

---

U.S. Nuclear Regulatory Commission

---



**Privacy Impact Assessment  
Security Executive Agent Directive 3 (SEAD3)  
Office of Administration**

**Version 1.0  
10/05/2023**

Security Executive Agent Directive 3 (SEAD3)	Version 1.0
Privacy Impact Assessment	10/05/2023

## Document Revision History

Date	Version	PIA Name/Description	Author
10/05/2023	1.0	SEAD3 PIA - Initial Release.	ADM Oasis Systems, LLC
9/15/2023	DRAFT	SEAD3 PIA - Draft Release.	ADM Oasis Systems, LLC

Security Executive Agent Directive 3 (SEAD3)	Version 1.0
Privacy Impact Assessment	10/05/2023

## Table of Contents

1	Description	1
2	Authorities and Other Requirements	3
3	Characterization of the Information	4
4	Data Security	6
5	Privacy Act Determination	8
6	Records and Information Management-Retention and Disposal	10
7	Paperwork Reduction Act	12
8	Privacy Act Determination	14
9	OMB Clearance Determination	15
10	Records Retention and Disposal Schedule Determination	16
11	Branch Chief Review and Concurrence	17

Security Executive Agent Directive 3 (SEAD3)	Version 1.0
Privacy Impact Assessment	10/05/2023

*The agency is subject to the requirements of the E-Government Act and is committed to identifying and addressing privacy risks whenever it develops or makes changes to its information systems. The questions below help determine any privacy risks related to the E-Government Act or later guidance by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST).*

**Name/System/Subsystem/Service Name:** Security Executive Agent Directive 3 (SEAD3).

**Data Storage Location (i.e., Database Server, SharePoint, Cloud, Other Government Agency, Power Platform):** Database.

**Date Submitted for review/approval:** October 05, 2023.

## 1 Description

**1.1 Provide the description of the system/subsystem, technology (i.e., Microsoft Products), program, or other data collections (hereinafter referred to as “project”). Explain the reason the project is being created.**

The Security Executive Agent Directive 3 is an executive security directive issued by the Office of the Director of National Intelligence (ODNI) in December 2016. It is applicable to all executive branch agencies and covered individuals, which includes all U.S. Nuclear Regulatory Commission (NRC) employees, consultants, experts, panel members, cleared contractors, cleared licensees, cleared licensee contractors, and other cleared persons designated by the Executive Director for Operations (EDO), such as individuals from the Organization of Agreement States. SEAD3 is designed to strengthen the safeguarding of national security equities, and establishes the reporting requirements for covered individuals who have access to classified information or hold a sensitive position. These reporting requirements are generally consistent with the elements included in the Standard Form 86 (SF-86), "Questionnaire for National Security Positions", which is completed by NRC employment applicants and clearance holders during the initial and periodic reinvestigation processes, respectively.

Additionally, SEAD3 requires these elements to be reported by covered individuals prior to participation in certain activities, or as soon as possible following the start of their involvement if prior reporting is not possible. In response to the Federal Government requirement to track employee, contractor, and licensee personal travel to foreign countries in the interest of national security, Security Executive Agent Directive 3 (SEAD3) was added to the Office of Administration's (ADM) Moderate ADM Support Systems (MASS) boundary as a module of the Personnel Security Adjudication Tracking System (PSATS). SEAD3 is a web portal used to report, record, and track foreign travel of NRC personnel who hold a security clearance.

Please note, licensees and other individuals who possess an NRC security clearance do not use the SEAD3 portal to report personal foreign travel. These individuals are required to submit their unofficial foreign travel requests to NRC through the [UnofficialTravel.Resource@nrc.gov](mailto:UnofficialTravel.Resource@nrc.gov) email address. An external portal for non-NRC personnel use is planned to be developed within the next year to replace the current email process.

Security Executive Agent Directive 3 (SEAD3)	Version 1.0
Privacy Impact Assessment	10/05/2023

Please mark appropriate response below if your project/system will involve the following:

<input type="checkbox"/> PowerApps	<input type="checkbox"/> Public Website
<input type="checkbox"/> Dashboard	<input checked="" type="checkbox"/> Internal Website
<input type="checkbox"/> SharePoint	<input type="checkbox"/> None
<input type="checkbox"/> Other:	

**1.2 Does this privacy impact assessment (PIA) support a proposed new project, proposed modification to an existing project, or other situation? Select options that best apply in table below.**

Mark appropriate response.

