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.

Electronic Information Exchange (EIE)

Date: October 22, 2020

A. GENERAL SYSTEM INFORMATION

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

The Electronic Information Exchange (EIE) system is the U.S. Nuclear Regulatory Commission's (NRC) main portal for authorized customer users to transmit electronic submissions in order to meet various regulatory reporting requirements. The EIE is owned by the Office of the Chief Information Officer (OCIO). The system is managed by the OCIO's Business Application Development Branch on behalf of various Information Owners, i.e. those NRC Program Offices who are responsible (over the term of the lifecycle of the maintenance of the information in NRC systems) for the proper management of the information submitted via the EIE to the NRC. The EIE thus contains a number of subsystems (Workflows), with each consisting of an automated set of business processes for the electronic receipt of a particular category of information on behalf of the Information Owners (see list at A.3.).

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

The EIE is an electronic mail service for various NRC Program Offices / Information Owners. In effect, it delivers the equivalent of certified, return receipt requested mail (i.e. digitally signed electronic submissions) to a mailbox (i.e. file folder) for pickup (i.e. read and copy to a database repository in a separate system owned by the appropriate Information Owner). The EIE does not read the mail, does not retain the mail past a purge limit, and does not control what is done with the mail by the Information Owner once it has been picked up from the Information Owner's mailbox. The EIE's only function is to provide a mechanism to securely and timely deliver electronic submittals to a location accessible by the Information Owner.

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

The EIE Workflows and their respective Information Owners are as follows: General Form (GF) Workflow - Various NRC Program Offices, to include the Office of Nuclear Reactor Regulation (NRR), the Office of Nuclear Material Safety and Safeguards, and the Office of Nuclear

Safety and Incident Response (NSIR) (to include Fitness for Duty reporting), all receive GF submissions of various regulatory reports and other documents of interest to the NRC.

Adjudicatory (ADJ), (both Public and Non-Public) Workflow - The Office of the Secretary receives ADJ submissions of discovery and evidentiary material in support of adjudicatory hearings.

Criminal History (CH) Workflow – NSIR receives attachments to CH submissions (the submission form and the related attachments are collectively a "Submission") from NRC Licensees requesting Federal Bureau of Investigation (FBI) and Department of Defense (DoD) criminal history checks on potential hires. Resultant FBI and DoD criminal history reports (collectively "CH Reports") are returned via EIE to the submitting Licensees.

Note that NSIR owns backend CH components (collectively "NSIR CH") that are used to process EIE CH submission files and communicate with the FBI and DoD. These components are outside of the EIE boundary. They are, however, an essential component of the complete criminal history check process performed by the NRC on behalf of Licensees.

- The CH Workflow contains personally identifiable information (PII) about the potential hires.

Note that this information is only retained temporarily; once the Licensee submitters have retrieved the CH Reports detailing results of the criminal history checks, the PII is deleted from the EIE system in accordance with a purge limit set by the CH Workflow Administrator (WFA).

Operator Digitized Docket (ODD) Workflow – NRR receives ODD submissions from NRC Licensees under 10 Code of Federal Regulations (CFR) Part 55 concerning various actions related to Operator Licensing (OL) Actions, e.g. license issuance). This includes registration for the Generic Fundamentals Examination (GFE), which is a condition precedent to obtaining an Operator License. NRR staff can also utilize the ODD Workflow to send Requests for Additional Information (RAI) to the individuals wishing to obtain a license (ODD Applicants).

- A GFE submission form contains PII about the individual (the Registrant) wishing to sit for the GFE.

- ODD submissions for OL Actions contain attachments with PII about the ODD Applicant. At a minimum, these include the following: NRC Form 398 Personal Qualification Statement–Licensee (NRC Form 398) and NRC Form 396 – Certification of Medical Examination by Facility Licensee (NRC Form 396).

- ODD RAI about the ODD Applicant may contain attachments with PII. For instance, the NRR could attach NRC Form 398 with questions about missing or clarifying information.

Note that this information is only retained temporarily; the PII is deleted from the EIE system upon expiration of the purge limit set by the ODD WFA.

