Introduction:

The Department of the Interior (DOI) requires the DI-4001 Privacy Impact Assessments (PIA) form to be conducted and maintained for all IT systems that collect, maintain, use, or share personally identifiable information (PII), whether the system is new, undergoing significant modification, or already in operation as well as electronic collections under the Paperwork Reduction Act. The PIA is a critical tool for evaluating privacy risks, documenting safeguards, ensuring compliance with the E-Government Act of 2002 (Section 208) and OMB Guidance. This form must be completed electronically and submitted to the Department Privacy Office for review and determination via our Privacy Office Support Request Page. For further guidance, consult the DOI PIA Guide.

System Information

System or Project Name:	Grand Coulee Power Office Federal Fire Department
System or Project Acronym:	GCPO-Fire RMS
Date submitted for review:	April 17, 2026
System Operational Status:	Initiation

Point of Contact

Name:	Dianna Taylor
Title:	Privacy Officer
Office:	Office of the Chief of Information Officer
Phone:	703-787-1763
E-mail:	dianna_taylor@ios.doi.gov

Section 1: System Overview

1. What triggered this PIA? (Check one)

☒ New System
☐ Significant Modification
☐ New Electronic Collection
☐ Other: Describe below

This PIA is being conducted due to the implementation of the First Due Records Management System (RMS) as a new system for the Bureau of Reclamation (BOR), Grand Coulee Power Office Fire Department. The system supports fire protection, emergency response, and operational management activities, including the collection and processing of personally identifiable information (PII) related to fire personnel and members of the public involved in emergency incidents.

As a new system, the RMS introduces the collection, use, and maintenance of PII within a centralized records management platform. This PIA evaluates these activities to ensure compliance with the Privacy Act of 1974, the E-Government Act of 2002, and applicable Department of the Interior (DOI) privacy policies and requirements.

2. What is the purpose of the system or project?

The First Due Records Management System (RMS) supports the Bureau of Reclamation (BOR), Grand Coulee

Power Office Fire Department in carrying out fire protection, emergency response, and operational management activities. The system is used by authorized personnel to document fire and emergency medical services (EMS) incidents, inspections, training, certifications, and personnel activities.

The RMS provides a centralized capability to create, maintain, and retrieve records related to fire and EMS operations. It enables real-time documentation of incident response, supports tracking of training and certifications, and facilitates management of equipment, inspections, and operational readiness. The system may include information related to members of the public involved in fire or EMS incidents, as well as information about fire department personnel.

Information in the RMS is used to support mission-critical emergency response, incident documentation, operational oversight, and compliance with applicable federal, state, and local requirements. Where personally identifiable information (PII) is involved, it is used to accurately document incidents, support continuity of care, and maintain accountability for response activities.

By supporting accurate recordkeeping, coordination, and reporting, the RMS enhances operational efficiency, accountability, and continuity of care, directly supporting BOR's mission to protect life, property, and critical infrastructure.

3. Is the system registered in BisonGRC?

☒ Yes: If applicable What is the project's UII code?
☐ No: Explain why this is not either done or required.

The First Due Records Management System (RMS) is registered in BisonGRC as a subsystem under the Bureau of Reclamation General Support System (BOR-0018-GSS). The system is tracked within BisonGRC as part of the Authorization and Assessment (A&A) process, including associated security categorization, privacy documentation, and system inventory records.

4. What legal authorities authorize the collection and use of data in this system or project?

The collection and use of data within the First Due Records Management System (RMS) is authorized under the following authorities:

- **Privacy Act of 1974, 5 U.S.C. § 552a** – Establishes requirements for the collection, maintenance, use, and disclosure of records containing personally identifiable information (PII). This is relevant because the RMS maintains records related to fire personnel and members of the public involved in fire and emergency medical service (EMS) incidents that may be retrieved by personal identifiers.
- **E-Government Act of 2002, Pub. L. No. 107-347, § 208** – Requires federal agencies to conduct Privacy Impact Assessments (PIAs) for systems that collect, maintain, or disseminate PII. This PIA is conducted to ensure transparency and compliance with federal privacy requirements.
- **OMB Circular A-130, "Managing Information as a Strategic Resource"** – Establishes federal policy for the management of information resources, including privacy and security requirements. The RMS must comply with these requirements to ensure proper safeguarding and management of PII.
- **Department of the Interior Manual, 383 DM 1–13, "Privacy Act Policy and Responsibilities"** – Provides DOI policy governing the management of PII and outlines responsibilities for system owners and

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

program officials. The RMS operates in accordance with these Departmental Privacy requirements.

- **Federal Fire Prevention and Control Act of 1974, 15 U.S.C. § 2201 et seq.** – Establishes federal support for fire prevention, control, training, and data systems to reduce loss of life and property from fire. This is relevant because the RMS supports fire incident reporting, emergency response documentation, and related operational activities.
- **Reclamation Act of 1902, 43 U.S.C. § 371 et seq.** – Provides the Bureau of Reclamation (BOR) with authority to manage and operate federal facilities and infrastructure. This is relevant because the RMS supports fire protection and emergency response operations that protect BOR-managed facilities and personnel.