Status Options	
<input type="checkbox"/>	New system/project
<input type="checkbox"/>	Modification to an existing system/project. <i>If modifying or making other updates to an existing system/project, provide the ADAMS ML of the existing PIA and describe the modification.</i>
<input checked="" type="checkbox"/>	Annual Review <i>If making minor edits to an existing system/project, briefly describe the changes below.</i> Annual update and migration to new PIA template for SEAD3. ADAMS ML: ML22124A227
<input type="checkbox"/>	Other (explain)

**1.3 Points of Contact:**

	Project Manager	System Owner/Data Owner/Steward	ISSO	Business Project Manager	Technical Project Manager	Executive Sponsor
<b>Name</b>	Michael England	Jennifer Golder	Zia Anderson	N/A	Denis Brady	Timothy Pulliam
<b>Office/Division /Branch</b>	ADM/DFS/ SMOB	ADM	ADM/ DRMA/BITT	N/A	ADM/DFS/ SMOB	ADM/DFS
<b>Telephone</b>	301-415-0178	301-287-0741	301-415-3483	N/A	301-415-5768	301-415-8080

Security Executive Agent Directive 3 (SEAD3)	Version 1.0
Privacy Impact Assessment	10/05/2023

## 2 Authorities and Other Requirements

### 2.1 What specific legal authorities and/or agreements permit the collection of information for the project?

*Provide all statutory and regulatory authorities for operating the project, including the authority to collect the information; NRC internal policy is not a legal authority. Please mark appropriate response in table below.*

Mark with an "X" on all that apply.	Authority	Citation/Reference
<input checked="" type="checkbox"/>	<b>Statute</b>	42 United States Code (U.S.C). 2011 et seq.; 42 U.S.C. 2165, 2201(i), 2201a, and 2284; and 42 U.S.C. 5801 et seq.
<input checked="" type="checkbox"/>	<b>Executive Order</b>	Executive Order (E.O.) 9397, as amended by E.O. 13478; 10450, as amended; 10865, as amended; 12968, 13467, 13488, 13526, and 13587.
<input checked="" type="checkbox"/>	<b>Federal Regulation</b>	10 Code of Federal Regulation (CFR) Parts 10, 11, 14, 25, 50, 73, 95; OMB Circular No. A-130, Revised; and 5 CFR Parts 731, 732.
<input type="checkbox"/>	<b>Memorandum of Understanding/ Agreement</b>	
<input checked="" type="checkbox"/>	<b>Other (summarize and provide a copy of relevant portion)</b>	Security Executive Agent Directive (SEAD) 3, "Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position"

### 2.2 Explain how the information will be used under the authority listed above (i.e., *enroll employees in a subsidies program to provide subsidy payment*).

Unofficial travel information collected by the SEAD3 portal (and email correspondence for non-NRC personnel) is used to report, record, and track foreign travel of personnel who hold a security clearance. This portal was developed in response to the Federal Government requirement to track employee, contractor, and licensee personal travel to foreign countries in the interest of national security. Information collected becomes part of the individual's personnel security record and supports national security and the adjudication for continued access to classified information and systems.

The data will be used to track and catalog unofficial foreign travel as a part of the Continuous Evaluation (CE) process for covered individuals who have access to classified information or hold a sensitive position.

Security Executive Agent Directive 3 (SEAD3)	Version 1.0
Privacy Impact Assessment	10/05/2023

If the project collects Social Security Numbers (SSNs), state why this is necessary and how it will be used.

N/A.

### 3 Characterization of the Information

In the table below, mark the categories of individuals for whom information is collected.

Category of individual	
<input checked="" type="checkbox"/>	Federal employees
<input checked="" type="checkbox"/>	Contractors
<input type="checkbox"/>	Members of the Public (any individual other than a federal employee, consultant, or contractor)
<input checked="" type="checkbox"/>	Licensees
<input type="checkbox"/>	<b>Other:</b>

In the table below, is a list of the most common types of PII collected. Mark all PII that is collected and stored by the project/system. If there is additional PII not defined in the table below, a comprehensive listing of PII is provided for further reference in ADAMS at the following link: [PII Reference Table 2023](#).

