**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 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:** Cultural Resource Application Systems (CRPS)
**Bureau/Office:** National Park Service, Cultural Resources, Partnerships, and Science Directorate
**Date:** January 11, 2022
**Bureau/Office Contact Title:** NPS Associate Privacy Officer
**Point of Contact**
Name: Felix Uribe
Title: NPS Associate Privacy Officer
Email: nps_privacy@nps.gov
Phone: 202-354-6925
Address: 12201 Sunrise Valley Drive, 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

**B. What is the purpose of the system?**

The National Park Service (NPS) Cultural Resources, Partnerships, and Science (CRPS) Directorate consists of various programs under an Associate Director, including the Technical Preservation Services (TPS) office, National Register of Historic Places and National Historic Landmarks programs (NR/NHL), Park Archeology program, Cultural Landscapes, Historic and

Prehistoric Structures, and State, Tribal, and Local governments program, Tribal relations and American Cultures and 10 other programs.

CRPS system is a web-based application and database system that provides NPS CRPS program managers the information needed to make informed cultural resources management decisions. CRPS is used to track the receipt and processing of applications for NPS certification for Federal income tax incentives for historic preservation, track and process grant applications and results, and to comply with legal and regulatory requirements for cataloging and reporting on cultural resources and historic properties. Additionally, the system makes NPS CRPS program data and research available to the State and Local Government, Tribal Historical Preservation Office (THPO), State Historical Preservation Office (SHPO), Congress, non-profit organizations, and public users. CRPS system can be accessed through NPS public and internal network portals via web browsers.

CRPS system is a moderate-risk system that leverages many of its privacy and security controls through the general services system controls with some custom application-specific controls hosted on Windows Server infrastructure. CRPS sub-systems are managed following a common governance model, infrastructure, and management procedures. User management tools are available to program managers and system administrators to manage user accounts, maintain security and access controls, and specify terms of use for data records.

CRPS system can be accessed by NPS authorized employees, contractors, and volunteers (collectively, NPS users) using the Personal Identity Verification (PIV) Credentials and DOI Active Directory for authentication and role/permission management. All NPS 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-NPS users, including users from other federal agencies, state governments, local governments, tribal organizations, universities, or the general public, first need to obtain approval from program managers and register to have a user account created. System user management tools provide multifactor authentication using a valid e-mail account and a temporary encrypted account confirmation code.

## C. What is the legal authority?

- Archaeological Resources Protection Act (Title 16 U.S.C. 470aa-470mm)
- Archeological and Historic Preservation Act (Title 16 U.S.C. 469-469c-2)
- Protection of Archaeological Resources (43 CFR Part 7)
- Protection of Historic Properties (36 CFR Part 800)
- National Historic Preservation Act (NHPA), 54 U.S.C. 300.101 et. sq.
- National Park Service and Related Programs, 54 U.S.C.
    - Section 106 of the National Historic Preservation Act (Title 54 U.S.C. 306108)
    - Section 304 of the National Historic Preservation Act (Title 54 U.S.C. 306101-306114)

  - Section 110 of the National Historic Preservation Act (Title 54 U.S.C. 307103)
- National Historic Landmarks Program (Title 54 U.S.C. 302102-302108)
- Archaeological Resources Protection Act (Title 16 U.S.C. 470aa-470mm)
- Code of Federal Regulations (CFR): 36 CFR 60; 36 CFR 63; 36 CFR 65; 36 CFR 800
- National Park Service Centennial Act (Public Law 114-289; signed 12/16/2016)
- Administrative Procedures Act (Title 5 U.S.C.701-706) Appendix Q-NPS management plan
- Internal Revenue Code (IRC), 26 U.S.C.
  - Rehabilitation Credit (26 U.S.C. Part 47)
  - Charitable, etc., Contributions and Gifts (26 U.S.C. Part 170)
  - Identifying Numbers (26 U.S.C. Part 6109)
- Department of the Interior regulations (36 CFR Part 67)
- African American Civil Rights Network Act of 2017 (Public Law 115-104)

**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:

**E. Is this information system registered in CSAM?**

☒ Yes:

The Cultural Resources, Partnership, and Science System Security and Privacy Plan is in development.