NOTE: As described above, only the CH and ODD Workflows contain PII, therefore, the discussion in this Privacy Impact Assessment (PIA) applies to the CH and ODD Workflows ONLY.

In all instances, the EIE system only temporarily retains the PII as part of its transaction processing; there is no long-term storage of the PII within EIE.

4. What legal authority authorizes the purchase or development of this system? (*What law, regulation, or Executive Order authorizes the collection and maintenance of the information necessary to meet an official program mission or goal? NRC internal policy is not a legal authority.*)

Title 10 - Energy, Code of Federal Regulations (10 CFR):

- Part 2, Subpart C
- Part 13.26 (Program Fraud Civil Remedies)
- Part 26.11 (Fitness for Duty)
- Part 40.5 (Domestic Source Material Licensing)
- Part 50.4 (Licensing of Production and Utilization Facilities)
- Part 52.3 (Licenses, Certifications and Approvals for Nuclear Power Plants)
- Part 55 (Operators' Licenses)
- Part 70.5 (Licensing of Special Nuclear Material)
- Part 73.57 (Criminal History)
- Part 110.4 (Export and Import of Nuclear Equipment and Material)

CH Workflow
Title 10 CFR Part 73.57

ODD Workflow
Title 10 CFR Part 55

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

The U.S. NRC established the EIE system to comply with the Government Paperwork Elimination Act, Title XVII of Public Law 105-277, which requires Federal agencies to use electronic forms, electronic filing, and electronic signatures to conduct official business with the public.

The EIE system supports the NRC's mission:

- To regulate civilian use of byproduct, source, and special nuclear materials to ensure adequate protection of public health and safety;
- To promote the common defense and security; and
- To protect the environment by providing a secure method to transmit digitally signed documents pertaining to licensing actions, associated hearings, and other regulatory matters as required by 10 CFR as listed above.

CH Workflow
To comply with 10 CFR Part 73.57, which requires Licensees to submit fingerprint cards to the NRC for the purpose of processing criminal history checks of individuals requiring unescorted access to the Licensee's nuclear power facility.

ODD GFE Workflow
To comply with 10 CFR Part 55, which requires Licensees to submit certain information regarding OL Actions, to include information needed to sit for the GFE.

6. Points of Contact: (*Do not adjust or change table fields. Annotate N/A if unknown. If multiple individuals need to be added in a certain field, please add lines where necessary*.)

A non-publicly available list of EIE points of contact can be found in the ADAMS Contact LIST (ML13343A122).

Project Manager	**Office/Division/Branch**	**Telephone**
Pushpa Jayapal	OCIO/ITSDOD/ADSB	703-400-7245
Business Project Manager	**Office/Division/Branch**	**Telephone**
Mackenzie Stevens	OCIO/ITSDOD/ADSB	301-415-2718
Technical Project Manager	**Office/Division/Branch**	**Telephone**
Eugenia Shyu	OCIO/ITSDOD/ADSB	301-415-1396
Executive Sponsor	**Office/Division/Branch**	**Telephone**
Kathryn Harris	OCIO/GEMSD/CSB	301-287-0515
ISSO	**Office/Division/Branch**	**Telephone**
David Nelson	OCIO/D	301-415-8700
System Owner/User	**Office/Division/Branch**	**Telephone**
Thomas Ashley	OCIO/ITSDOD/D	301-287-0771

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

a. ____ New System

__X__ Modify Existing System

____ Other

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

Yes.

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

10/26/2018, ADAMS ascension number is ML18120A168.

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

Moved into new PIA template and updated to reflect current points of contact for the system.

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

Yes.

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

20040005.

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.

For the purpose of this PIA, the following terms are applicable:

CH Workflow
"CH Applicant" refers to any individual (Licensee employee, potential employee, or contractor) who may require unescorted access to one or more of the Licensee's nuclear facilities.

ODD GFE Workflow
"Registrant" refers to any Licensee employee who is applying to register for the GFE preparatory to application for a new Operator License. "ODD Applicant" refers to any Licensee employee who is applying for an Operator License.

