.
- **PWS** – It is viewed through a Web portal. It can also be exported to PDF.

ERDS: N/A.

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

CH: No.

OCIMS:

- **HOO Event Database** – No.
- **ANS** – No.
- **Voice Conferencing System** – No.
- **PWS** – Yes.

ERDS: N/A.

(1) **If yes, who?**

CH: N/A.

OCIMS:

- **HOO Event Database** – N/A.
- **ANS** – No.

- **Voice Conferencing System** – N/A.
- **PWS** – Authorized licensees, other Federal Agencies such as DHS and FBI, and state and local Law Enforcement personnel.

ERDS: N/A.

(2) **Will access be limited?**

CH: N/A.

OCIMS: Yes.

ERDS: N/A.

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

CH: The Office of Nuclear Security and Incident Response, Reactor Security Branch operates the criminal history system.

The Office of Chief Information Officer, IT Services Development and Operations Division maintains the infrastructure on which the criminal history system operates.

OCIMS:

- **HOO Event Database** – To rapidly inform emergency responders.
- **ANS** - To rapidly inform emergency responders.
- **Voice Conferencing System** - To rapidly inform emergency responders.
- **PWS** – Viewing, entering, and tracking status of reports on potential security threats to nuclear facilities.

ERDS: N/A.

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

CH: N/A.

OCIMS:

- **HOO Event Database** – N/A.
- **ANS** – N/A.
- **Voice Conferencing System** – N/A.
- **PWS** – Threat information is made available via a Web portal. It can also be exported to PDF.

ERDS: - 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 \(GRS\)](#)?**

CH: Yes.

OCIMS:

- **HOO Event Database** – Yes.
- **ANS** – Yes.
- **Voice Conferencing System** – Yes.
- **PWS** – No.

ERDS: Yes.

- 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?**

CH:

- [GRS 5.6](#) item 180: Records of personnel security and access clearance records. Records of people not issued clearances. **Temporary:** Destroy **1 year** after consideration of the candidate ends, but longer retention is authorized if required for business use. **BASED ON NRC SORN:** According to Section E2 of PIA dated 7/26/2018, this system retains submission records for **30 days**.

- [GRS 5.6](#) item 181: Records of personnel security and access clearance records.
Temporary: Destroy **5 years** after employee or contractor relationship ends, but longer retention is authorized if required for business use. According to Section E2 of PIA dated 7/26/2018, this system retains submission records for **30 days**.

OCIMS:

- [GRS 3.2](#) ITEM 020 – Computer security incident, handling, reporting and follow-up records;
Temporary. Destroy **3 years** after all necessary follow-up actions have been completed, but longer retention is authorized if required for business use. This applies to incidents related to computer security only.
- [N1-431-08-20](#) approved ~~September 12, 2008~~ September 11, 2014, covers HOO Event Database, ANS. PWS is not covered in this retention schedule.

Differing retentions exist (permanent and temporary) for items in the records schedule:

HOO – Permanent and Temporary

- Events Master File, N1-431-08-20 item A.1.b.i;
Permanent: Cut off at the end of the calendar year. Transfer files to the National Archives 10 years after cutoff according to NARA guidance in 36 CFR 1228.270. Transfer to NARA in 5-year blocks when the oldest record is 15 years old.
- HOO Log, N1-431-08-20 item A.1.b.iii;
Temporary: Cut off information accumulated during the year at the end of the fiscal year. Destroy/delete 10 years after cutoff.
- HOOdb Outputs Reports, N1-431-08-20, item A.1.c;
Temporary: Cut off and destroy/delete when no longer needed for business purposes.

ANS – Temporary

- ANS Master File, N1-431-08-20 item A.3.b;
Temporary: Delete when superseded.

ERDS:

- [N1-431-08-11](#), approved September 6, 2012
- ERDS Master File, N1-431-08-11 item 2a, Data Collected During an Alert or Event;
Temporary: Cut off upon termination of the license (following the completion of the decommissioning procedure) for the nuclear power plant covered by the Event. Destroy 20 years after cutoff.