In addition, the system operates in accordance with applicable federal privacy and information management policies, including OMB Circular A-130 and Department of the Interior Manual 383 DM 1–13.

The RMS supports incident reporting and records management practices aligned with nationally recognized fire and emergency services standards (e.g., National Fire Protection Association (NFPA) standards). These standards inform the type of operational data collected but do not independently authorize the collection, use, or maintenance of PII.

5. Does the system or project require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: If yes, list the applicable citations below.
☐ No

The First Due Records Management System (RMS) retrieves records by personal identifiers, including full name, EMS responder license number, user account identifier, and other identifying information related to fire personnel, authorized system users, and members of the public involved in Fire/EMS incident and emergency response records. Because records may be retrieved by personal identifier, the system meets the Privacy Act definition of a system of records.

At this time, INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service (EACS)), 72 FR 11040 (March 12, 2007), as modified at 86 FR 50156 (September 7, 2021), provides coverage for identity, credential, authentication, logical access, and system access records associated with authorized users of the system.

INTERIOR/DOI-47 does not cover Fire/EMS operational records, EMS documentation, incident reports, patient-related information, emergency response documentation, responder activity records, or related operational records maintained in First Due RMS. The Department Privacy Office is developing a new Department of the Interior SORN to provide formal Privacy Act notice for these Fire/EMS operational and EMS-related records. While the new SORN is being developed, this PIA provides initial transparency regarding the system's purpose, categories of individuals, categories of records, PII collected and maintained, intended uses, sharing practices, safeguards, retention considerations, access and amendment processes, and breach response procedures. This PIA does not replace the required SORN and will be updated, as appropriate, once the SORN is published.

6. Does this project involve an information collection that requires OMB approval under the Paperwork Reduction Act?

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

☐ Yes
☒ No

The First Due Records Management System (RMS) does not collect information directly from members of the public through standardized forms or surveys. Information related to members of the public is documented by authorized personnel as part of fire and emergency medical service (EMS) response activities. As the data collection does not involve 10 or more members of the public completing identical questions or a public-facing collection instrument, the requirements of the Paperwork Reduction Act do not apply.

7. List all minor applications or subsystems that are hosted on this system and covered under this PIA.

The First Due Records Management System (RMS) does not host any minor applications or subsystems. All functionality is integrated within the primary platform and there are no separately managed components covered under this PIA.

Section 2: Data Description and Use

1. What categories of PII and sensitive data types will the system collect, use, or store? Check all that apply.

☒ Name (full, first or last)	☐ Home telephone number	☐ Employment or resume info
☐ Aliases/nickname	☐ Personal Email	☐ Full or Truncated SSN
☐ Driver's license	☒ Mailing or home address	☐ Physical characteristics
☐ Citizenship	☐ Religious preference	☐ Biometrics/facial recognition
☐ Legal Status	☐ Mother's maiden name	☐ Vehicle information
☐ Sex	☐ Marital status	☐ Passport information
☐ Race or ethnicity	☐ Spouse Information	☐ Travel information
☒ Date of birth	☐ Child or family information	☐ Parent's name
☐ Place of birth	☒ Emergency contact info	☐ Credit card number
☐ Personal cell phone number	☐ Financial information	☐ Nationality
☒ Username / user ID / acct ID	☒ IP address / network ID	☒ Device ID / online ID
☐ Geolocation / GPS / location	☒ Photos / video / audio	☒ Health / medical information
☐ Tribal or other ID number	☐ Education information	☒ Disability Information
☐ Criminal / disciplinary info	☐ Military records	☐ Other: Describe below

The system collects and maintains personally identifiable information (PII) related to fire department personnel and members of the public involved in emergency response activities. This includes personnel names and professional certification or license numbers used to manage system access, document incident response activities, and support operational accountability.

EMS personnel license numbers are associated with incident reports and may be linked to identifiable individuals participating in emergency response activities.

The system also processes PII related to members of the public receiving emergency medical services. EMS response documentation may include patient information such as name, mailing address, and date of birth. In addition, the system may contain medical or health-related information, including patient condition

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

observations, medical assessments, treatments provided, and changes in patient condition recorded during emergency response activities.

This information is collected and maintained to support incident documentation, operational reporting, and continuity of care during emergency response activities.

The system may also maintain user account identifiers, IP or network identifiers, device or online identifiers, emergency contact information, photos or other incident-related media, disability-related information, audit logs, and system activity records where those elements are necessary for system access, incident documentation, EMS response, operational accountability, or security monitoring.

2. What is the source for the PII collected? Check all that apply.

☒ Individual
☐ Federal Agency
☐ Tribal Agency
☐ Local Agency
☒ DOI Records
☐ Third Party Records
☐ State Agency
☐ Other: *Describe Below*

The system manages login credentials for authorized federal employees and contractors using PIV/CAC authentication. These credentials, including user identifiers and authentication certificates, are considered personally identifiable information (PII) as they are uniquely linked to individual users.

Access to the system is restricted to authorized personnel and is controlled through role-based access controls and multi-factor authentication. Credentials are not collected from or used by members of the public. All authentication processes are managed in accordance with DOI Identity, Credential, and Access Management (ICAM) requirements and applicable federal security standards.