Categories of Information			
<input checked="" type="checkbox"/>	Name	<input type="checkbox"/>	Resume or curriculum vitae
<input checked="" type="checkbox"/>	Date of Birth	<input type="checkbox"/>	Driver's License Number
<input type="checkbox"/>	Country of Birth	<input type="checkbox"/>	License Plate Number
<input type="checkbox"/>	Citizenship	<input checked="" type="checkbox"/>	Passport Number
<input type="checkbox"/>	Nationality	<input type="checkbox"/>	Relatives Information
<input type="checkbox"/>	Race	<input type="checkbox"/>	Taxpayer Identification Number
<input type="checkbox"/>	Home Address	<input type="checkbox"/>	Credit/Debit Card Number
<input type="checkbox"/>	Social Security Number (Truncated or Partial)	<input type="checkbox"/>	Medical/health information
<input type="checkbox"/>	Gender	<input type="checkbox"/>	Alien Registration Number
<input type="checkbox"/>	Ethnicity	<input type="checkbox"/>	Professional/personal references
<input type="checkbox"/>	Spouse Information	<input type="checkbox"/>	Criminal History
<input type="checkbox"/>	Personal e-mail address	<input type="checkbox"/>	Biometric identifiers (e.g., facial images, fingerprints, iris scans)
<input type="checkbox"/>	Personal Bank Account Number	<input type="checkbox"/>	Emergency contact (e.g., a third party to contact in case of an emergency)
<input type="checkbox"/>	Personal Mobile Number	<input type="checkbox"/>	Accommodation/disabilities information
<input type="checkbox"/>	Marital Status	<input checked="" type="checkbox"/>	<b>Other:</b> Unofficial foreign travel dates, purpose, companion name/relationship, passport information, countries visited,
<input type="checkbox"/>	Children Information		

Security Executive Agent Directive 3 (SEAD3)	Version 1.0
Privacy Impact Assessment	10/05/2023

Categories of Information	
<input type="checkbox"/>	Mother's Maiden Name
	travel itinerary, and lodging information.

**3.1 Describe how the data is collected for the project (i.e., NRC Form, survey, questionnaire, existing NRC files/databases, response to a background check).**

For NRC employees and contractors with a security clearance, the SEAD3 portal is used to complete the “NRC Personal International Travel Form” (<https://sead3portal.nrc.gov/sead3portal/landing>) prior to, or immediately after returning from unofficial foreign travel. For licensees and other individuals who possess an NRC security clearance, unofficial foreign travel requests are submitted to NRC through the [UnofficialTravel.Resource@nrc.gov](mailto:UnofficialTravel.Resource@nrc.gov) email address. An external portal for non-NRC personnel use is planned to be developed within the next year to replace the current email process.

Both forms of travel requests are reviewed by a limited number of ADM Division of Facilities and Security’s Security Management and Operations Branch (ADM/DFS/SMOB) personnel. Requests are either approved or denied accordingly by SMOB. After a travel request has been reviewed and a decision has been made, the collected travel request information is retained in PSATS as part of the individual’s personnel security file.

**3.2 If using a form to collect the information, provide the form number, title, and/or a link.**

NRC personnel use the SEAD3 portal to complete the “NRC Personal International Travel Form” (<https://sead3portal.nrc.gov/sead3portal/landing>).

Non-NRC personnel do not use forms to submit unofficial foreign travel requests.

**3.3 Who provides the information? Is it provided directly from the individual or a third party.**

Information is entered into the portal (or sent via email) directly by the subject individual.

**3.4 Explain how the accuracy of the data collection is validated. If the project does not check for accuracy, please explain why.**

There are limited information validation checks done by the SEAD3 portal. Information from travel request submissions can be cross-checked by SMOB with the individual’s information in PSATS, if necessary.

**3.5 Will PII data be used in a test environment? If so, explain the rationale.**

No.

**3.6 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?**

Individuals can retrieve their draft travel requests, correct submissions, and update requests with post-travel details in the SEAD3 portal. In the event a travel request is rejected because it requires additional information, the SMOB will correspond with the individual over email to either go into the portal (for NRC personnel) and edit their request or provide clarifying information in a follow up email message (for non-NRC personnel).



Security Executive Agent Directive 3 (SEAD3)	Version 1.0
Privacy Impact Assessment	10/05/2023

## 4 Data Security

### 4.1 Describe who has access to the data in the project (i.e., internal NRC, system administrators, external agencies, contractors, public).