1. INFORMATION ABOUT INDIVIDUALS

a. Does this system maintain information about individuals?

The system does not maintain or store information about individuals, but it does temporarily retain it until processing of a transaction is complete. Information in a Submission (an EIE form and any related attachments) is deleted from the EIE system after a WFA defined purge limit.

(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 Workflow
The CH Workflow of the EIE system processes electronic Submissions (EIE forms and related attachments) from NRC Licensees that contain PII of CH Applicants in accordance with 10 CFR Part 73.57.

Note that the maintainers of the EIE system do not read the information; it is transmitted by NSIR CH in a secure manner to the FBI and DoD who use it to conduct a criminal history check, the results of which are recorded in a file (a CH Report). This CH Report is made available, via attachment to an EIE response form (the EIE response forms and attachments are collectively "Responses"), to the Licensee who made the original Submission. Once the Response has been transmitted, the PII information is purged from the EIE system.

ODD GFE Workflow
The ODD Workflow of EIE processes Submissions (EIE forms and related attachments) relative to OL Actions in accordance with 10 CFR Part 55. The ODD Workflow may also include transmission of GFE registration forms, which contain PII of Registrants.

Note that the maintainers of the EIE system do not read the information; it is retrieved in a secure manner by the ADAMS Case Manager, a component of the ADAMS Business Process Application Stack (BPAS) architecture. The ADAMS Case Manager in turn communicates with the Replacement Reactor Program System (RRPS), which is owned by OCIO. Once the ODD information has been transmitted, the PII information is purged from the EIE system.

(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 Workflow
The Submission attachment(s) are not maintained in the EIE. As submissions are received, the attachment(s) are extracted from the EIE system by an automated process to a server owned by NSIR.

Note: Both the extraction program, which deletes the PII from the EIE system upon extraction, and the NSIR CH components are outside the EIE system.

A Submission attachment contains all or some of the following PII: applicant's name, residence, social security number, sex, height, weight, race, eye color, hair color, birthplace, birth date, scars or other identifying marks, and fingerprints.

The CH Workflow of the EIE temporarily, within a purge limit set by the CH WFA, retains Response attachment(s). The purge limit is the length of time provided for the Licensee to retrieve the Response after they have been notified that it is available (normally less than 24-48 hours).

- The Response attachment repeats all or some of the above information in addition to the results of the FBI's and DoD's criminal history checks (i.e. the CH Report) on the Applicant.

ODD GFE Workflow

GFE Registration Form - The GFE Registration forms are not maintained in the EIE system. As GFE transmissions are received, the information in the GFE forms is encrypted and written to an Extensible Markup Language (XML) file, which is temporarily stored in a folder on the EIE file system. This file is copied by a BPAS Case Manager automated process to an ADAMS BPAS server. After notification of successful processing by BPAS, the EIE system deletes the encrypted XML file.

- A GFE Registration form contains the following PII: Registrant's name and date of birth.

OL Action Submissions - The OL Action Submission (EIE form and attachments) is not maintained in EIE. As an OL Action transmission is received, the information in the form is encrypted and written to an XML file, which is temporarily stored in a folder on the EIE file system. Similarly, the attachments are encrypted and stored in the same folder. These files are copied by the BPAS Case Manager automated process to the ADAMS BPAS server. After notification of successful processing by BPAS, the EIE system deletes the encrypted XML file and encrypted attachments.

Note: Both the BPAS extraction program, which copies the PII from the EIE system and the ADAMS BPAS server, on which it resides, are outside the EIE system.

- An OL Submission contains an attached NRC Form 398 that contains the following PII: ODD Applicant's 1) name and address, 2) citizenship, 3) birth date, 6) docket number and license history, 7-9) employer's name, address and docket number, 10) current position, 11) education history, 12-14) power reactor operator training history and 15-16) work experience; and an attached NRC Form 396 that contains the ODD Applicant's name, docket number, facility, facility docket number, and information about the ODD Applicant's medical exam.