- ERDS System Operations Records, N1-431-08-11 item 3.a;
Temporary: Cut off at end of calendar year. Destroy 5 years after cutoff.
- Data Printouts from ERDS Data File, N1-431-08-11, item 4.a;
Temporary: Delete or destroy when no longer needed for analysis or other business reason.
- NRC Report or Analysis of the Event, N1-431-08-11 item 4.b;
Permanent: Cut off at end of Calendar Year of last action and file in ADAMS. Transfer to the legal custody of the National Archives 20 years after cut off and destroy the NRC copy of the files after receiving notification that the transfer to NARA was successful.

VOICE CONFERENCING SYSTEM:

- Employee emergency contact information, [GRS 5.3](#) item 020;
Temporary: Destroy when superseded or obsolete, or upon separation or transfer of employee.

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).

CH: Access to the systems in the NFS boundary is controlled by PIV card authentications, both to the network infrastructure and to the individual system applications. It, along with Role-Based Access Controls (RBAC), ensures only authorized persons can access data, and only data they need to conduct their job duties.

OCIMS:

- **HOO Event Database** – The database requires a username and password in order to access the system. The database can only be accessed by users with access to OCIMS.
- **ANS** – Authorized users are given a username and password.
- **Voice Conferencing System** – Authorized users are given a username and password. The application can only be accessed through client software installed on a limited number of workstations.
- **PWS** – Authorized users are given a username and password to access the Web portal. The web portal has a Secure Socket Layer (SSL) Certificate installed that provides encryption as well as authentication for PWS.

ERDS:

- ERDS requires a username and password in order to access the system.

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

CH: All system transactions are tied to a specific, unique person's identity by strict identification and authentication protocols. The system logs all user activities.

OCIMS:

- **HOO Event Database** – The HOO Event Database is located in the Ops Center, and only available to authorized users on authorized machines.
- **ANS** – ANS is located in the Ops Center, and only available to authorized users on authorized machines.
- **Voice Conferencing System** - The Video Conferencing System is located in the Ops Center, and only available to authorized users on authorized machines.
- **PWS** – Users need to have an authorized account to log in. Access requests are processed by NSIR threat assessment personnel. Approval is based on the applicant's affiliation, role within their organization, and a need-to-know.

ERDS:

- All system transactions are tied to a specific, unique person's identity by strict identification and authentication protocols. The system logs all user activities.

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

CH: Yes.

OCIMS: Yes.

ERDS: Yes.

(1) If yes, where?

CH:

The criteria, procedures, controls, and responsibilities regarding access to the system are documented:

- NFS Security Policies and Procedures (SPP), (ADAMS accession number: ML#TBD), version 1.0, April 09, 2021.
- NFS System Security Plan, (RCATS Workflow #449296), September 12, 2022.

The documents are reviewed yearly.

OCIMS:

- **HOO Event Database** – HOO procedures as well as system and administration guides.
- **ANS** – HOO procedures as well as system and administration guides.
- **Voice Conferencing System** - HOO procedures as well as system and administration guides.
- **PWS** – System and administration guides.

ERDS:

- ERDS procedures as well as system and administration guide.

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

CH: Yes.

OCIMS: Yes.

ERDS: Yes.

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

CH: All persons in the same role go through the same training, sign the same agreements, have the same access restrictions, and are subject to the same oversight independent of their physical location.

OCIMS:

- **HOO Event Database** – Data is replicated between HQ and Region 4.
- **ANS** – Data is transferred from the HOO Event Database.
- **Voice Conferencing system** – Data is transferred from the HOO Event Database.
- **PWS** – Data is replicated between HQ and Region 4.

ERDS:

- Data is replicated between HQ and Region 4.

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

CH:

- Application Administrators,
- Server Administrators.

OCIMS:

- **HOO Event Database** – System administrators and users.
- **ANS** – System administrators and users.
- **Voice Conferencing system** – System administrators and users.
- **PWS** - System administrators and users.

ERDS:

- System administrators and users.

