U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Integrated Resource Management Applications (IRMA)
Bureau/Office: National Park Service/Natural Resource Stewardship & Science (NRSS) Directorate
Date: January 20, 2021
Bureau/Office Contact Title: NPS Associate Privacy Officer
Point of Contact
Name: Felix Uribe
Email: nps_privacy@nps.gov
Phone: (202) 354-6925
Address: 12201 Sunrise Valley Drive, MS 242, Reston, VA 20192

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☐ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☒ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Natural Resource Stewardship & Science Directorate's (NRSS) Integrated Resource Management Application (IRMA) is a web-based “one-stop” solution that provides NPS Resource managers the information needed to make informed resource management decisions. Additionally, IRMA makes NPS natural resource data and research available to the

general public. IRMA systems may be accessed through a single IRMA portal via web browsers or dedicated desktop client tools for specific functions.

IRMA does not maintain or display personally identifiable information (PII) beyond the limited data described in this privacy impact assessment. PII stored is primarily for the creation and management of user accounts and to allow registered users to interact with NPS. Limited incidental PII may be maintained to track metadata on specific items to properly cite the creator or origin of some content.

IRMA is an on-premise FISMA rated Moderate-risk application that leverages many of its privacy and security controls through the Department of the Interior's Enterprise Service Network (ESN) and National Park Service's One GSS, hybrid controls with some custom application-specific controls hosted on Windows Server infrastructure. All IRMA systems are managed following a common governance model, infrastructure, and management procedures. Tools and settings are available to system administrators to manage user accounts, maintain security and access controls, and specify terms of use for data.

IRMA enables access for DOI authorized employees, contractors, and volunteers (collectively, DOI users) through the use of the Personal Identity Verification (PIV) Credentials and DOI Active Directory using User Principal Name (UPN) or UserID attributes for authentication and role/permission management. DOI users must complete a background check, are required to sign the DOI's Rules of Behavior, and must complete security and privacy training prior to accessing a DOI computer system or network.

Non-DOI users, including users from other federal agencies, local governments, tribal organizations, universities or the general public, may voluntarily self-register by creating a user account with the Partner Security Token Service (PSTS) for the intent of interacting with specific subsystems. The PSTS provides multifactor authentication using a valid e-mail account and a temporary encrypted account confirmation code to allow the user to specify a unique username. Non-DOI users may only access the PSTS and the Enjoy the View, Research Permit Reporting System, Data Store and the Researcher Check-in subsystems.

If anonymous access is enabled for a subsystem, users can access data that has been approved for sharing with the general public and excludes PII without the need for a user account or signing in. No PII is captured on anonymous users.

C. What is the legal authority?

- 54 U.S. Code § 100101. Promotion and regulation
- 54 U.S. Code § 100701. Protection, interpretation, and research in System
- 54 U.S. Code § 100704. Inventory and monitoring program
- 54 U.S. Code § 100705. Availability of System units for scientific study
- 54 U.S. Code § 100707. Confidentiality of information
- 54 U.S. Code § 100751. Regulations

- 36 CFR 1.6 Permits
- 36 CFR 2.1 Preservation of Natural, Cultural and Archeological Resources
- 36 CFR 2.5 Research Specimens

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection
☒ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*
UII Code: 010-000000570
SSP Name: Integration of Resource Management Applications (IRMA)