NRR Requests for Additional Information – RAIs consist of an email from EIE (composed by NRR staff) to a Licensee. The email contains a link that accesses EIE and allows the Licensee to download attachment(s) provided to EIE by NRR staff through the BPAS Case Manager.

- The attachment(s) could contain PII similar to that contained in NRC Forms 398 or 396.

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

No, the information is collected by the Licensee.

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

N/A.

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

CH Workflow
Yes, the Licensees collect information on CH Applicants, none of which are federal employees. Approximately 35-40,000 criminal history checks are processed per year.

ODD Workflow
Yes, the Licensees collect information on ODD Applicants, none of which are federal employees.

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

CH Workflow
Yes

ODD Workflow
Yes

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

CH Workflow
1110-0046

ODD Workflow
NRC Form 398 – 3150-0090
NRC Form 396 – 3150-0024

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

No.

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

N/A.

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?

CH Workflow
As described above in 1.a. and 1.b - Licensees collect PII and fingerprints from Applicants and the FBI and DoD provide the criminal history of the Applicants.

ODD Workflow
As described above in 1.a. and 1.b – Licensees provide Registrant's PII in the GFE form, ODD Applicant's provide PII in NRC Form 398 or NRC Form 396 and NRR staff may provide PII in emails or related attachments in RAIs.

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

This is the responsibility of the submitter. The EIE merely transmits the information in Submissions (and Responses in the case of the CH Workflow). The EIE system neither displays nor retains the information.

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

A Submission consists of an EIE form (created by EIE for each Workflow) with file attachments (if any).

CH Workflow
The CH attachment file(s) are generated by Licensees using a proprietary Northrop Grumman application (the NG Application); the file(s) contain the CH Applicants' PII, which includes fingerprint cards. The CH Response consists of an EIE form with attachments (i.e. CH Reports, files generated by the FBI and DoD that contain Applicants' PII and results of criminal history check).

ODD Workflow
The GFE form is presented by EIE and completed by the Licensee.

The OL Action form is presented by EIE and completed by the Licensee. The attachments to an OL Action form are completed by the ODD Applicant.

The NRR RAI email is composed by EIE from information input by NRR staff into the BPAS Case Manager.

2. INFORMATION NOT ABOUT INDIVIDUALS

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

Yes.

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

Metadata only, e.g., Submission logs and (in the case of CH) Response logs.

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

Logs are updated when information passes through the system.

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 Workflow
Neither the EIE system nor the NRC makes any use of the CH information. Licensees make facility access and operating decisions based on the information transmitted by the EIE system.

ODD Workflow
The EIE system does not make any use of the GFE and OL Action information; it passes it to BPAS Case Manager (which uses it as input for its ODD process). The EIE system uses input from BPAS Case Manager to compose emails to Licensees for RAIs. The EIE Licensees make operating license decisions based on the information provided by BPAS and EIE.

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

Yes.

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

CH Workflow
Licensees, NSIR, the FBI, and the DoD

ODD GFE Workflow
Licensees, ADAMS, NRR and OCIO

3. 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?

EIE Security Categorization - ML13249A194, and EIE System Requirements Specification - ML16061A152 (access restricted documents).

4. 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?

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.

5. 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.)

CH Workflow
The EIE system attaches the CH Report (i.e. the files containing the Applicants' criminal history checks) to an EIE Response Form and dispatches the Response. This process sends an email with an EIE URL to the Licensee who originally transmitted the Submission. Using the URL to access the EIE system, the Licensee is able to view the Response (EIE Response Form and attached CH Report) and copy the CH Reports to their workstation.

Note the following:

- The email notification can only be sent to the email address contained in the digital certificate used to send the Submission
- Only the person holding the digital certificate who sent the Submission can use the certificate to open the Response
- Neither the forms nor the attachment file names of Submissions and Responses contain any PII; therefore, no information is retrieved from the EIE CH Workflow by the PII of an individual.