The SEAD3 portal is an internal NRC-accessible website. All NRC employees and contractors with an NRC LAN ID can access the system from the NRC network. Within PSATS, a limited number of SMOB personnel have the ability to review and approve/reject/deny travel requests in the SEAD3 module. Finalized travel requests are accessible to the PSATS Administrator, Security Manager, Senior Adjudicator, Facilities Security Specialists, SMOB Elevated Reviewer, and Adjudicators.

### 4.2 If the project/system shares information with any other NRC systems, identify the system, what information is being shared, and the method of sharing.

PSATS retains unofficial foreign travel information from SEAD3 in its databases as part of an individuals' personnel security file. This information is also referred to for verification when an individual renews their clearance.

### 4.3 If the project/system connects, receives, or shares information with any external non-NRC partners or systems, identify what is being shared.

The National Security Agency (NSA) occasionally sends NRC requests for information regarding the foreign travel of clearance-holding personnel. This request typically consists of asking how many NRC-cleared individuals traveled to a specific country/region, for the purpose of national security. No PII is shared with the NSA in response, only the number of individuals, and a list containing the names of individuals who traveled to the specific location during the timeframe requested.

Identify what agreements are in place with the external non-NRC partner or system in the table below.

Agreement Type	
<input type="checkbox"/>	Contract Provide Contract Number:
<input type="checkbox"/>	License Provide License Information:
<input type="checkbox"/>	Memorandum of Understanding Provide ADAMS ML number for MOU:
<input type="checkbox"/>	Other
<input checked="" type="checkbox"/>	None

### 4.4 Describe how the data is accessed and describe the access control mechanisms that prevent misuse.

SEAD3 resides behind the NRC network firewall, authorized users must first gain access to the NRC network using valid authentication credentials. SEAD3 user accounts are integrated with the Information Technology Infrastructure (ITI) Identity, Credential, and Access Management (ICAM) for Single Sign-On (SSO) access. The system employs differing user access/privileges that keeps the data segregated within the system.

Security Executive Agent Directive 3 (SEAD3)	Version 1.0
Privacy Impact Assessment	10/05/2023

Access to submitted travel requests awaiting approval are restricted to SMOB personnel with a need-to-know, based on roles and responsibilities, and with elevated permissions. An audit log tracks modification to applicable data fields within SEAD3.

**4.5 Explain how the data is transmitted and how confidentiality is protected (i.e., encrypting the communication or by encrypting the information before it is transmitted).**

SEAD3 is accessible to NRC staff from the NRC VPN, using secure (HTTPS) Internet connections. Email correspondence from external clearance holders are encrypted if they contain PII.

**4.6 Describe where the data is being stored (i.e., NRC, Cloud, Contractor Site).**

SEAD3 data is stored at NRC HQ.

**4.7 Explain if the project can be accessed or operated at more than one location.**

The SEAD3 portal is a web-based system that operates from the NRC HQ Data Center. User access is through authorized network connectivity. Login requirements and access levels remain the same no matter from what location an approved user attempts to access the system.

**4.8 Can the project be accessed by a contractor? If so, do they possess an NRC badge?**

Yes, all NRC contractors accessing and supporting SEAD3 are NRC badged personnel.

**4.9 Explain the auditing measures and technical safeguards in place to prevent misuse of data.**

Audit logs track modifications to certain data fields within SEAD3. All access to data in SEAD3 is restricted to need-to-know based on roles and responsibilities. Audit logs are reviewed by system administrators to monitor activities and report any anomalies within the system. The date and time of the last login is captured.

**4.10 Describe if the project has the capability to identify, locate, and monitor (i.e., trace/track/observe) individuals.**

N/A – Although SEAD3 is used to observe unofficial travel data, it does not have a real-time tracking capability.

**4.11 Define which FISMA boundary this project is part of.**

PSATS is included as a subsystem of the MASS FISMA boundary; SEAD3 is a module of PSATS.

Security Executive Agent Directive 3 (SEAD3)	Version 1.0
Privacy Impact Assessment	10/05/2023

#### 4.12 Is there an Authority to Operate (ATO) associated with this project/system?

Authorization Status	
<input type="checkbox"/>	Unknown
<input type="checkbox"/>	No <i>If no, please note that the authorization status must be reported to the Chief Information Security Officer (CISO) and Computer Security Organization (CSO's) Point of Contact (POC) via e-mail quarterly to ensure the authorization remains on track.</i>
<input type="checkbox"/>	In Progress provide the estimated date to receive an ATO. Estimated date:
<input checked="" type="checkbox"/>	Yes Indicate the data impact levels (Low, Moderate, High, Undefined) approved by the Chief Information Security Officer (CISO) Confidentiality – Moderate Integrity – Moderate Availability – Moderate

#### 4.13 Provide the NRC system Enterprise Architecture (EA)/Inventory number. If unknown, contact [EA Service Desk](#) to get the EA/Inventory number.