In addition to authentication data, the system collects and maintains PII related to members of the public involved in fire and emergency medical service (EMS) response activities. This information is obtained from individuals during emergency response interactions and is documented in the system by authorized personnel based on observations and information provided at the scene.

All information is entered into the system by authorized personnel and is subject to standard operational review processes to support accuracy and completeness.

3. How will the information be collected? Check all that apply.

☐ Paper Format
☐ Email
☒ Face-to-Face Contact
☒ Website
☐ Fax
☐ Telephone Interview
☒ Shared Between Systems: *Describe*
☒ Other: *Describe*

The system collects PII through the following methods:

- **Website** – Authorized personnel access the system through secure web-based and mobile interfaces (SaaS platform) to enter and manage incident reports, personnel data, and EMS documentation. Data

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

transmission is protected using HTTPS encryption and access is restricted through role-based access controls and multi-factor authentication.

- **Information Shared Between Systems** – Personnel identity and access information is obtained from DOI identity and access management systems to support authentication and account management. Data is transmitted through secure, DOI-approved processes.
- **Face-to-Face Contact** – Information related to members of the public is obtained during in-person emergency response interactions and is subsequently documented in the system by authorized personnel.
- **Other (Operational Data Entry)** – Internal operational forms are completed by authorized personnel to document fire and EMS activities. These forms are entered into the system as part of routine operations.

4. What is the intended use of the PII collected?

The First Due Records Management System (RMS) collects and uses PII to support fire protection, emergency response, and operational management activities.

- **System Access Control and Authentication** – PII such as names and user identifiers is used to verify identity, manage user accounts, and assign role-based access in accordance with DOI identity and access management requirements.
- **Incident Documentation and Reporting** – PII is used to document fire incidents and response activities, including identifying personnel involved and maintaining accurate operational records.
- **EMS Response Documentation and Continuity of Care** – PII related to members of the public is used to document emergency medical service (EMS) activities, including patient information necessary to support treatment, coordination, and continuity of care.
- **Operational Recordkeeping and Accountability** – PII is used to support internal recordkeeping, track personnel certifications and activities, and ensure accountability for fire and EMS operations.
- **Compliance with Regulatory Requirements** – PII is used to meet applicable regulatory and reporting requirements, including National Fire Protection Association (NFPA) standards and other legal obligations.

All uses of PII are directly related to the operational purpose of the system and are not used for unrelated purposes such as profiling or marketing. Use of PII will be aligned with applicable Privacy Act requirements. The Department Privacy Office is developing a new SORN to provide formal Privacy Act notice for Fire/EMS operational and EMS-related records. This PIA provides initial transparency regarding the system's collection, use, sharing, retention, safeguards, and individual access and amendment processes while the SORN is being developed but does not replace the required SORN.

5. How does this project limit the collection and use of PII to only what is necessary?

The system is designed to collect only the minimum necessary PII for operational, reporting, and compliance purposes.

- **Limited Data Collection** – Data fields are restricted to information required to support fire incident reporting, EMS documentation, personnel management, and system access. Social Security Numbers (SSNs) and other unnecessary sensitive data elements are not collected.
- **Operational Relevance** – PII related to members of the public is limited to information necessary to

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

document emergency response activities and support continuity of care. Personnel data is limited to identifiers and credentials required for authentication and operational accountability.

- **Access Controls** – Access to PII is restricted through role-based access controls, ensuring that only authorized personnel with a need to know can view or use the information. All authentication processes follow DOI Identity, Credential, and Access Management (ICAM) requirements.
- **System Configuration and Review** – Data collection is limited through system configuration and is periodically reviewed to ensure continued alignment with operational needs and to prevent the collection of unnecessary data elements.

Through these measures, the system ensures that the collection and use of PII is limited to what is directly relevant and necessary to accomplish its mission.

Section 3: Data Sharing and Individual Rights

1. With whom will the PII be shared, both within DOI and outside DOI? Check all that apply.

☒ **Within the Bureau/Office:** Describe how the data will be used below.
☒ **Tribal, State or Local Agencies:** Describe how the data will be used below.
☐ **Other Bureaus/Offices:** Describe how the data will be used below.
☒ **Contractor:** Describe how the data will be used below.
☐ **Other Federal Agencies:** Describe the federal agency and how the data will be used
☒ **Other Third-Party Sources:** Describe how the data will be used below.

The First Due Records Management System (RMS) shares PII only with authorized recipients to support fire protection, emergency response, and regulatory compliance.

- **Within the Bureau/Office (Bureau of Reclamation)** – PII is shared with authorized fire department personnel for operational purposes, including incident reporting, EMS documentation, and internal coordination. Access is restricted through role-based access controls and audit logging.
- **Contractors** – Authorized contractors supporting system operations and maintenance may access PII as necessary to perform their duties. Access is governed by contract requirements, including Privacy Act clauses and nondisclosure provisions.
- **Other Federal Agencies** – PII may be shared with other federal agencies for emergency response coordination, law enforcement activities, and regulatory compliance, as authorized.
- **Tribal, State, or Local Agencies** – PII may be shared with emergency response partners to support coordinated response efforts and continuity of care.
- **Other (Hospitals and Legal Disclosures)** – PII may be disclosed to hospitals for continuity of care and in response to legal processes such as court orders or subpoenas, in accordance with applicable laws and policies.