ODD Workflow
Submissions - Licensees complete an EIE ODD Workflow form and submit it via EIE. For OL Actions, the form is accompanied by attached files. The EIE System creates an XML file from the data in the form. The XML file and any related attachments are placed in a folder on the EIE file system. The BPAS ODD Case Manager application accesses the folder and 1) copies the files to its system for further processing and 2) returns a receipt file to the EIE system.

Note: Upon receipt of the BPAS receipt file, the EIE system deletes the Submission files from its file system.

RAIs – NRR staff utilize BPAS ODD Case Manager to create input that is transmitted (along with any related attachments) to EIE, which uses it to compose and send an email to the Licensee. The Licensee utilizes its email system to access the information.

Note: Upon expiration of a purge limit set by the ODD WFA, the EIE system deletes the email XML file and any related attachments.

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

N/A.

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

No.

a. If "Yes," provide name of SORN and location in the Federal Register.

N/A.

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

N/A.

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

No.

a. If yes, explain.

N/A.

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

N/A.

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

Only administrative reports that use metadata (e.g. system transaction logs) are produced. No data is included in these reports from Submission (or Response, for CH Workflow) attachments.

a. What are the reports used for?

Reporting of metadata (e.g. volumes of Submissions made, turnaround timeliness, etc.) for management reporting purposes.

b. Who has access to these reports?

Each Workflow's WFA and the EIE Administrator.

D. ACCESS TO DATA

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

CH Workflow
OCIO and NSIR

ODD GFE Workflow
OCIO and NRR

(1) For what purpose?

To administer their respective Workflows and process Submissions (and Responses, for CH) in accordance with the requirements of 10 CFR.

(2) Will access be limited?

Yes, to only Workflow WFAs and the EIE System Administrator.

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

Yes.

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

CH Workflow
NSIR CH

ODD Workflow
OCIO BPAS (components of ADAMS) and NRR RRPS

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

CH Workflow
CH Applicant information is automatically moved from EIE to NSIR CH by an automated program resident on the NSIR CH Store and Forward (SnF) server.

ODD Workflow
Registrant and ODD Applicant information is automatically moved from EIE to BPAS (component of ADAMS) by an automated program resident on the BPAS Case Manger server.

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

Yes.

(1) If yes, who?

CH Workflow
Licensees, the FBI, and the DoD

ODD Workflow
Licensees

(2) Will access be limited?

Yes.

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

CH Workflow
Submission attachments (files generated by Licensees using proprietary Northrup Grumman application; the files contain the CH Applicants' PII) – Used for identification of the individual requiring the criminal history check.

The Response attachments (i.e. CH Reports, files generated by the FBI and DoD that contains Applicants' personal identification information and the results of each agencies criminal history check) – Used for Licensees' consideration in making a hiring decision concerning the Applicant.

ODD Workflow
Submissions - Attachments (files containing the ODD Applicants' PII) – Used by Licensees to process the applications for GFE or OL Actions.

RAIs – Emails may contain ODD Applicant's PII in either the email itself or in attachments to the email – Used by Licensees to request additional information relative to the applications for GFE or OL Actions.

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

CH Workflow
Licensees transmit the Submission to the NRC via the EIE system. NRC transmits the Response to the Licensees via the EIE system.

Note: No disclosure of the information is made by the EIE system; the Submission is digitally signed, and the Response can only be viewed by the Licensee holding the digital certificate used to create the original Submission.

ODD Workflow
Submissions - Licensees transmit GFE and OL Action Submissions to the NRC via the EIE system.

RAIs – NRR staff use the EIE system (which in turn uses the NRC email system) to transmit an email (potentially with attachments) to Licensees.

E. RECORDS AND INFORMATION MANAGEMENT (RIM) - RETENTION AND DISPOSAL

The National Archives and Records Administration (NARA), in collaboration with federal agencies, approves whether records are temporary (eligible at some point for destruction/deletion because they no longer have business value) or permanent (eligible at some point to be transferred to the National Archives because of historical or evidential significance). These determinations are made through records retention schedules and NARA statutes (44 United States Code (U.S.C.), 36 Code of Federation Regulations (CFR)). Under 36 CFR 1234.10, agencies are required to establish procedures for addressing records management requirements, including recordkeeping requirements and disposition, before approving new electronic information systems or enhancements to existing systems. The following question is intended to determine whether the records and data/information in the system have approved records retention schedule and disposition instructions, whether the system incorporates Records and Information Management and NARA's Universal Electronic Records Management requirements, and if a strategy is needed to ensure compliance.