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
Acoustical Bat Monitoring (NABat)	NABat collects information on the detection of bat species occurrences throughout the NPS.	Yes	Stores the device location and first name, last name, position, address, title and group affiliation of individuals, including members of the public, who deployed and recovered monitoring devices in the field. Stores UPN, first name, last name, email, business phone of DOI users of the system.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
Cooperative Ecosystem Studies Unit Project Tracking (CESUPT)	CESUPT tracks and reports on projects associated with the Cooperative Ecosystem Studies Units (CESU) Network.	Yes	Stores name, address, phone, email, title and group affiliation and/or employment of individuals associated with CESU projects which may include DOI users and/or members of the public. Stores UPN, first name, last name, email, business phone of DOI users.
Data Store	The Data Store subsystem provides the tools to add, organize, discover, and retrieve metadata and finalized documents, datasets and scientific products about natural and cultural resources in the parks. https://irma.nps.gov/DataStore/	Yes	Stores first name, last name and group affiliation of authors, including members of the public, of finalized documents, datasets and scientific products. Stores account name, first name, last name, email of non-DOI users. Stores UPN, first name, last name, email of DOI users.
Enjoy the View (ETV)	Enjoy the View (ETV) tracks visual resource inventory data to establish a baseline assessment of scenic quality for park planning, internal, and external decisions that affect scenic resources. https://irma.nps.gov/ETV/	Yes	Stores first name, last name and affiliation of the individual, including members of the public who conducted the scenic inventory. Stores UPN of DOI users and account name of non-DOI users for authentication.
Environmental Review Tracking (ERTS)	ERTS is used to manage and track internal NPS reviews and responses of Environmental Impact Statements (EIS), Policy Proposals, and project proposals prepared by other agencies.	Yes	Project information that includes first name, last name, address, phone number, and email of applicants, reviewers and other associates points of contact, including members of the public. Stores UPN of DOI users.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
National Invasive Species Information Management System (NISIMS)	NISIMS collects information on the treatment of invasive species on NPS lands for reporting on types of treatment and acres treated.	Yes	Stores first name, last name and affiliation of individual conducting invasive species treatments and locations on NPS lands where treatments occurred. This information may be collected on members of the public. Stores UPN, FirstName, Last Name and e-mail of DOI users.
National Natural Landmark Tracking (NNL Tracking)	The NNL Tracking subsystem stores information on lands designated as Natural National Landmarks.	Yes	Stores landowners' names, addresses, phone number, email, and group affiliation of individuals associated with Natural Landmarks, including members of the public. Stores UserID of DOI users.
NPS Adaptation Project Tracking (NP Adapt)	The NP Adapt subsystem collects information on the management of resources impacted by the effects of climate change by documenting climate drivers, stressors, and mitigation efforts.	Yes	Stores first name, last name, group affiliations, and email addresses of individuals associated with an impacted resource, including members of the public. Stores First Name, Last name and UserID of DOI users of the subsystem.
NPS Species (NPSpecies)	NPSpecies documents the presence and status of species in National Parks for use in park resource management and responsible visitor use. https://irma.nps.gov/NPSpecies/	Yes	Stores email of individuals, including members of the public, who have suggested a change to park species profile attribution. Stores UPN, first name, last name, business email, business phone, business email alternate, business phone alternate of the DOI users and non-DOI Users of the subsystem.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
NRSS Air Project Tracking (APT) System	The Air Project Tracking (APT) subsystem stores information relevant to air quality projects in the areas of air permits, NEPA, regulatory review, and park planning to facilitate the review, analysis, and response for each phase of a project.	Yes	Stores first name, last name, Address, Phone, group affiliations, and email addresses of individuals associated with a project, including members of the public. Stores UPN, first name, last name, email, business phone of DOI users of the subsystem.
Observations and Vouchers (Evidence)	Species Evidence stores information on recorded sightings or the collection of a physical species specimen for the purpose of documenting the presence (current or historical) of a species in a Park.	Yes	Stores first name, last name and affiliations of individuals, including members of the public, who have recorded a sighting, done specimen collection, or identification of an evidence record. Stores UPN, first name, last name, email, business phone of DOI users.
Partner Security Token Service (PartnerSTS)	PartnerSTS is a claims-based identity system using a Multi Factor Authentication approach for Non-Federal users to establish a user account for the purpose of interacting with IRMA based systems. https://irma.nps.gov/PartnerSTS/	Yes	Stores first name, last name, email addresses, encrypted passwords and encrypted security question answers for application user identification. This information is collected on members of the public.
Pesticide use Proposal (PUPS)	PUPS stores information on proposed pesticide treatments and tracks the approval and use, of pesticides on NPS lands.	Yes	Stores first name, last name, e-mail and phone of park resource contacts (employees and contractors). Stores UPN, first name, last name, business email, business phone, business email alternate, business phone alternate of DOI users of the subsystem.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
Research Permit and Reporting System (RPRS)	RPRS supports the process of issuing, and management of Scientific Permits within the National Park system. https://irma.nps.gov/RPRS/	Yes	Stores name, office mailing address, office phone, alternate phone, office fax, and office email of applicants, including members of the public, for NPS Scientific Research and Collecting Permit. Stores name, business phone number, and business email addresses of park contacts for scientific research (employees, contractors and volunteers). Stores name and email of persons identified as co-investigators, including members of the public, by persons submitting applications for NPS Scientific Research and Collecting Permit. Stores the mailing address of the Repository in which NPS collections are managed. Also stores the name, office phone, office fax, and office business email of the primary contact at repositories which manage NPS collections (employees, contractors and volunteers). Stores account name, first name, last name, email of non-DOI users. Stores UPN, first name, last name, email of DOI users.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
Researcher Check In (RCI)	RCI provides a means for scientific research permit holders to check in and report to a park that they are on premise and doing scientific collection. https://irma.nps.gov/RCI/	Yes	Stores field contact name, phone, vehicle description including license plate, residence during field visit of individuals participating in research project on NPS lands, including members of the public. Stores account name of non-DOI users, including members of the public. Stores UPN of DOI users of the subsystem.
SEUG-ArcDoc	SEUG-ArcDoc stores inventory, monitoring, and treatment actions to archeological sites throughout southeast Utah group of parks.	Yes	Stores first name, last name and phone for site contacts, including members of the public. Stores UserID of DOI users of the subsystem.
Threatened and Endangered Species Reporting (TE-Reporting)	TE-Reporting stores annual costs incurred for management of threatened and endangered species by Park and Region for reporting to the Fish and Wildlife Service (FWS).	Yes	Stores first name, last name and phone number of an individual, including members of the public, that confirmed species population records at a park. Stores UPN, first name, last name, business email for DOI users of the subsystem.
Wildlife Mortality and Morbidity Observations (WHMMO)	WHMMO stores wildlife morbidity and mortality observations on NPS lands, and tracks samples and diagnostic results of testing for wildlife and public health consultation.	Yes	Stores first name, last name and affiliations of individuals, including members of the public, who have recorded a wildlife observation or specimen collection. Stores UPN, first name, last name, business email, business phone of DOI users of the subsystem.
Abandoned Mineral Lands (AML)	The Abandoned Mineral Lands supports the management and tracking of mitigation and reclamation projects for abandoned mineral sites on NPS lands.	Yes	Stores UPN, first name, last name, email, business phone of DOI users.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
Network Project Request (NPR)	The NPR subsystem supports requests for technical projects from I&M Network staff. The NPR component is a single data system, which is served through a single internet website, available to DOI internal users only.	Yes	Stores UPN, first name, last name, email, and business phone number of the DOI users.
PartnerSTS Admin	PartnerSTS Administration is the administrative interface to the PartnerSTS subsystem used to manage user accounts, authorization and expirations.	Yes	Stores UPN and business email of DOI users of the subsystem.
Protocol Tracking	Stores information on the implementation status of programs conducting inventory and monitoring of natural resources on NPS lands.	Yes	Stores UPN, first name, last name, business email, business phone of DOI users of the subsystem.
Park Visitor Use Statistics (STATS)	The STATS component provides statistics for visitation in national parks.	Yes	Stores UPN, first name, last name, business email, business phone of DOI users of the subsystem.
Report Portal	Allows for General distribution of reports that may not be available through an IRMA application. https://irma.nps.gov/ReportPortal/	No	N/A
Solution for Internal Document Review (SIDR)	SIDR coordinates NRSS internal review of NPS planning, policy, and project review documents that are in early stages of development.	Yes	Stores UPN, first name, last name, business email, business phone of DOI users of the subsystem.
Solution for Technical Assistance Requests (STAR)	STAR stores Park and region requests for technical assistance from (Natural Resource Stewardship and Science (NRSS) Divisions.	Yes	Stores UPN, first name, last name, business email, business phone of the DOI users of the subsystem.
State of the Parks Resource Condition Application & Database (RCAD)	RCAD supports data collection, analysis, and documentation for the State of the Parks (SotP) reporting program.	Yes	Stores users userID, first and last name of the DOI users of the subsystem.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
Taxonomy (Species Taxonomy)	The Taxonomy subsystem is used for storing biological taxonomy lookup information.	Yes	Stores UPN of subsystem DOI users.
Unit (NPS Units)	Stores park, region, program, and office codes, their names, and their relationships to other NPS Organizations.	No	N/A
YELL-Milestones	Stores information on the environmental and cultural compliance process for research and non-research projects in Yellowstone National Park (YELL).	Yes	Stores UPN, first name, last name, business email, business phone of DOI users of the subsystem.