All sharing is limited to the minimum necessary and must be supported by applicable legal authority, DOI policy, and Privacy Act requirements. The Department Privacy Office is developing a new SORN to document the routine uses and disclosure practices for Fire/EMS operational and EMS-related records. While the SORN is being developed, this PIA provides initial transparency regarding anticipated sharing practices. Data is transmitted using secure methods consistent with DOI security policies.

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

2. Does this system have an MOU/MOA/ISA with other Federal Agencies or State/Local/Tribal Agencies with which it shares information?

☐ Yes
☒ No

The system does not currently rely on a system-specific MOU, MOA, or ISA solely for routine internal use of First Due RMS. However, Fire/EMS records may be shared with emergency response partners, hospitals, contractors, or other authorized recipients when necessary to support emergency response, continuity of care, regulatory compliance, legal process, or system maintenance. Any recurring external sharing will be reviewed to determine whether a written agreement, mutual aid arrangement, interconnection agreement, contract provision, or other documented authorization is required. Sharing will be limited to authorized purposes and aligned with applicable legal authority, DOI policy, and the new SORN being developed for Fire/EMS operational and EMS-related records.

3. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII? If not, what steps are in place to ensure individuals are aware of how their information is being used?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*
☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

Individuals providing PII to the First Due Records Management System (RMS) are informed of how their information will be used and, in limited cases, may decline to provide certain information where practicable.

- **System Access (Employees and Contractors)** – Only the minimum required PII (e.g., name and user identifiers) must be provided for system access. This information is necessary to authenticate users, assign roles, and maintain accountability for system use. Individuals are informed of the use of their information through applicable policies and system access requirements.
- **Emergency Response (Members of the Public)** – PII is collected as part of fire and emergency medical service (EMS) response activities. While individuals may not be able to decline providing information necessary for emergency response and treatment, they are informed of how their information will be used through applicable privacy notices and statements provided where practicable.
- **Notice and Use of Information** – A Privacy Act Statement is provided at the time information is collected, where practicable, and informs individuals of the authority, purpose, routine uses, and whether providing the information is mandatory or voluntary.

Declining to provide required PII will prevent system access for authorized users or may limit the ability to provide emergency services where information is necessary for treatment and documentation. Use of PII will be consistent with this PIA and will be covered under a new System of Records Notice (SORN) currently being developed.

4. How does the project provide notice to individuals prior to the collection of information? Check all that apply.

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

☒ Privacy Act Statement: ☐ Other: *Describe Below*
☐ Privacy Notice: ☐ None: *Example - law enforcement cases.*

The project provides a Privacy Act Statement (PAS) at the point of collection where practicable. The PAS informs individuals of the authority for collection, the purpose of the information, routine uses, and whether providing the information is voluntary or mandatory.

For federal employees and contractors, the PAS and related notice are provided through system access requirements, user agreements, and applicable policies that describe how PII is collected, used, and protected.

For members of the public, PII is collected during fire and emergency medical service (EMS) response activities. In emergency situations, providing notice prior to collection may not always be feasible; however, a Privacy Act Statement will be provided where practicable. Information is collected only as necessary to support emergency response, documentation, and continuity of care.

5. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Records in the system are retrieved through secure search functions and reporting tools available to authorized users. Records may be retrieved using the following identifiers:

- **Incident Case/Report Number** – Used to retrieve specific incident reports and associated EMS documentation.
- **Event Date and Incident Location** – Used to search for records related to specific emergency response events.
- **EMS Responder License Number** – Used to retrieve records associated with specific personnel involved in response activities.
- **Full Name** – Used to retrieve records related to fire personnel and members of the public involved in incidents.

Because records may be retrieved by personal identifiers, including full name and EMS responder license number, the system meets the definition of a Privacy Act system of records. The Department Privacy Office is developing a new SORN to provide formal Privacy Act notice for Fire/EMS operational and EMS-related records. This PIA offers preliminary transparency about retrieval practices and privacy safeguards, but does not substitute for the required SORN.

6. Will reports be produced on individuals, whose PII is contained in this system? If yes, who has access and what is the purpose of these reports?

☒ Yes: Describe the use of these reports and who will have access to them.
☐ No

Types of Reports:

- **Incident and EMS Reports** – Document emergency response activities, including personnel involved and

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

information related to members of the public receiving services.

- **Operational and Personnel Reports** – Summarize responder activity, certifications, and participation in incidents.
- **Audit and Compliance Reports** – Track system access, user activity, and data changes to support accountability and regulatory compliance.

Access and Purpose:

Access to these reports is restricted to authorized fire department personnel, supervisors, and system administrators with a need to know. Reports are used for incident documentation, operational management, compliance monitoring, and audit purposes. Access is controlled through role-based permissions and system activity is logged to prevent unauthorized use.