1) Can you map this system to an applicable retention schedule in NRC's Comprehensive Records Disposition Schedule (NUREG-0910), or NARA's General Records Schedules (GRS)?

Yes.

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?**

Email

EIE email for ODD Workflow: EIE system generates an email (XML file) which in turn uses the NRC email system to transmit an email (potentially with attachments) to Licensees. This email and its attachments are deleted once it is sent (or) is purged within 14 days and therefore falls under the following NARA GRS:

Common Office Records: GRS 5.1 – 020
Non-recordkeeping copies of electronic records.

Per the GRS 5.1 – 020, a senders' and recipients' versions of electronic mail messages that meet the definition of Federal records, and any related attachments have the following retention:

Temporary: Destroy immediately after copying to a recordkeeping system or otherwise preserving, but longer retention is authorized if required for business use.

Logs, Metadata Files and Response Files

The submission metadata (e.g. system transactional data) is kept in the database table (tables for each workflow). The metadata files are used to produce administrative reports. It would be recurring or special reports, or an inventory of activity on the system in order to answer inquiries from customers on the usage or for administrative purposes (audit logs). No PII data is included in these reports from Submission (or Response, for CH Workflow) attachments.

See table below for purge limits for deletion of log files, response files, and submission files on the EIE application Server for each of the EIE workflows:

Description	Purge Limit in Days
ADJ (Adjudicatory) Workflow	30 (for both public and non-public submissions)
CH (Criminal History) Workflow	Remove immediately after the content is stored in the EIE database
GF (General Form) Workflow	45
ODD (Operator Digital Docket) Workflow	14
Response Files	30
Log Files	14

The above files may fall under the following GRS depending on the business use of the metadata and if superseded/transferred to another recordkeeping system:

General Technology Management Records: GRS 3.1– 040
Information technology oversight and compliance records.

Temporary: Destroy 5 years after the project/activity/transaction is completed or superseded, but longer retention is authorized if required for business use.

Systems and data security records: GRS 3.2 item 010

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 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 Workflow
Application Users - Licensees must have an NRC-approved, valid digital certificate to access the EIE system and must be in a CH Workflow ACL to make a CH Submission / receive a CH Response. Licensee client-to-EIE server communication utilizes an approved Federal information system protocol, which provides authentication and confidentiality of transmitted data.

ODD Workflow
Application Users - Licensees must have an NRC-approved, valid digital certificate to access the EIE system and must be in an ODD Workflow ACL to make an ODD Submission.

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

See the EIE System Security Plan - ML082560557 (access restricted). The ability to view an Applicant's or Registrant's PII and criminal history record is very limited. Controls include, but are not limited to, the fact that Submissions are digitally signed; transmissions utilize a secure, mandated protocol; data at rest is encrypted; there are physical controls over access to the NSIR CH personnel workspace, NRC servers, and other devices; and privileged account issuance is controlled by the NRC CCB and NRC operations staff.

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

Yes.

(1) If yes, where?

In the EIE System Security Plan - ML082560557.

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

The EIE system is located and operated at one location; the NRC data center at NRC Headquarters in Rockville, Maryland.

Externally, the EIE system is accessed at multiple locations by NRC Licensees via workstations at their offices. See Section F – Technical Access and Security for automated interfaces with external service providers.

Internally, the EIE system is accessed by NRC staff (employees and contractors) via the NRC Managed Network (primarily located at NRC HQ, but also at the Regions and other NRC-managed sites).

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

All access is via the same infrastructure and utilizes the same internal controls.

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

Privileged group accounts and privileged System User accounts in each group are managed by the OCIO operations staff for the NRC Managed Network (which hosts EIE).