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

NPS –26, Integrated Resource Management Applications (IRMA), (New SORN)
DOI-05, Interior Volunteer Services File System, (May 23, 2001, 66 FR 28536)
DOI-89, Grants and Cooperative Agreements: FBMS (July 28, 2008, 73 FR 43775)
NPS-25 - Research Permit and Reporting System (RPRS), (New SORN)
DOI Active Directory credentials are covered under:
DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), (March 12, 2007, 72 FR 11040)

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☒ Yes: *Describe*
For the RPRS subsystem only, OMB Control No. 1024-0236; Forms 10-741A, 10-741B, and 10-226; Research Permit and Reporting System Applications and Reports, 09/30/2023.

☐ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Personal Cell Telephone Number
☒ Personal Email Address
☒ Group Affiliation
☒ Employment Information
☒ Mailing/Home Address
☒ Other: *Specify the PII collected.*

IRMA does not maintain or display personally identifiable information (PII) beyond the limited data described in this privacy impact assessment. PII stored is primarily for the creation and management of user accounts and to allow registered users to interact with NPS. Limited incidental PII may be maintained to track metadata on specific items to properly cite the creator or origin of some content.

Location information may be included with the first name and last name as incidental information regarding the geographic location of a specific action taken, such as the location of a study, invasive species treatment or sampling collection.

This system contains records concerning corporations and other business entities, which are not subject to the Privacy Act. However, records pertaining to individuals acting on behalf of corporations and other business entities may reflect personal information.

DOI users use their government issued Personal Identity Verification (PIV) card authenticated through the Enterprise Active Directory (AD). The system collects the subsystem user's name, official email address, username, date of last login, and role or access level for authorized users.

Non-DOI users may voluntarily self-register a user account via the PartnerSTS subsystem. The PII required to create a user account includes the individual's name, email address, username, password and answers to security questions.

Employment information is limited to collection of employer name, group affiliation, title, business email address, phone number, and project information for individuals working under contract or agreements with NPS or another Federal agency.

NPS Scientific Research and Collecting permit holders submit the contact information of a primary contact when conducting research activities in the field. The contact information consists of the personal cell telephone number and vehicle information (including license plate), and residence (such as hotel) during park visit. The contact information is needed to protect the

safety of the persons conducting the research activities, inform law enforcement of when and where activities which would be illegal without a permit are taking place, and enable the park to monitor the impact of the activities on park resources.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☒ DOI records
☐ Third party source
☐ State agency
☒ Other: *Describe*

PII may be collected from electronic documents or records submitted to NPS or in the public domain as metadata regarding authors and publishers of reports and documents or as reports of a specific action(s) taken such as an invasive species treatment or sampling collection.