7. How will data collected from sources other than DOI records be verified for accuracy?

PII collected from sources other than DOI records is verified through a combination of automated validation, manual review, and operational procedures.

- **Operational Verification** – PII related to members of the public is collected during fire and emergency medical service (EMS) response activities and is verified by authorized personnel at the time of collection to the extent practicable based on information provided by individuals, observations, and available documentation.
- **Automated Validation** – The system applies validation checks (e.g., required fields and data format) during data entry to ensure completeness and consistency.
- **Manual Review** – Incident reports and EMS documentation are reviewed by authorized personnel to identify and correct errors or inconsistencies.
- **Cross-Referencing with Official Records** – Where applicable, personnel information may be compared against official records (e.g., certification or identity records) to ensure accuracy.

These processes support the accuracy, relevance, timeliness, and completeness of records in accordance with Privacy Act requirements.

Section 4: Data Management and Retention

1. What is the retention period for the data and under what records schedule?

The Grand Coulee Power Office Federal Fire Department Records Management System (GCPO-Fire RMS) retains data in accordance with Department of the Interior (DOI) and National Archives and Records Administration (NARA)–approved records schedules:

- **Fire and EMS Incident Records** – Retained in accordance with Wildland Fire Records Schedule 2.1.2.06 (ADM-11.00), Mission – Natural & Cultural Resources – Disaster & Incident Management. Historically significant records are designated as permanent (PERM) and retained in accordance with National Archives and Records Administration (NARA) approved disposition requirements.

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

- **Training and Certification Records** – Retained in accordance with Training Reports Records Schedule 1.2.05 (PER-14.00), Administrative – Human Resources – Long-term Records. Records are retained for seven (7) years after the end of the fiscal year and are securely destroyed in accordance with approved disposition requirements.

- **Inspection, Equipment, and Maintenance Records** – Retained in accordance with Inspection Report Records Schedule 2.2.4.22 (PRJ-8.10), Mission – Sustainably Manage Water – Water Project Contracts, Engineering & Quality Records. Records are retained for seventy-five (75) years following the triggering event and are managed in accordance with approved disposition requirements.

- **User Activity/System Use Records, and Audit Logs/System Activity** Records – Retained in accordance with Records Schedule 1.4.14, Administrative – Information Technology – Documentation Records. Records are retained for three (3) years and are securely destroyed or purged in accordance with approved records disposition requirements.

All records are disposed of in accordance with NARA-approved schedules and DOI records management policies. Electronic records are destroyed using secure media sanitization methods consistent with NIST SP 800-88, Rev. 1, where applicable.

2. What measures are in place to validate the accuracy and completeness of data received from external sources?

The system applies multiple measures to validate the accuracy and completeness of data received from external sources, including information provided by members of the public during emergency response activities and, where applicable, external personnel or agency records.

- **Automated Validation** – The system performs validation checks on incoming data, including required field completion and data format validation, to ensure consistency and completeness at the time of entry.
- **Operational Verification** – Information collected during fire and emergency medical service (EMS) response activities is verified by authorized personnel at the time of collection to the extent practicable based on information provided by individuals, observations, and available documentation.
- **Manual Review** – Incident reports and EMS documentation are reviewed by authorized personnel and supervisors to identify errors, inconsistencies, or incomplete information.
- **Cross-Referencing with External or Authoritative Records** – Where applicable, personnel information or supporting data may be compared against external records (e.g., certification or agency records) to ensure accuracy.
- **Error Correction Process** – When discrepancies are identified, records are updated based on corrected information obtained from individuals or supporting documentation.

These measures ensure that externally sourced data is accurate, relevant, timely, and complete in accordance with Privacy Act requirements.

3. Does the project include logging capabilities to record and monitor access to PII?

☒ Yes

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

☐ No

The system includes logging capabilities to record and monitor access to PII for security, accountability, and audit purposes.

- **Types of Logs** – Audit logs, user access logs, and system activity logs capture user authentication, access to records, and data modifications.
- **PII-Related Activities Monitored** – Logging tracks activities involving PII, including viewing, creating, modifying, and deleting records, as well as administrative actions.
- **Log Protection** – Logs are protected through system security controls, including role-based access restrictions, and maintained in a secure environment to prevent unauthorized access or tampering.
- **Log Review and Monitoring** – Logs are reviewed regularly by authorized personnel to support oversight, incident response, and compliance.
- **Retention** – Log retention is managed in accordance with applicable DOI and NARA-approved records schedules.

Section 5. Privacy Risks and Mitigation Strategies

1. What privacy risks are associated with the collection, use, retention, and disclosure of PII, and how are they mitigated at each stage of the information lifecycle?

The system collects, uses, retains, and shares PII to support fire protection, emergency response, and operational management. Privacy risks have been identified at each stage of the information lifecycle, with mitigations implemented to address those risks.

Collection Risks – Risks include over-collection of PII.

- **Mitigation:** Data minimization practices are applied to ensure only the information necessary for operational and compliance purposes is collected. Administrative safeguards and privacy training support proper collection practices.