EA Number: 20110002.

## 5 Privacy Act Determination

### 5.1 Is the data collected retrieved by a personal identifier?

Mark the appropriate response.

Response	
<input checked="" type="checkbox"/>	<b>Yes, the PII is retrieved by a personal identifier (i.e., individual's name, address, SSN, etc.)</b>
<input checked="" type="checkbox"/>	<b>List the identifiers that will be used to retrieve the information on the individual.</b> SMOB personnel with elevated privileges can retrieve information from SEAD3 by a keyword search (i.e., name, country of travel, and/or trip dates).
<input type="checkbox"/>	<b>No, the PII is not retrieved by a personal identifier.</b> <b>If no, explain how the data is retrieved from the project.</b>

Security Executive Agent Directive 3 (SEAD3)	Version 1.0
Privacy Impact Assessment	10/05/2023

**5.2 For all collections where the information is retrieved by a personal identifier, the Privacy Act requires that the agency publish a System of Record Notice (SORN) in the Federal Register. As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some other personal identifier assigned to the individual.”**

Mark the appropriate response in the table below.

Response	
<input checked="" type="checkbox"/>	<b>Yes, this system is covered by an existing SORN. (See existing SORNs: <a href="https://www.nrc.gov/reading-rm/foia/privacy-systems.html">https://www.nrc.gov/reading-rm/foia/privacy-systems.html</a>) Provide the SORN name, number, (List all SORNs that apply): NRC-39 – “Personnel Security Files and Associated Records”</b>
<input type="checkbox"/>	<b>SORN is in progress</b>
<input type="checkbox"/>	<b>SORN needs to be created</b>
<input type="checkbox"/>	<b>Unaware of an existing SORN</b>
<input type="checkbox"/>	<b>No, this system is not a system of records and a SORN is not applicable.</b>

**5.3 When an individual is asked to provide personal data (i.e., form, webpage, survey), is a Privacy Act Statement (PAS) provided? A Privacy Act Statement is a disclosure statement required to appear on documents used by agencies when an individual is asked to provide personal data. It is required for any forms, surveys, or other documents, including electronic forms, used to solicit personal information from individuals that will be maintained in a system of records.**

Mark the appropriate response.

Options	
<input checked="" type="checkbox"/>	<b>Privacy Act Statement:</b> “NRC Personal International Travel Form” ( <a href="https://sead3portal.nrc.gov/sead3portal/landing">https://sead3portal.nrc.gov/sead3portal/landing</a> )
<input type="checkbox"/>	<b>Not Applicable</b>
<input type="checkbox"/>	<b>Unknown</b>

**5.4 Is providing the PII mandatory or voluntary? What is the effect on the individual by not providing the information?**

Disclosure of PII elements (described above in section 3) is mandatory. Failure to report the information in a timely manner prior to travel and/or immediately upon return could result in disciplinary action and/or affect eligibility for a security clearance.

Security Executive Agent Directive 3 (SEAD3)	Version 1.0
Privacy Impact Assessment	10/05/2023

## 6 Records and Information Management-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). Records/data and information with historical value, identified as having a “permanent” disposition, are transferred to the National Archives of the United States at the end of their retention period. All other records identified as having a “temporary” disposition are destroyed at the end of their retention period in accordance with the NARA Records Schedule or the General Records Schedule.

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, agencies are required to establish procedures for addressing Records and Information Management (RIM) requirements. This includes strategies for establishing and managing recordkeeping requirements and disposition instructions before approving new electronic information systems or enhancements to existing systems.

The following questions are intended to determine whether the records/data and information in the system have approved records retention schedules and disposition instructions, whether the system incorporates RIM strategies including support for [NARA’s Universal Electronic Records Management \(ERM\) requirements](#), and if a mitigation strategy is needed to ensure compliance.