C. How will the information be collected? Indicate all that apply.

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

DOI users may research, analyze and record PII from electronic documents or records submitted to NPS or in the public domain for information on authors of finalized documents, datasets and scientific products.

The Office of Management and Budget Paperwork Reduction Act approved forms, application for an NPS Scientific Research and Collecting Permit and Investigator's Annual Report are served, and data is collected through the web-based Research Permit and Reporting System.

PII collected for creation and management of accounts for non-DOI users is collected directly from the individual during self-registration through the PSTS website.

For DOI users, information is collected from the individual during onboarding or generated as DOI records (e.g. email address, UPN, username) during operational activities. To establish an account, for a DOI user, an authorized NPS manager, for the DOI user, emails (encrypted) a IRMA subsystem account request to the IRMA subsystem administrator. The IRMA subsystem administrator grants permissions to that user's account. Upon the user's account accessing the subsystem, IRMA services communicate with Active Directory to authenticate, and collect PII stored in Active Directory about the DOI user.

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

PII collected on authors of finalized documents, datasets and scientific products is used to support natural resources research and reporting and to ensure proper citation of the authors. PII collected from individuals reporting natural resources action(s) taken, such as an invasive species treatment or sampling collection, is used for research support and analysis and may be used to support analysis of information to assess accuracy or determine need for further study. These individuals are working under contracts or agreements for work authorized by NPS or another DOI Bureau or Office.

RPRS collects the minimum contact information required to process applications. Applicants for a Scientific Research and Collecting Permit provide name, business phone, office email, mailing address, and institution represented. Alternate business phone and Office Fax are optional. RPRS collects park contact information, consisting of name, business phone and business email, in order to facilitate communication between parks and persons applying for Scientific Research and Collecting Permits, and for persons conducting permitted scientific research activities in the parks. RPRS stores name and email of persons identified as co-investigators by persons submitting applications for NPS Scientific Research and Collecting Permit. This information informs the parks who will be participating in permitted scientific research studies and who may be in the field conducting scientific research activities. RPRS stores the mailing address of the Repository in which NPS collections are managed. RPRS also stores the name, office phone, office fax, and office business email of the primary contact at repositories which manage NPS collections; this information facilitates fulfillment of the permit agreement that NPS collections are managed to NPS requirements. RPRS stores UPN, first name, last name, email of DOI users to securely authenticate individuals to the system, manage user roles and permissions, and enable change and audit logging. RPRS stores account name, first name, last name, email of non-DOI users to securely authenticate individuals to the system, manage user roles and permissions, and enable change and audit logging. Data elements were examined to minimize the impact on an individual's privacy and to limit the information to business contact data (i.e. business phone number). Information solicited is only what is required to administer scientific research in units of the National Park Service.

PII collected from the public during account creation and management is used to authenticate individuals and to enable the individuals to participate in natural resource conservation and research activities. Information collected is limited to first name, last name, email address, a self-assigned username, and answers to security questions. A multi-factor authentication model

is used that relies on the user having an external e-mail account where an encrypted e-mail is sent for account activation, account reset and change alerts.

PII collected from Government Users will be used by IRMA to securely authenticate individuals to the system, manage user roles and permissions, and enable change and audit logging.

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

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

Data developed by NRSS Programs and Divisions are used to help inform natural resources decisions throughout the NPS. PII associated with research documents and data sets will be shared with Natural Resources Offices and Programs through the NPS as necessary to assist in resource management responsibilities. Some data may also be shared with the Cultural Resources Office and Programs where cultural resources may be associated with or impacted by natural resources activities. Information is shared with law enforcement to protect the safety of the persons conducting the research activities, and to inform law enforcement of when and where activities which would be illegal without a permit are taking place.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

PII associated with research documents and data sets will be shared with other Natural Resources programs and offices across DOI. IRMA will be used across DOI Bureaus and Offices to catalog research and data collection on natural resources activities, such as sample collection or invasive species treatments, and will provide data for study and support of natural resources conservation and scientific research. Data sharing will be restricted between and within the DOI Bureaus based on the user's role, permission and organizational assignment.

Account creation and management data of DOI Users will be shared with DOI and its Bureaus and Offices through Active Directory.

Account creation and management data of public users of the PSTS is only accessible to NPS system administrators and security personnel and would only be shared with DOI in the event of a security incident.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

System users may be from other Federal agencies and will have access to shared information available through IRMA.

The CESU Project Tracking subsystem tracks and reports on projects associated with the CESU Network. The Cooperative Ecosystem Studies Units (CESU) Network is a national consortium of federal agencies, tribes, academic institutions, state and local governments,

nongovernmental conservation organizations, and other partners working together to support informed public trust resource stewardship. The CESU Network includes 354 partners, including Federal agencies, in seventeen CESUs representing biogeographic regions encompassing all 50 states and U.S. territories as a platform to support research, technical assistance, education and capacity building that is responsive to long-standing and contemporary science and resource management priorities. Participating Federal agencies include Department of Agriculture, Department of Interior, U.S. Army Corp of Engineers-Civil Works, Department of Defense, Defense Prisoners of War/Missing in Action Accounting Agency, National Oceanic and Atmospheric Administration, and the National Aeronautics and Space Administration.