Semi-privileged accounts are managed by the EIE application developer (as authorized by the EIE System Owner) and limited to individual accounts (no group accounts) for the EIE System Administrator (all Workflows), the EIE CH WFA, and the EIE ODD WFA.

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

Yes.

a. If yes, what will be collected?

Transaction logs - NRC data center and EIE application

Audit / Monitoring reports – Operating system audit events collected by an OCIO operations tool (currently, Splunk)

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

Users are not limited to Federal employees. The EIE currently utilizes contractors to develop, maintain, and operate the EIE system.

Outside of the EIE system boundary, it is possible that the various systems that interact with EIE may utilize contractors to perform / manage the functions performed by their systems to include NRC Licensees, DigiCert, pay.gov, NRC Information Technology Infrastructure system, NSIR CH components of ACCESS, ODD components of RRPS, etc.

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?

See the EIE System Security Plan - ML082560557 (access restricted). The ability to view an Applicant's or Registrant's PII and criminal history record is very limited. Controls include, but are not limited to, the fact that Submissions are digitally signed; transmissions utilize a secure, mandated protocol; data at rest is encrypted; there are physical controls over access to the NSIR CH personnel workspace, NRC servers, and other devices; and privileged account issuance is controlled by the NRC CCB and NRC operations staff.

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

Yes.

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

EIE was last authorized on September 26, 2019.

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

System Name: Electronic Information Exchange (EIE)

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

A. PRIVACY ACT APPLICABILITY REVIEW

__X__ Privacy Act is not applicable.

____ Privacy Act is applicable.

Comments:

The NRC does not retrieve any information from EIE by an individual's name or other personal identifier. EIE is used to transmit information only.

Reviewer's Name	Title
Signed by Hardy, Sally on 11/25/20	Privacy Officer

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

____ No OMB clearance is needed.

__X__ OMB clearance is needed.

__X__ Currently has OMB Clearance. Clearance No._____

Comments:

EIE is the main portal for electronic submissions to the NRC including submissions covered by various OMB Clearances. This PIA only discusses those collections that include PII. Those collections include the following:

- 1100-0046 is the FBI clearance for collecting fingerprints used by the Criminal History System workflow
- 3150-0090 and 3150-0024 for NRC Forms 398 and 396 used by NRR's Operator Licensing program

The PIA mentions that EIE also communicates with pay.gov for Submitters wishing to pay the CH processing fee with credit card, but no PII is exchanged between EIE and pay.gov. This appears to be a separate collection of credit card information outside of the NRC's approved method using Form 629 or Pay.gov under OMB 3150-0190. The Form 629 clearance needs to be amended to include the burden for these payments.

Reviewer's Name	Title
 Signed by Cullison, David on 11/23/20	Agency Clearance Officer

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

____ No record schedule required.

____ Additional information is needed to complete assessment.

____ Needs to be scheduled.

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

Comments:

Reviewer's Name	Title
 Signed by Dove, Marna on 11/23/20	Sr. Program Analyst, Electronic Records Manager

D. BRANCH CHIEF REVIEW AND CONCURRENCE

__X__ 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 Partlow, Benjamin on 01/05/21

Acting Chief
Cyber Security Branch
Governance and Enterprise Management
Services Division
Office of the Chief Information Officer

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

TO: Thomas Ashley, Jr., ITSOD Director, Office of the Chief Information Officer (OCIO)	
Name of System: Electronic Information Exchange (EIE)	
Date CSB received PIA for review: October 22, 2020	**Date CSB completed PIA review:** November 25, 2020
Noted Issues:	
Acting Chief Cyber Security Branch Governance and Enterprise Management Services Division Office of the Chief Information Officer	Signature/Date: Signed by Partlow, Benjamin on 01/05/21
Copies of this PIA will be provided to: *Thomas G. Ashley, Jr.* *Director* *IT Services Development and Operations Division* *Office of the Chief Information Officer* *Jonathan R. Feibus* *Chief Information Security Officer (CISO)* *Office of the Chief Information Officer*	