U.S. Nuclear Regulatory Commission

Privacy Impact Assessment

Enterprise Vetting Center / Law Enforcement Enterprise Portal (EVC/LEEP)

Office of Administration (ADM)

Version 1.0

9/12/2023

Template Version 2.0 (03/2023)

Document Revision History

Date	Version	PIA Name/Description	Author
9/12/2023	1.0	EVC/LEEP PIA - Initial Release.	ADM Oasis Systems, LLC
8/18/2023	DRAFT	EVC/LEEP PIA - Draft Release.	ADM Oasis Systems, LLC

Table of Contents

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: Enterprise Vetting Center / Law Enforcement Enterprise Portal (EVC/LEEP).

Data Storage Location (i.e., Database Server, SharePoint, Cloud, Other Government Agency, Power Platform): Federal Bureau of Investigation (FBI).

Date Submitted for review/approval: December 4, 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.

FBI's EVC/LEEP supports the personnel security functions of the NRC Office of Administration (ADM). EVC/LEEP provides name checks for the spouses/cohabitants of NRC employees and applicants holding or requiring a security clearance. Information from FBI records are used to ensure there is not a security risk regarding the employees or applicants initial or continuing eligibility for NRC employment or access authorization.

EVC/LEEP has two modules:

- The Customer Facing Element (CFE), used by FBI customers, provides a secure, web-based interface for customer submissions using a separate agency organizational account and individual accounts for each user. CFE allows for electronic name check submissions, name check submission status, response packages, automated billing process, and reporting capability.
- The Processing Element (PE), used by the FBI, provides a web-based PE for research analysts that includes search interfaces, automated billing process, automated workflow, application replacement, application consolidation, metrics, auditing, and reporting capability.

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

☐ PowerApps	☒ Public Website
☐ Dashboard	☐ Internal Website
☐ SharePoint	☐ None
☐ 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	
☐	New system/project
☒	Modification to an existing system/project. *If modifying or making other updates to an existing system/project, provide the ADAMS ML of the existing PIA and describe the modification.* The functionality of FBI's "Next Generation Name Check Program / Law Enforcement Enterprise Portal (NGNCP/LEEP)" system has renamed to "EVC/LEEP". ADAMS ML: ML20288A500
☐	Annual Review *If making minor edits to an existing system/project, briefly describe the changes below.*
☐	Other (explain)

1.3 Points of Contact:

	Project Manager	System Owner/Data Owner/Steward	ISSO	Business Project Manager	Technical Project Manager	Executive Sponsor
Name	Emily Robbins	Jennifer Golder	Zia Anderson	N/A	N/A	N/A
Office/Division /Branch	ADM/ DFS/PSB	ADM	ADM/ DRMA/BITT	N/A	N/A	N/A
Telephone	301-310-7197	301-287-0741	N/A	N/A	N/A	N/A

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
☒	**Statute**	Section 145 of the "Atomic Energy Act of 1954," as amended.
☒	**Executive Order**	Executive Order (E.O.) 13467 as amended, 10865, and 12968 as amended.
☒	**Federal Regulation**	10 Code of Federal Regulation (CFR) Part 10, Subpart B.
☐	**Memorandum of Understanding/Agreement**	
☐	**Other (summarize and provide a copy of relevant portion)**	

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*).

The purpose of EVC/LEEP is to electronically submit name check requests to the FBI and to receive the results (responses) electronically. The data collected is reviewed by NRC Personnel Security to provide assurance that employees, consultants, contractors, licensees, and others are reliable and trustworthy to have access to NRC facilities, classified information, sensitive NRC information and equipment, nuclear power facilities, and special nuclear material.

If the project collects Social Security numbers, state why this is necessary and how it will be used.

Social Security Numbers (SSNs) are needed to uniquely identify the employee/applicant to support their initial or continuing eligibility for a security clearance and/or NRC access authorization. The SSN of spouses/cohabitants are not collected by the NRC for usage of the service; criminal history checks are conducted by name only.

3 Characterization of the Information

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

Category of individual	
☒	Federal employees
☒	Contractors
☒	Members of the Public (any individual other than a federal employee, consultant, or contractor)
☒	Licensees
☒	**Other:** Consultants

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			
☒	Name	☐	Resume or curriculum vitae
☒	Date of Birth	☐	Driver's License Number
☒	Country of Birth	☐	License Plate Number
☒	Citizenship	☐	Passport number
☐	Nationality	☒	Relatives Information
☐	Race	☐	Taxpayer Identification Number
☒	Home Address	☐	Credit/Debit Card Number
☒	Social Security number (Truncated or Partial)	☐	Medical/health information
☐	Gender	☒	Alien Registration Number
☐	Ethnicity	☐	Professional/personal references
☒	Spouse Information	☒	Criminal History
☐	Personal e-mail address	☐	Biometric identifiers (e.g., facial images, fingerprints, iris scans)
☐	Personal Bank Account Number	☐	Emergency contact (e.g., a third party to contact in case of an emergency)
☐	Personal Mobile Number	☐	Accommodation/disabilities information
☒	Marital Status	☒	**Other:** Date of marriage, place of marriage, other names used by employee/applicant, and other names used by spouse/cohabitant.
☐	Children Information		
☐	Mother's Maiden Name		

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).