The CESU Network is coordinated and provided support by the CESU Council. The Council includes representatives of participating Federal agencies operating under a Memorandum of Understanding (MOU) for the CESU Network. CESU Council and Federal agency representatives and participants may be system users with access to CESUPT information.

The IRMA system does not have electronic data interfaces or interconnection agreements with any other Federal agency.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

System users may be from Tribal, State or Local Agencies and will have access to shared information available through IRMA. Tribal, State or Local Agencies may be representatives or participants in the CESU network or cooperative agreements awarded to CESU network participants. Tribal, State or Local Agencies representatives and participants may be system users with access to CESUPT information.

The system does not have electronic data interfaces or interconnection agreements with any Tribal, State or Local Agencies.

☒ Contractor: *Describe the contractor and how the data will be used.*

NPS may contract with other commercial organizations to provide application development, configuration and operations, and maintenance of IRMA or specific subsystems. Contractor staff will be required to undergo background checks as defined by NPS policy and procedures. Contractor staff access will be restricted to data on a need to know basis. Privileged accounts will be audited, and authentication and other security and privacy controls will be enforced as defined in the System Security Plan and Privacy Plan. This maintenance is critical to protecting the system and the PII contained within the system. IRMA undergoes a security assessment by a third-party assessment organization each year.

CESUs include nongovernmental and nonprofit conservation organizations, and other nonfederal entities to significantly expand the capabilities and skills of a CESU. Field-based scientists (such as those located in a national park or forest) may be affiliated with the CESU through a

university or a partner institution. CESUs provide skills, research and services pursuant to their cooperative agreement with a Federal agency or the CESU Council. Federal agencies retain administrative oversight of the CESU networks and cooperative agreements awarded to CESU network participants. CESU network participants may be system users with access to CESUPT information.

☒ Other Third-Party Sources: *Describe the third party source and how the data will be used.*

A condition of holding a Scientific Research and Collecting Permit requires that an annual report be submitted concerning the progress of the research project. This report is part of the public record of scientific research within units of the National Park Service (exceptions may be made for reports which contain sensitive information which may negatively impact park resources). Investigator's Annual Reports (IAR) which have been checked in by Parks as non-sensitive are provided to the public by the Research Permit Reporting Subsystem. The report includes permit holder's work contact information: name, office phone, office email, mailing address, and institution represented. If the permit holder has provided their Office Fax, that information will also be available on the report. The annual report may also include the names, business phone number and email of co-investigators. The Application Procedures and Requirements for NPS Scientific Research and Collection Permits guidance document (accessible from the RPRS help link) provides notice to applicants regarding sharing of the IAR with the public.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Non-DOI individuals voluntarily provide information when creating a profile or contact in the Partner Security Token Service subsystem and when submitting applications, agreements, reports and correspondence. Users will be provided a Privacy Act Statement at the time of registration and will be offered the opportunity to accept or decline to provide information; however, declining to provide information may impact the ability of NPS to communicate with an individual and may impact an individual's ability to effectively participate or receive communication relative to areas of research or scientific inquiry.

Non-DOI users voluntarily provide information when creating a user account in the Research Permit and Reporting System for the purpose of submitting applications for NPS Scientific Research and Collecting Permits and submitting reports on permitted scientific research activities. Users are provided a Privacy Act Statement at the time of registration and are offered the opportunity to accept or decline to provide information. However, no permit transaction can take place without the provision of contact information because the NPS Scientific Research and Collecting Permit is an agreement between an individual and the National Park Service.

For DOI users, information is collected from the individual during onboarding or generated as DOI records (e.g. email address, UPN, username) during operational activities. To establish an account for a DOI user, an authorized NPS manager emails (encrypted) a user account request to the IRMA system administrator. The IRMA system administrator creates the user account with the information provided, and the IRMA queries the Active Directory Federated Services to validate and complete the account creation.

Non-DOI users, that wish to elevate permissions higher than an anonymous user, voluntarily provide information (username, email, first name, lastname) to create a user account within the Partner Security Token Service subsystem. If the non-DOI user declines to provide the requisite information a user account is not created.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement: *Describe each applicable format.*

For all IRMA applications the NPS Privacy Policy is included on every web page as a link in the footer and directs the user to: https://www.nps.gov/aboutus/privacy.htm. A Privacy Act Statement is provided on the PartnerSTS registration page and on the web forms used by the RPRS subsystem (Forms 10-741A, 10-741B, and 10-226). The RPRS opening page, https://irma.nps.gov/RPRS/Investigator/Create, is the opening page of the investigator account creation. The account creator provides contact information that will leveraged in permit transactions (i.e. pre-fill application contact information). The Privacy Act Statement is posted on the landing page for the RPRS application (Form 10-741A Application for Scientific Research and Collecting Permit) and the Investigator's Annual Report (Form 10-226 Investigator's Annual Report). It is also posted on RPRS generated PDFs of these forms.

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through publication of this PIA and the applicable published SORNs.