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

CH: Yes.

OCIMS:

- **HOO Event Database** – No.
- **ANS** – No.
- **Voice Conferencing system** – No.
- **PWS** – Yes.

ERDS: - No.

a. If yes, what will be collected?

CH: All operator transactions are logged within the system. Audit logs are generated for all transactions and security events.

OCIMS:

- **HOO Event Database** – N/A.
- **ANS** – N/A.
- **Voice Conferencing system** – N/A.
- **PWS** - Login statistics.

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?

CH: Has role-based restrictions, and persons with access privileges have undergone personnel security screening. These persons undergo mandatory user awareness, role-based cybersecurity, and PII training related to their role on the information system. Data is safeguarded in transmission using encryption and access controlled private virtual networks. The information system security officers receive audit logs daily.

OCIMS:

- **HOO Event Database** – Review of system logs.
- **ANS** – Review of system logs.
- **Voice Conferencing system** – Review of system logs.
- **PWS** - Review of system logs, SSL Certificate / Encryption.

ERDS: - Review of system logs.

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

CH: Yes.

OCIMS:

- **HOO Event Database** – Yes.
- **ANS** – Yes.
- **Voice Conferencing System** – Yes.
- **PWS** - Yes.

ERDS: Yes.

a. If yes, when was Assessment and Authorization last completed? And what FISMA system is this part of?

CH: Subsystem of NFS,

FY14 ACCESS Authority to Operate – April 17, 2014, ML14070A318.

OCIMS: Subsystem of NFS,

- **HOO Event Database** – October 31, 2013.
- **ANS** – October 31, 2013.

- **Voice Conferencing System** - October 31, 2013.
- **PWS** - October 31, 2013.

ERDS: Subsystem of NFS,

August 28, 2012.

- b. **If no, is the Assessment and Authorization 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: NSIR FISMA System (NFS).

Submitting Office: Office of Nuclear Security and Incident Response (NSIR)

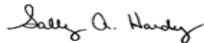
A. PRIVACY ACT APPLICABILITY REVIEW

Privacy Act is not applicable.

Privacy Act is applicable.

Comments:

Criminal History is cover by NRC's Privacy Act system of records NRC-39, Personnel Security Files and Associated Records. OCIMS does maintain personally identifiable information in the HOO, ANS, Voice Conferencing System, of these subsystems, only the HOO, ANS, and Voice Conferencing System is retrieved by an individual's name to contact the individual regarding matters of official business. NRC maintains this information as part of NRC's Privacy Act system of records, NRC-36, "Employee Locator Records." NRC does not retrieve information from PWS by use of an individual's name or other personal identifier. And ERDS does not maintain information about individuals.

Reviewer's Name	Title
 Signed by Hardy, Sally on 04/19/23	Privacy Officer

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION


No OMB clearance is needed.

OMB clearance is needed.

Currently has OMB Clearance. Clearance No.PWS (3150-0219), Part 73 (3150-0002)

Comments:

The clearances listed above are not all inclusive since information collections by the HOO are required by CFR parts not in this PIA.


Reviewer's Name	Title
 Signed by Cullison, David on 04/18/23	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.
- Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:


Additional information/data/records kept in this system may need to be scheduled; 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 04/18/23	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.
- 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 Harris, Kathryn
on 04/25/23

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: Mirela Gavrilas, Director, Office of Nuclear Security and Incident Response	
Name of System: NSIR FISMA System (NFS).	
Date CSB received PIA for review: March 1, 2023	Date CSB completed PIA review: April 19, 2023
Noted Issues: 	
Chief Cyber Security Branch Governance and Enterprise Management Services Division Office of the Chief Information Officer	Signature/Date:  Signed by Harris, Kathryn on 04/25/23 ture:
<p><i>Copies of this PIA will be provided to:</i></p> <p><i>Gwen Hayden Acting Director IT Services Development and Operations Division Office of the Chief Information Officer</i></p> <p><i>Garo Nalabandian Chief Information Security Officer (CISO) Office of the Chief Information Officer</i></p>	