This form will be completed by persons who marry or cohabitate after the time they submit the Standard Form 86 (SF-86), "Questionnaire for National Security Positions," or marries or cohabitates after having been granted an access authorization, or employment clearance in connection with the U.S. Nuclear Regulatory Commission (NRC) access authorization (security clearance).This form will be submitted to the Federal Bureau of Investigations for the purpose of conducting name checks on the spouse/cohabitant and spouse's parents. The form is signed by the employee/applicant and spouse/cohabitant, to certify that the information on the form is current, accurate, and complete. The form must then be submitted to NRC Personnel Security for review. Information collected on the NRC Form 354 is entered directly into EVC/LEEP by NRC Personnel Security for FBI criminal history reporting.

On the FBI side, criminal record checks are conducted based on name only. If there is no criminal record, the data check will reflect no record. If there is a criminal record, the record will

be revealed. The information revealed permits NRC Personnel Security to make security determinations as to whether or not any information on a specific individual has an impact on an employee or applicant's initial or continued eligibility for access authorization or employment clearance.

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

NRC Form 354 – "Data Report on Spouse."

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

NRC Form 354 is completed by NRC employees, applicants, and their spouses/cohabitants.

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

The NRC Form 354 is signed by the employee/applicant and spouse/cohabitant, to certify that the information on the form is current, accurate, and complete. NRC reviews the form for accuracy and completeness and will return the form to the employee/applicant for correction and recertification. If the form is accurate, NRC Personnel Security enter the contents of the form into EVC/LEEP. If there are validation errors, the system will not allow the information to be submitted.

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

N/A. EVC/LEEP is owned and operated by FBI, NRC Personnel Security are only users.

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

In the event an employee/applicant submitted the NRC Form 354 to NRC and needs to correct inaccurate/erroneous information, they must contact the personnel security team. NRC Personnel Security will return the form to the employee/applicant for update, recertification, and resubmission to NRC. If a name check request has already been submitted in EVC/LEEP, NRC Personnel Security will reach out to FBI in the portal to cancel the request. When provided the new NRC Form 354, NRC Personnel Security will submit a new name check request in EVC/LEEP.

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).

FBI, as the system owner, has access to criminal history records in their databases, used to support EVC/LEEP. Criminal record data is available to NRC Personnel Security users with accounts in the system, as applicable to their submitted name checks. Other FBI customers would have access to their own name check information. It is possible that other agencies would be seeking information on the same individuals as the NRC.

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.

EVC/LEEP does not share information with NRC systems. However, after the information on the NRC Form 354 is entered into EVC/LEEP, the form is submitted to the NRC Personnel Security Adjudication Tracking System (PSATS). The form is retained in PSATS as part of the employee/applicant's record.

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

EVC/LEEP is owned and operated by FBI, NRC Personnel Security staff are only users.

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

Agreement Type	
☐	Contract Provide Contract Number:
☐	License Provide License Information:
☒	Memorandum of Understanding Provide ADAMS ML number for MOU: FBI EVC/LEEP: ML23216A015
☐	Other
☐	None

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

NRC is an end user of EVC/LEEP, limited by need-to-know based on roles and responsibilities. The FBI determines the user accounts by accrediting the users and requiring them to sign user agreements. The NRC users only have access to the NRC data for their role-based account, and records that they specifically requested.

FBI customers must apply for user accounts, sign a user agreement, and receive FBI approval to access EVC/LEEP. Once a user is approved, users access the portal via username, password, challenge picture and passcode, and one-time password (OTP). If the end user does not access the system for 90 days, the account will automatically expire. FBI reaches out to customers annually to confirm customers still require system access.

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).

NRC Personnel Security staff access the system from the NRC VPN, using secure (HTTPS) Internet connections.

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

Information in EVC/LEEP is stored by FBI.

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

FBI, as the system owner, controls which agencies can access EVC/LEEP; NRC users access the system at NRC HQ.

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

Yes, all NRC contractors accessing EVC/LEEP are NRC badged personnel.

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

EVC/LEEP allows users to track submission details, dates, and the current stage of processing; all data can be sorted and filtered. NRC users only have access to the NRC data based on roles and responsibilities.

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

N/A.

4.11 Define which FISMA boundary this project is part of.

EVC/LEEP is included as a service under the ADM External Services (AES) subsystem of the Moderate ADM Support System (MASS) FISMA boundary.

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

Authorization Status	
☐	Unknown
☐	No *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*.
☐	In Progress provide the estimated date to receive an ATO. Estimated date:
☒	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: 20180003.