☒ Other: *Describe each applicable format.*

Privacy Act Notice: Scientific research, education and collecting activities within units of the National Park System that may impact parks invoke a permitting and reporting requirement per regulations at 36 CFR 1.6 (Permits), 36 CFR 2.1 (Preservation of Natural, Cultural and Archeological Resources), and 36 CFR 2.5 (Research Specimens). The National Park Service collects information about permit applicants and permittees to administer and document research,

collecting, and reporting activities within parks. The information disclosed on this form is required and may result in denial of permit applications if not provided. A Privacy Act notice is provided on the RPRS application and Investigator's Annual Report landing pages.

Users are provided with a privacy and security warning banner when accessing the system.

☐ None

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

Datasets are retrieved from both pre-generated and dynamic search results. First name, last name, email and UPN identifiers are utilized to filter results directly (specific identifier retrieval) and indirectly (keyword).

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

In RPRS, reports are produced to obtain user statistics available to authorized internal users only.

Park staff generates reports about research investigators historical study activity as input to the decision process to determine annual permit issuance and renewals.

☐ No

Section 3. Attributes of System Data

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

For DOI users, information is collected from the individual during onboarding or generated by NPS or DOI as DOI records (e.g. email address, UPN, first name and last name) during operational activities.

For Non-DOI users, PII information is collected from the individual during their voluntary account creation process in the Partner Security Token Service (PartnerSTS) subsystem. Whenever a Non-DOI user uses the PartnerSTS to authenticate, and subsequently request elevated access to any other IRMA subsystem, it is up to the administrator of the IRMA subsystem to review and validate that the user's information is accurate and truly belongs to the requestor of permissions.

Information is collected directly from Non-DOI users when they voluntarily request a user account in the Research Permit and Reporting System, submit applications for NPS Scientific Research and Collecting Permits, and submit reports on permitted scientific research activities. Information is verified with the individual user who has the ability to update their account information. Users are responsible for ensuring the accuracy of the data they submit.

B. How will data be checked for completeness?

For members of the public, NPS relies on the completeness of the information provided by the individual. Validation rules in individual IRMA components prevent users from submitting information not conforming to data entity definitions. Users are responsible for ensuring the completeness of the data they submit when requesting an account or submitting an application.

DOI users are responsible for ensuring the completeness of the data associated with their user accounts and content posted in the system. PII used for account creation is initially provided by the individual during onboarding. During the account creation process, the user account administrator will validate the account request against DOI Active Directory information, and incomplete data will result in an error preventing creation of the account. Incorrect data may prevent user authentication or may be identified by supervisors when reviewing activity reports. Users may contact the help desk for assistance to validate account information and follow published Role-Based Management System (RBMS) procedures to have the data updated.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

DOI User information (UPN, First Name, Last Name, UserID) is obtained from DOI's Active Directory, any changes made within Active Directory are reflected within the IRMA system.

Non-DOI User information is maintainable by the user using the PartnerSTS system. The user may make changes to (First Name, Last Name). Any changes made within PartnerSTS are reflected within the IRMA system. Users may update or correct their contact information or resubmit an application to ensure data remains current.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Records in IRMA subsystems are retained in accordance with the National Park Service Records Schedule, Resource Management and Lands (Item 1), which has been approved by the National Archives and Records Administration (NARA) (Job No. N1-79-0801). The disposition of Cultural and Natural Resource Management Program and Planning records, including applications for permits, permits and investigator annual reports, is permanent. Periodic transfer of special media and electronic records along with any finding aids or descriptive information (including linkage to the original file) and related documentation by calendar year are transmitted to the NARA when 3 years old. Final transfer of all permanent records to NARA

occurs 15 years after closure. Digital records will be transferred according to standards applicable at the time.

The disposition of records with short-term operational value and not considered essential for ongoing management of land, cultural and natural resources is temporary, including account management records, these operational records are destroyed/deleted 15 years after closure. The disposition for routine housekeeping and supporting documentation is temporary and records are destroyed/deleted 3 years after closure. Detailed disposition procedures and processes are defined and published to internal system administration staff within the IRMA technical reference manuals.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Workflows are in place to manage the disposition of permanent records in conformance with requisite retention schedules. Periodic transfer is accomplished through delivery of permanent special media and electronic records along with any finding aids or descriptive information (including linkage to the original file) and related documentation by calendar year to the NARA when 3 years old. Digital records, and their inherent machine-readable formats, will be transferred according to standards applicable at the time.

Final transfer of all permanent records to NARA 15 years after closure is facilitated through exchange of IRMA records to NPS's authoritative archive (eTIC). Transfer from eTIC, and ultimately to NARA, is facilitated by inherent retention logic in eTIC which regulates release of information. Only users with AD credentials or granted non-DOI accounts are able to contribute content to IRMA systems, and only NPS personnel with AD credential can access the eTIC archive so PII is protected throughout this process and the record's information lifecycle.

The approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and 384 Departmental Manual 1.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

IRMA is categorized as a moderate risk system; however, multiple controls have been implemented to mitigate and substantially lower privacy risks. All information acquisition and collection is done through electronic web forms over encrypted communication channels that comply with the required federal standards and stored within an encrypted database to minimize risk of data breaches while in transit and while stored. Information access and retrieval is done through electronic web forms over encrypted channels following defined application security roles and permissions to ensure proper distribution and disclosure of information guided by the

principle of least privilege to minimize the risk of improper information disclosure. The protection and maintenance of information for recovery and backup purposes is done following NPS data center policy and process for backup and retention of information.

There is an increased risk for retention of permanent records containing PII; however, no sensitive PII is retained in the permanent records managed in the IRMA system. Disposition of all information are guided by the NPS Records retention schedules for systems that manage information pertaining to natural resources and appropriate risk levels.

There are privacy risks related to hosting, processing and sharing of data, unauthorized access to records, or any inappropriate use and dissemination of information. These risks are mitigated through a combination of physical, administrative, and technical controls, many of which are referenced in the System Security and Privacy Plans. Risk is also mitigated through system configuration controls that limit or prevent access to privacy information.

There is a risk that unauthorized persons could potentially gain access to the PII on the system or misuse the data. To mitigate this risk, access to data is restricted to authorized personnel who require access to perform their official duties.

IRMA enables access for DOI authorized employees, contractors, and volunteers (collectively, DOI users) through the use of the Personal Identity Verification (PIV) Credentials and DOI Active Directory using User Principal Name (UPN) or UserID attributes for authentication and role/permission management. DOI users must complete a background check, are required to sign the DOI's Rules of Behavior, and must complete security and privacy training prior to accessing a DOI computer system or network.

Non-DOI users, including users from other federal agencies, local governments, tribal organizations, universities or the general public, may voluntarily self-register by creating a user account with the Partner Security Token Service (PSTS) for the intent of interacting with specific subsystems. The PSTS provides multifactor authentication using a valid e-mail account and a temporary encrypted account confirmation code to allow the user to specify a unique username. Account management data is encrypted at rest and in transit. Non-DOI users may only access the PSTS and the Enjoy the View, Research Permit Reporting System, Data Store and the Researcher Check-in subsystems.

If anonymous access is enabled for a subsystem, users can access data that has been approved for sharing with the general public and excludes PII without the need for a user account or signing in. No PII is captured on anonymous users.

Transport Layer Security (TLS) technology is employed to protect information in transit using both server authentication and data encryption. Platform and device level encryption have been deployed to encrypt data at rest. Other security mechanisms have also been deployed to ensure data security, including but not limited to, firewalls, virtual private network, and intrusion detection.

There is a risk that user PII may be inappropriately used or disseminated by personnel authorized to access the system or view records. The system uses audit logs to protect against unauthorized access, changes or use of data. Federal employees and contractors are required to take annual mandated security, privacy and records management as well as role-based training where applicable and sign the NPS Rules of Behavior prior to accessing the system. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, criminal, civil, and administrative penalties.

There is a risk that erroneous information may be collected. This risk is mitigated by allowing individuals to access and update only their records in the system. For DOI user accounts, this risk is further mitigated by validating information against DOI Active Directory, authentication results, and activity report and audit log content. No sensitive PII is collected or managed by the IRMA system.

There is a risk that information in the system will be maintained longer than necessary to achieve the agency's mission or may be improperly disposed or destroyed. This risk is mitigated by maintaining and disposing of records in accordance with a records retention schedule approved by NARA. Users are reminded through policy and training that they must follow the applicable retention schedules and requirements of the Federal Records Act. Detailed procedures and automated scripts for data disposal/destruction will be developed and secured under change management. Contingency plans and procedures will be defined to ensure the ability to recover in the event of improper data disposal.

There is a low risk of improper disclosure of PII during the records transfer process. This risk is mitigated by limiting access to the NPS eTIC archive to NPS personnel with AD credentials and the file transfer to eTIC is affected entirely within the NPS internal network and requisite encryption is applied to data at rest and in transit.

There is a risk that individuals providing information do not have adequate notice on how their PII will be collected or used. This risk is mitigated by the publication of this PIA, SORNs, and Privacy Act Statements within the application.

Section 4. PIA Risk Review

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

☒ Yes: *Explanation*

Information collected from the public is used to improve NPS resource management utilizing best-available information. IRMA and subsystems deliver comprehensive information about National Park Service (NPS) parks and programs to a global Internet audience and makes NPS resources, research, and information easily accessible to the public.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

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

☐ Yes: *Explanation*

☒ No

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

☐ Yes: *Explanation*

☒ No

E. How will the new data be verified for relevance and accuracy?

N/A. There is no new data being created.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors

☐ Developers
☒ System Administrator
☐ Other: *Describe*

All application users are provided access from either a web interface or desktop client that enforces a permission-based security model over encrypted connections using the HTTPS protocol. Permissions are administered and managed by an assigned subsystem administrator to ensure all access is authorized and proper training and usage completed for the subsystem. All IRMA subsystems follow the principle of least privilege, and expose information following only the allowed actions per user classification:

a. **Anonymous User -** A user who accesses publicly available applications or functions without identifying themselves. No PII is collected from anonymous users, and anonymous users cannot access any PII in the system.
b. **Public User** - A user from the general public who has self-registered their account in the system. These users can only access the PII information they provided in their user account.
c. **DOI Users:** An employee, contractor, or volunteer authorized for DOI network credentials and authorized for IRMA system access including:
   i. **General Users** - General users may view records which may include limited incidental PII associated with documents, deliverables or activities, such as sampling collection of invasive species treatments.
   ii. **Privileged Users** – Employees and contractors providing operational support have access to user accounts, system logs and databases through the use of the DOI.NPS privileged accounts only.