### If the project/system:

- Does not have an approved records retention schedule and/or
- Does not have an *automated* RIM functionality,
- Involves a cloud solution,
- And/or if there are additional questions regarding Records and Information Management - Retention and Disposal, please contact the NRC Records staff at [ITIMPolicy.Resource@nrc.gov](mailto:ITIMPolicy.Resource@nrc.gov) for further guidance.

**If the project/system has a record retention schedule or an automated RIM functionality, please complete the questions below.**

### 6.1 Does this project map to an applicable retention schedule in NRC’s Comprehensive Records Disposition Schedule (NUREG-0910), or NARA’s General Records Schedules?

<input type="checkbox"/>	<a href="#">NUREG-0910, “NRC Comprehensive Records Disposition Schedule”</a>
<input checked="" type="checkbox"/>	<a href="#">NARA’s General Records Schedules</a>
<input checked="" type="checkbox"/>	Unscheduled

Security Executive Agent Directive 3 (SEAD3)	Version 1.0
Privacy Impact Assessment	10/05/2023

**6.2 If so, cite the schedule number, approved disposition, and describe how this is accomplished.**

<b>System Name (include sub-systems, platforms, or other locations where the same data resides)</b>	SEAD 3 Portal
<b>Records Retention Schedule Number(s)</b>	<p>Please note, after travel requests are submitted (either via the SEAD3 portal or over email) and approved by ADM/DFS/SMOB, the collected information resides in PSATS, where it is retained as part of an individual’s case file. Retention for the “NRC Personal International Travel Form” and licensee travel email correspondence is documented in the PSATS PIA.</p> <p><u>Email Records</u></p> <p><a href="#">GRS 6.1 item 010</a> – Email and other electronic messages of Capstone officials</p> <p><a href="#">GRS 6.1 item 11</a> – Email and other types of electronic messages of Non-Capstone officials. All other except those in item 012.</p> <p><b><u>Travel Records</u></b></p> <p><a href="#">GRS 1.1 item 011</a> – Financial transaction records related to procuring good and services, paying bills, collecting debts, and accounting. All other copies used for administrative or reference purposes.</p>
<b>Approved Disposition Instructions</b>	<p>Travel Records</p> <p><a href="#">GRS 1.1 item 011</a> – <b>Temporary.</b> Destroy when business use ceases.</p> <p>Email Records</p> <p><a href="#">GRS 6.1 - Item 010</a> – <b>Permanent.</b> Cut off and transfer in accordance with the Agency’s approved NA-1005, Verification for Implementing GRS 6.1. This will be between 15 and 30 years, or after declassification review (when applicable), whichever is later. For NRC Capstone officials, records are transferred after 15 years.</p>

Security Executive Agent Directive 3 (SEAD3)	Version 1.0
Privacy Impact Assessment	10/05/2023

	<b><u>GRS 6.1 - Item 011 - Temporary</u></b> . Delete when 7 years old, but longer retention is authorized if required for business use.
Is there a current automated functionality or a manual process to support RIM requirements? This includes the ability to apply records retention and disposition policies in the system(s) to support records accessibility, reliability, integrity, and disposition.	
<b>Disposition of Temporary Records</b>  Will the records/data or a composite be automatically or manually deleted once they reach their approved retention?	N/A.
<b>Disposition of Permanent Records</b>  Will the records be exported to an approved format and transferred to the National Archives based on approved retention and disposition instructions?  If so, what formats will be used?  <b><u><a href="#">NRC Transfer Guidance (Information and Records Management Guideline - IRMG)</a></u></b>	N/A.

## 7 Paperwork Reduction Act

The Paperwork Reduction Act (PRA) of 1995 requires that agencies obtain an Office of Management and Budget (OMB) approval in the form of a "control number" — before promulgating a paper form, website, surveys, questionnaires, or electronic submission from 10 or more members of the public. If the data collection is from federal employees regarding work-related duties, then a PRA clearance is not necessary.

### 7.1 Will the project be collecting any information from 10 or more persons who are not Federal employees?

For NRC employees and contractors with a security clearance, the SEAD3 portal is used to complete the "NRC Personal International Travel Form" (<https://sead3portal.nrc.gov/sead3portal/landing>) prior to, or immediately after returning from unofficial foreign travel. For licensees and other individuals who possess an NRC security clearance, unofficial foreign travel requests are submitted to NRC via the [UnofficialTravel.Resource@nrc.gov](mailto:UnofficialTravel.Resource@nrc.gov) email address.