5 Privacy Act Determination

5.1 Is the data collected retrieved by a personal identifier?

Mark the appropriate response.

Response	
☒	**Yes, the PII is retrieved by a personal identifier (i.e., individual's name, address, SSN, etc.)** A unique identifier number is assigned to each name check request. The NRC Personnel Security user will click on a link on a returned name check to see the report. If the name check located any sensitive information at all, the report will be revealed in the portal to the original requester.
☐	**List the identifiers that will be used to retrieve the information on the individual.**
☐	**No, the PII is not retrieved by a personal identifier.** **If no, explain how the data is retrieved from the project.**

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	
☒	***Yes, this system is covered by an existing SORN. (See existing SORNs: https://www.nrc.gov/reading-rm/foia/privacy-systems.html)*** ***Provide the SORN name, number, (List all SORNs that apply):*** NRC SORN-39 – "Personnel Security Files and Associated Records" FBI Central Records System (CRS), FBI-002: • 63 FR 8659, 8671* • 66 FR 17200 • 66 FR 29994
☐	**SORN is in progress**
☐	**SORN needs to be created**
☐	**Unaware of an existing SORN**
☐	**No, this system is not a system of records and a SORN is not applicable.**

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	
☒	**Privacy Act Statement:** NRC Form 354, “Data Report On Spouse”
☐	**Not Applicable**
☐	**Unknown**

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

PII disclosure is mandatory, needed to uniquely identify the employee/applicant to support their initial or continuing eligibility for a security clearance and/or NRC access authorization.

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** 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?

☐	NUREG-0910, "NRC Comprehensive Records Disposition Schedule"
☒	NARA's General Records Schedules
☒	Unscheduled *Please note, after the NRC Form 354 information is entered into EVC/LEEP, the form is retained in NRC PSATS. Retention for the NRC Form 354 is documented in the PSATS PIA.*

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

System Name (include sub-systems, platforms, or other locations where the same data resides)	EVC/LEEP
Records Retention Schedule Number(s)	GRS 5.6 item 170 – Personnel security investigative reports. Personnel suitability and eligibility investigative reports Additional information/data/records 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.
Approved Disposition Instructions	*Please note, after the NRC Form 354 information is entered into EVC/LEEP, the form is retained in NRC PSATS. Retention for the NRC Form 354 is documented in the PSATS PIA.* GRS 5.6 item 170 **Temporary**. Destroy in accordance with the investigating agency instruction. Additional information/data/records 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.
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.	N/A
Disposition of Temporary Records Will the records/data or a composite be automatically or manually deleted once they reach their approved retention?	N/A
Disposition of Permanent Records 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? **NRC Transfer Guidance (Information and Records Management Guideline - IRMG)**	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?

Yes - NRC Form 354, “Data Report on Spouse” (OMB No. 3150-0026).

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?

Yes, 10 CFR Part 25.

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.

8 Privacy Act Determination

Project/System Name: Enterprise Vetting Center / Law Enforcement Enterprise Portal (EVC/LEEP)

Submitting Office: Office of Administration (ADM)

Privacy Officer Review

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

Comments:

Covered by NRC SORN-39 – Personnel Security Files and Associated Records and FBI Central Records System (CRS), FBI-002:

Reviewer's Name	Title
Sally A. Hardy Signed by Hardy, Sally on 02/27/24	Privacy Officer

9 OMB Clearance Determination

NRC Clearance Officer Review

Review Results	
☐	No OMB clearance is needed.
☐	OMB clearance is needed.
☒	Currently has OMB Clearance. Clearance No. 3150-0026

Comments:

Reviewer's Name	Title
 Signed by Cullison, David on 02/23/24	Agency Clearance Officer

10 Records Retention and Disposal Schedule Determination

Records Information Management Review

Review Results	
☐	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 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 02/23/24	Sr. Program Analyst, Electronic Records Manager

11 Branch Chief Review and Concurrence

Review Results	
☐	This project/system **does not** collect, maintain, or disseminate information in identifiable form.
☒	This project/system **does** collect, maintain, or disseminate information in identifiable form.
☒	I concur with the Privacy Act, Information Collections, and Records Management reviews.

Signed by Feibus, Jonathan
on 02/27/24

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

ADDITIONAL ACTION ITEMS/CONCERNS

Name of Project/System: Enterprise Vetting Center / Law Enforcement Enterprise Portal (EVC/LEEP)	
Date CISD received PIA for review: December 7, 2023	**Date CISD completed PIA review:** February 26, 2024
Action Items/Concerns:	
Copies of this PIA will be provided to: *Gwendolyn Hayden* *Acting Director* *IT Services Development and Operations Division* *Office of the Chief Information Officer* *Jonathan Feibus* *Chief Information Security Officer* *Chief Information Security Division* *Office of the Chief Information Officer*	