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Access will be restricted for all users. Each user will be assigned permissions, groups of permissions may be used to define a user's role. The permissions will determine what function the user may execute in the system and define what records the user can create, read, edit or delete. For example, a STATS data collector will have permissions to access only the Park usage statistics for the park units for which they are responsible.

System management staff may on occasion be required to view PII in the performance of their duties for troubleshooting or system maintenance purposes. Employee or contractor staff with privileged accounts will be subject to routine auditing to ensure compliance with policies and procedures for managing data confidentiality and integrity.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Contractors are responsible for designing, developing and maintaining the system, and in accordance with DOI policies, Privacy Act contract clauses are included in all contractor agreements in accordance with and subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations.

Contractor employees interfacing with the system and/or related data or providing services, administration or management are required to sign nondisclosure agreements as a contingent part of their employment. Contractor employees are also required to sign the DOI's Rules of Behavior and complete security and privacy training prior to accessing a DOI computer system or network. Information security and role-based security training must be completed on an annual basis as an employment requirement. Contractor and/or contractor personnel are prohibited from divulging or releasing data or information developed or obtained in performance of their services, until made public by the Government, except to authorized Government personnel. Contractors are also subject to Federal Acquisitions Regulations (FAR) with regard to sensitive data; however, no sensitive PII is collected or managed by the IRMA system.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*

☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

Monitoring will primarily target users with privileged accounts, such as system administrators who can change configuration settings or escalate access permissions or roles; however, login history is recorded for all users, and field history tracking is recorded for select data fields, including some PII data elements.

IRMA is not intended for monitoring users; however, the system does identify and monitor user activities within the system through audit logs. Audit logs automatically collect and store information about a user's visit, including UPN, identity verification method, action attempted and the status of the attempt, as well as create/update/delete activities performed by users to support user access controls, troubleshooting, and incident response support. Audit logs may also be used to identify unauthorized access or monitoring.

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

The irma.nps.gov uses three levels of logging, at the: application layer, web server, and system level.

The application layer logs the components of the application accessed, the application action taken and user id of the individual who performed the action.

The web server logs the date and time the system was accessed over the https protocol. Information collected includes time, source IP, the method used, url requested, port, username and type of agent used.

System logging records all attempted access to the system from users and internal processes, including monitoring, maintenance and audit processes. Items logged include unique identifiers, account names, timestamp, event information, source and successful/unsuccessful login attempts.

A system administrator may access platform configuration settings, and all platform configuration settings are monitored for changes. All system administrator accounts are monitored and routinely audited.

M. What controls will be used to prevent unauthorized monitoring?

All IRMA based applications are governed and managed by the IRMA Operations guide and associated internal Service Level Agreements (SLA). The SLA defines and establishes individual subsystem ownership, data and systems accountability and technical ownership for each subsystem. The SLA defines that for all irma.nps.gov applications, only system administrators have access to resources where log files are stored. When a system administrator accesses the system, they must acknowledge the DOI system usage statement.

In addition to accepting the warning, all system administrators are required to take annual Role Based Security Training (RBST), annual Role Based Privacy Training (RBPT), and annual FISMA Training.

Separation of duties, permission restrictions, and audit controls are implemented to prevent unauthorized monitoring. Procedures are published for granting accounts, and privileged accounts are routinely audited for compliance.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

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

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

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

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The irma.nps.gov Information System Owner is the official with ultimate responsibility for implementing adequate controls and protecting the privacy rights of individuals affected by the use of the system and interactions on the irma.nps.gov website.

The Information System Owner, the Privacy Act system manager and the Information System Security Officer are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with the Federal laws, regulations and policies for the data collected, used and managed, and for making decisions on privacy issues, in consultation with the NPS Associate Privacy Officer.

The NRSS Data & Systems Officer serves as the IRMA Information System Owner and the official responsible for oversight and management of the security and privacy controls and the protection of the information processed and stored in IRMA. The Information System Owner and Information System Security Officer are responsible for addressing privacy rights and complaints, and ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored within IRMA, in consultation with NPS and DOI Privacy Officials.

P. 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?

The IRMA Information System Owner and IRMA Information System Security Officer are responsible for daily operational oversight and management of the security and privacy controls, for ensuring to the greatest possible extent that data is properly managed and that all access to the data has been granted in a secure and auditable manner. The IRMA Information System Owner and Information System Security Officer are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC and appropriate NPS and DOI officials in accordance with DOI policy and established procedures, and appropriate remedial activities are taken to mitigate any impact to individuals in coordination with the NPS Associate Privacy Officer.

System administrators and contractors are required to report any potential loss or compromise to the Information System Owner and Information System Security Officer.