Use Risks – Risks include unauthorized access and inaccurate use of PII.

- **Mitigation:** Access is restricted through role-based access controls and multi-factor authentication. Audit logging is implemented to monitor user activity, and privacy training reinforces appropriate use of information.

Retention Risks – Risks include excessive retention of PII.

- **Mitigation:** Data is retained in accordance with DOI and federal standards. Administrative and physical safeguards support proper storage and secure disposition of records.

Disclosure Risks – Risks include unauthorized disclosure of PII.

- **Mitigation:** Encryption, role-based access controls, and administrative and physical safeguards are used

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

to protect PII. Sharing is limited to authorized recipients in accordance with DOI and federal standards.

These mitigations—including role-based access controls, multi-factor authentication, encryption, administrative and physical safeguards, privacy training, audit logging, and data minimization—ensure that risks related to unauthorized access, over-collection, inaccurate use, excessive retention, and unauthorized disclosure are appropriately managed.

2. Does the system generate new data or inferences through aggregation or analytics that may influence decisions or individual records? If so, how are those data verified, used, and protected?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*
☒ No

The system does not generate new data or inferences through aggregation or analytics. It records and reports information as entered by authorized personnel, and outputs are based only on existing records.

3. Will the new data be placed in the individual's record?

☐ Yes: *Provide explanation below*
☒ No

The system does not generate new or derived data; therefore, no new data is added to an individual's record beyond what is directly collected and entered.

4. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Provide explanation below*
☒ No

The system does not generate new data or perform analytics; therefore, it does not make determinations about individuals beyond the information directly collected and recorded

5. How will the new data be verified for relevance and accuracy? Enter N/A if new data is not derived or created.

N/A. There is no new or inferred data is created

Section 6: Automated Decision-Making and AI Risk Management

1. Does the system use AI, machine learning, or have a non-operational AI Component?

☐ Yes
☒ No, *Proceed to Section 7.*

2. How are models validated for fairness, accuracy, and transparency?

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

N/A.

3. Are individuals notified of AI-based decisions that affect them?

☐ Yes
☐ No

N/A.

4. Are safeguards in place to prevent bias or unintended consequences?

☐ Yes
☐ No

N/A.

5. Are models periodically reviewed or retrained to ensure ongoing reliability?

☐ Yes
☐ No

N/A.

6. Is federated learning used for privacy-preserving model training?

☐ Yes
☐ No

N/A.

Section 7: Security and Access Controls

1. Who will have access to project data and how is access determined, authorized, and restricted? Check all that apply and respond in the space below.

☒ Users
☐ Contractors
☒ Developers
☒ System Administrator
☐ Other: *Describe below*

Access to project data is restricted to authorized fire department personnel, system administrators, and contractors whose roles require access to perform operational or system support functions.

- **Users (Fire Department Personnel)** – Have role-based access to create, view, and update incident reports, EMS documentation, and operational records necessary to perform their duties.

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

- **System Administrators** – Have administrative access to manage system configuration, user accounts, and system maintenance.
- **Contractors** – Have limited, role-specific access for system maintenance and support, as authorized.

Authorization and Restrictions:
Access is granted according to written approval from relevant managers or system officials. Role-based access controls (RBAC) are used to limit access to only the data necessary for each user's role. Multi-factor authentication (MFA) is required for system access, and user access is reviewed periodically to ensure continued authorization.

2. What data protection policies apply to cloud-based PII storage?

The system is hosted in a DOI-approved cloud environment that has been validated as FedRAMP High authorized, as applicable to the approved system boundary. Cloud-based PII storage complies with DOI cloud security requirements, FedRAMP requirements, NIST SP 800-53 Rev. 5, and the applicable system authorization package. Cloud-based PII storage complies with:

- **DOI Cloud Computing Policy** – Requires use of DOI-approved cloud service providers that meet federal security and privacy requirements.
- **FedRAMP Authorization Requirements** – Ensures implementation of NIST SP 800-53 Rev. 5 security controls at the appropriate impact level.
- **NIST SP 800-53 Rev. 5** – Provides security and privacy controls governing access, encryption, auditing, and incident response.
- **NIST SP 800-144** – Provides guidance for securing cloud computing environments and protecting sensitive information.

PII is encrypted at rest and in transit using FIPS-validated cryptographic standards. Access to cloud-stored PII is restricted through role-based access controls (RBAC) and multi-factor authentication (MFA). System activity is logged and monitored to support continuous monitoring and incident response.

The cloud provider's security controls are expected to meet DOI and federal requirements for the protection of PII, pending confirmation of FedRAMP authorization status and level.

3. How does the system monitor and detect unauthorized access, use, or exfiltration of PII?

The system uses multiple monitoring capabilities to detect and respond to unauthorized access, use, or exfiltration of PII.

- **System Monitoring and Logging** – Audit logs and system monitoring tools track user activity, access to records, and system events to identify unusual or unauthorized behavior.
- **Intrusion Detection and Alerts** – Intrusion detection capabilities and automated alerts are used to identify suspicious activity, such as failed login attempts or abnormal access patterns.
- **Activities Monitored** – Monitoring includes user authentication, access to PII, data modifications, and other system activities that may indicate unauthorized use or potential exfiltration.
- **Incident Response** – Security and privacy incidents are reported to DOI-CIRC and the Privacy Officer and are handled in accordance with DOI incident response procedures and federal requirements.