An external portal for non-NRC personnel use is planned to be developed within the next year to replace the current email process.

Security Executive Agent Directive 3 (SEAD3)	Version 1.0
Privacy Impact Assessment	10/05/2023

**7.2 Is there any collection of information addressed to all or a substantial majority of an industry (i.e., Fuel Fabrication Facilities or Fuel Cycle Facilities)?**

No.

**7.3 Is the collection of information required by a rule of general applicability?**

No.

*Note: For information collection (OMB clearances) questions: contact the NRC's Clearance Officer. Additional guidance can be found on the NRC's internal Information Collections Web page at: <https://intranet.nrc.gov/ocio/33456>.*



Security Executive Agent Directive 3 (SEAD3)	Version 1.0
Privacy Impact Assessment	10/05/2023

## 8 Privacy Act Determination

**Project/System Name:** Security Executive Agent Directive 3 (SEAD3).

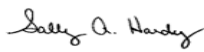
**Submitting Office:** Office of Administration.

### Privacy Officer Review

Review Results		Action Items
<input type="checkbox"/>	This project/system <b>does not contain PII</b> .	<b>No further action</b> is necessary for Privacy.
<input type="checkbox"/>	This project/system <b>does contain PII</b> ; the Privacy Act does <b>NOT</b> apply, since information is NOT retrieved by a personal identifier.	<b>Must be protected with restricted access</b> to those with a valid need-to-know.
<input checked="" type="checkbox"/>	This project/system <b>does contain PII</b> ; the <b>Privacy Act does apply</b> .	<b>SORN is required-</b> Information is retrieved by a personal identifier.

**Comments:**

Covered by System of Records Notice NRC-39 – “Personnel Security Files and Associated Records”

Reviewer's Name	Title
 Signed by Hardy, Sally on 12/27/23	Privacy Officer


## 9 OMB Clearance Determination

### NRC Clearance Officer Review

Review Results	
<input type="checkbox"/>	No OMB clearance is needed.
<input type="checkbox"/>	OMB clearance is needed.
<input checked="" type="checkbox"/>	Currently has OMB Clearance. Clearance No. <u>3150-0046</u>

**Comments:**

The collection of SEAD 3 related information is covered by OMB Control Number 3150-0046. The online portal for licensees is at OMB for approval as part of the renewal of the 10 CFR Part 25 clearance.


Reviewer's Name	Title
 Signed by Cullison, David on 12/20/23	Agency Clearance Officer

## 10 Records Retention and Disposal Schedule Determination

### Records Information Management Review

Review Results	
<input type="checkbox"/>	No record schedule required.
<input type="checkbox"/>	Additional information is needed to complete assessment.
<input type="checkbox"/>	Needs to be scheduled.
<input checked="" type="checkbox"/>	Existing records retention and disposition schedule covers the system - no modifications needed.

**Comments:**

Reviewer's Name	Title
 Signed by Dove, Marna on 12/18/23	Sr. Program Analyst, Electronic Records Manager

## 11 Branch Chief Review and Concurrence

Review Results	
<input type="checkbox"/>	This project/system <b>does not</b> collect, maintain, or disseminate information in identifiable form.
<input checked="" type="checkbox"/>	This project/system <b>does</b> collect, maintain, or disseminate information in identifiable form.
<input checked="" type="checkbox"/>	I concur with the Privacy Act, Information Collections, and Records Management reviews.



Signed by Feibus, Jonathan  
on 12/27/23

---

Chief Information Security Officer  
Chief Information Security Division  
Office of the Chief Information Officer

Security Executive Agent Directive 3 (SEAD3)	Version 1.0
Privacy Impact Assessment	10/05/2023

## ADDITIONAL ACTION ITEMS/CONCERNS

<b>Name of Project/System:</b> Security Executive Agent Directive 3 (SEAD3).	
<b>Date CISD received PIA for review:</b> December 6, 2023	<b>Date CISD completed PIA review:</b> December 21, 2023
<b>Action Items/Concerns:</b>          	
<p><i>Copies of this PIA will be provided to:</i></p> <p><i>Caroline Carusone</i> <i>Director</i> <i>IT Services Development and Operations Division</i> <i>Office of the Chief Information Officer</i></p> <p><i>Garro Nalabandian</i> <i>Deputy Chief Information Security Officer (CISO)</i> <i>Office of the Chief Information Officer</i></p>	