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

These layered controls enable the system to detect potential breaches early, contain unauthorized activity and support compliance with DOI and federal privacy and security requirements.

4. Does the project include any monitoring of user activity or tracking of individuals? If so, what controls ensure the appropriate use of this capability by authorized personnel?

☒ Yes: describe what controls ensure authorized and appropriate use of this capability.
☐ No

The system includes monitoring of user activity to support system security, operational oversight, and compliance with federal requirements.

- **Monitored Activities** – User activity monitoring includes login attempts, access to records and PII, and record creation, modification, and deletion.
- **Controls for Appropriate Use** – Access to monitoring data is restricted to authorized personnel with a documented need-to-know, including system administrators and security personnel. Monitoring activities are subject to periodic review to ensure appropriate use. Users are informed of monitoring through DOI Rules of Behavior and required privacy and security training, and any use of monitoring data for investigations is conducted in accordance with DOI incident response procedures.

5. Will contractors be involved in the following project activities? Check all that apply.

☒ Design
☒ Development
☒ Maintenance

Contractors are involved in system development and maintenance activities to support system functionality, updates, and operational performance.

- **Development** – Contractors may support system enhancements, updates, and configuration changes.
- **Maintenance** – Contractors perform system maintenance, troubleshooting, and technical support activities.

All contractor personnel with access to PII are required to:

- Comply with applicable Federal Acquisition Regulation (FAR) Privacy Act clauses (e.g., FAR 52.224-1 and 52.224-2)
- Complete DOI-approved privacy and security training
- Follow DOI Rules of Behavior and applicable security policies
- Sign non-disclosure agreements (NDAs), as required

Contractors may have limited, role-based access to PII only when necessary to perform authorized duties such as troubleshooting or system support.

6. What physical, technical, and administrative controls are implemented to protect PII? Check all that apply.

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

Physical Controls

☒ Security Guards
☐ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☐ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Lock
☐ Other: *Describe Below*

Describe the other types of controls implemented.

Technical Controls

☐ Password
☒ Firewall
☒ Encryption
☐ User Identification
☒ Other: *Describe Below*
☐ Intrusion Detection Systems (IDS)
☒ Virtual Private Network (VPN)
☐ Public Key Infrastructure (PKI) Certificates
☐ Biometrics

The system implements additional technical controls, including:

- **Multi-Factor Authentication (MFA)** – Required for all user accounts to ensure secure authentication.
- **Role-Based Access Controls (RBAC)** – Access to PII is restricted to authorized users based on a demonstrated need-to-know.
- **Encryption** – PII is encrypted at rest using FIPS-validated cryptographic standards and in transit via TLS 1.2 or higher.

Administrative Controls

☒ Periodic Security Audits
☐ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Other: *Describe Below*
☒ Methods to Ensure Only Authorized Personnel Have Access
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Records and Privacy Training
☒ Regular Monitoring of Users' Security Practices

The system implements additional administrative controls, including:

- **Incident Response Procedures** – Security and privacy incidents are managed in accordance with DOI incident response and breach response policies. Incidents involving PII are reported to appropriate authorities and handled in accordance with federal requirements.

7. What processes are in place for individuals to file a Privacy Act complaint relating to the project?

Individuals may file a Privacy Act complaint regarding this system through the Department of the Interior's established Privacy Act complaint process:

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

- **Submission Methods** – Complaints may be submitted by email to privacy@doi.gov, by mail to the Departmental Privacy Office, U.S. Department of the Interior, 1849 C Street NW, Washington, DC 20240, or via the DOI FOIA/Privacy Portal.
- **Responsible Office** – The DOI Chief Privacy Officer receives all Privacy Act complaints and assigns them to the appropriate Privacy Officer or Privacy Analyst for review.
- **Review Process** – The assigned reviewer evaluates the complaint, coordinates with the System Owner and relevant program staff, and determines whether a Privacy Act violation or policy issue occurred.
- **Resolution and Response** – DOI provides a written response to the complainant outlining findings and any corrective actions taken, in accordance with DOI procedures.
- **Notice to Individuals** – Information on the right to file a Privacy Act complaint is available through the DOI Privacy Program website and applicable DOI privacy guidance.

This process complies with 43 CFR Part 2, Subpart K, which establishes DOI's procedures for handling Privacy Act concerns.

8. What processes are in place for individuals to access their information?

Individuals may access their records by submitting a written Privacy Act request to the DOI Departmental Privacy Office or the Bureau of Reclamation (BOR) Privacy Office in accordance with the Privacy Act of 1974 (5 U.S.C. § 552a) and DOI regulations at 43 CFR Part 2, Subpart K.

- **Request Methods** – Requests may be submitted using the DI-4016 form, by email to DOI_Privacy@ios.doi.gov, or by mail to the Departmental Privacy Office, U.S. Department of the Interior, 1849 C Street NW, Washington, DC 20240. Requests may also be submitted to the System Manager. The request must include the individual's full name, contact information, a description of the records sought, and proof of identity (e.g., signed declaration under penalty of perjury or notarized statement).
- **Processing and Review** – Upon receipt, the DOI Privacy Office verifies the requester's identity and coordinates with the System Owner and appropriate program offices to locate responsive records.
- **Response** – DOI or BOR responds within the timeframes established in 43 CFR Part 2, Subpart K, providing the requested records or explaining any lawful exemptions or redactions.
- **Notice to Individuals** – Information on how to request access to records is available through the DOI Privacy Program.

This process ensures compliance with the Privacy Act's access provisions and protects the security and privacy of the record

9. What processes are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals may request correction or amendment of their records in accordance with the Privacy Act of 1974 (5 U.S.C. § 552a(d)) and DOI regulations at 43 CFR Part 2, Subpart K.

- **Submission of Amendment Request** – Individuals may submit a written request to the DOI Departmental Privacy Office or the Bureau of Reclamation (BOR) Privacy Office identifying the specific record to be corrected and the reason for the requested amendment.
- **Review and Coordination** – The Privacy Office verifies the requester's identity and coordinates with the

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

System Owner and program officials to determine whether the information is inaccurate, irrelevant, untimely, or incomplete.

- **Determination and Response** – If the amendment is approved, the record is corrected and the individual is notified in writing. If the request is denied, the individual is provided with a written explanation and information on how to appeal the decision.
- **Appeal Process** – Individuals may appeal a denial in accordance with DOI procedures outlined in 43 CFR Part 2, Subpart K.

These procedures let people fix incorrect data and keep records secure.

10. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

Responsibility for assuring proper use of data and reporting any loss, compromise, unauthorized access, or disclosure of PII is shared among designated roles:

- **Information System Owner (ISO)** – Provides overall operational oversight and ensures the system operates in compliance with DOI privacy and security policies. The ISO ensures that agency data is properly managed and that access is granted in a secure and auditable manner.
- **Information System Security Officer (ISSO)** – Oversees the implementation of security controls, monitors system activity, and ensures compliance with the System Security Plan (SSP) and DOI security requirements.
- **Authorized Users** – Are responsible for complying with DOI Rules of Behavior, completing required training, and using PII only for authorized purposes.

All DOI personnel and contractors with access to the system are required to report any loss, compromise, unauthorized access, or disclosure of PII to the DOI Computer Incident Response Center (DOI-CIRC) and appropriate DOI officials within one hour of discovery, in accordance with federal policy and established DOI procedures.

These responsibilities ensure that data is properly managed, access is controlled and auditable, and privacy incidents are promptly reported and addressed.

Section 8: Incident Response and Review

1. In the event of a privacy breach, what steps will be taken to mitigate harm, notify affected individuals, and report to oversight agencies?

In the event of a privacy breach involving the Grand Coulee Power Office Federal Fire Department System (GCPO-Fire RMS), DOI will follow the procedures outlined in the DOI Privacy Breach Response Plan:

1. **Immediate Reporting** – Any suspected or confirmed breach must be reported within one hour of discovery to the DOI Computer Incident Response Center (DOI-CIRC) and the DOI or Bureau Privacy Officer.
2. **Containment and Mitigation** – The Information System Security Officer (ISSO) and DOI-CIRC work to secure affected systems, revoke compromised credentials, and prevent further data loss.

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

3. **Risk Assessment** – The Privacy Officer and breach response team assess the nature and scope of the breach, the sensitivity of the compromised PII, and the potential risk to affected individuals.
4. **Notification** – If required, affected individuals will be notified without unreasonable delay, consistent with OMB M-17-12 and DOI policy, providing:
    - A description of the incident
    - The type of information involved
    - Steps individuals can take to protect themselves
    - DOI contact information for questions and assistance
5. **Oversight Reporting** – DOI will report to OMB, Congress, DHS, and other required oversight bodies when thresholds for major incidents are met.
6. **Remediation and Prevention** – The system team will implement additional controls, update procedures, and retrain personnel to prevent recurrence.

These steps ensure a coordinated, timely, and compliant response to mitigate harm to individuals and uphold DOI's legal obligations.

2. How often will this PIA be reviewed and updated to reflect changes in privacy risks or system operations?

The Grand Coulee Power Office Federal Fire Department System (GCPO-Fire RMS) Privacy Impact Assessment will be reviewed and updated at least once every three years, in accordance with DOI policy and OMB requirements. Interim updates will occur sooner if any of the following events take place:

- Significant changes to system functionality, architecture, or hosting environment
- Collection of new categories of PII or expansion of data use beyond what is described in the current PIA
- New data sharing agreements or partnerships
- Implementation of emerging technologies (e.g., AI/ML features, cloud service changes) that could alter privacy risks
- Changes to applicable privacy laws, regulations, or DOI policies

The System Owner is responsible for initiating the review process in coordination with the DOI or Bureau Privacy Officer. All updated PIAs will undergo the standard review and approval process and be made publicly available on DOI's website unless publication is prohibited for security or law enforcement reasons.

Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.