UII: 010-000001765, 010-000000494, 010-000000495, 010-000000498, 010-000000499

☐ 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** |
|---|---|---|---|

| | | | |
|---|---|---|---|
| National Register & Landmarks Application (NRIS-NHL) | The purpose of the NRIS-NHL is to assist the NPS in managing and reporting on National Register resources in an effective and timely manner. The NRIS is currently an internal database system accessible only to NPS staff. | Yes | NRIS-NHL stores information on the significance of the site including associated persons, events, and/or cultural significance, address, site ownership, and point of contact information, identification of persons or organizations associated to the site, e.g., architect, builder.<br><br>Stores UPN, first name, last name, email of NPS users. |
| Historic Preservation Tax Incentives System (TaxAct) | The system tracks the processing of applications for Federal income tax incentives for historic preservation. The Internal Revenue Code (Sections 47 and 170) requires the Secretary of the Interior to provide certain "certifications" to the Secretary of the Treasury for the rehabilitation of historic buildings. Owners of historic buildings apply to the NPS for the required certifications using NPS application forms. | Yes | TaxAct stores building name and address, owner name, home mailing address, personal email, home phone number, and Social Security number or tax id, and associated tax benefit; name, email, and phone number of State, Tribal, or local historic preservation office contact.<br><br>Stores reference identifier for NRIS-NHL.<br><br>Stores NPS Reviewer comments, appeal number, project number, dates, and actions such as lack of payment, denials, late or second notices.<br><br>Stores UPN, first name, last name, email of NPS users. |
| Cultural Resources Inventory Systems (CRIS) | CRIS manages NPS's official inventory of cultural resource sites in parks. The system stores basic management, registration, and condition data about park | Yes | CRIS collects information on groups associated with the sites, e.g., architects, Tribal groups, non-profits, |

| | | | |
|---|---|---|---|
| | cultural resources to comply with federal laws (including the National Historic Preservation Act (NHPA) and the Archeological Resources Protection Act (ARPA) and to serve the NPS preservation mission. | | and may include first and last name, email, and work phone numbers of points of contact.<br><br>Stores UPN, first name, last name, userid, password, work phone, role, park, access to sensitive data (CUI), and email of NPS users and non-badged volunteers, interns, and contractors. |
| Historic Preservation Fund Application (HPF) | HPF provides the 59 State Historic Preservation Offices the ability to report digitally on their programmatic and financial activities using their annual appropriations from the Historic Preservation Fund. | Yes | HPF stores name and contact information for property point of contact and other persons associated to the site, including subgrantee, contractor, NEPA consulting parties, and easement holders.<br><br>Stores reference identifier for NRIS-NHL and IRMA.<br><br>Stores email, work phone number, name of State, Tribal, and local historic preservation office personnel system users and their association to system activity on the property.<br><br>Stores name, userid, password, email, work phone number of non-NPS users for authentication.<br><br>Stores UPN, first name, last name, email of NPS users. |
| Save America's Treasures Grants and Preserve | Save America's Treasures Grants and Preserve American Grants Application are two grant tracking system used to | Yes | SAT/PA collects information on grant applicants, tax ID, DUNS |

| | | | |
|---|---|---|---|
| American Grants Application (SAT/PA) | track grant milestones, fiscal and report information in grant life cycle. | | No., agency/employer points of contact and authorized representatives, including first, middle and last name, personal email, and work phone numbers. Stores grant ID and documents downloaded from Grants.gov.<br><br>Stores reference identifier for NRIS-NHL.<br><br>Stores UPN, first name, last name, email of NPS users. |
| Native American Graves Protection and Repatriation Act (NAGPRA) Application | National NAGPRA database application has provided the National NAGPRA Program the ability to track and process data related to 11 areas of program work. | Yes | NAGPRA collects applicant and/or institution information, employer ID no., name, company, title, phone, email, patrimony, case no., Tribe and Tribe contacts and activities. Stores grant ID and documents downloaded from Grants.<br><br>Stores dates, descriptions, and activity on penalties, violations, allegations, and name and email of associated NPS Reviewer. Stores UPN, first name, last name, email of NPS users. |
| Maritime Grant Application (MGA) | MGA system that allows grant application reviewers to score and comment on applications online. | Yes | Account management and audit logging information for users. MGA collects first and last name, personal email, and work phone numbers. |
| Historic Black Colleges and Universities System | Historic Black Colleges and Universities System Application is an electronic application system to handle submission, collection, reviewing process and then move to tracking process where | Yes | Account management and audit logging information for users. HBCU collects first and last name, |

| | | | |
|---|---|---|---|
| Application (HBCU) | information is maintained on each application to track its progress, create reports, and provide audit documentation. | | personal email, and work phone numbers. |
| Underrepresented CR State, Tribal and Local Plans and Grants System Application: Communities System Application (URC) | URC system is an electronic application system to handle submission, collection, reviewing process and then move to tracking process where information is maintained on each application to track its progress, create reports, and provide audit documentation. | Yes | Account management and audit logging information for users. URC collects first and last name, personal email, and work phone numbers. |
| Certified Local Government (CLG) Application | CLG is a Web based application to allow grant staff to track each state's CLG certification and decertified information. Application provides tools to let each state coordinator enter their own state CLG Accomplishment report. | Yes | Stores name and contact information for local government entities. Account management and audit logging information for users. CLG collects first and last name and work email, phone numbers, address, title. |
| National Archaeological Listing of Outlaw Treachery and Permit Database (LOOT) | LOOT is a web application for Archeological staff to enter new records and update and review LOOT permit information online. | Yes | Account management and audit logging information for users. LOOT collects first and last name and work phone numbers. |
| African American Civil Rights Network Application (AACRN) | The purpose of the African American Civil Rights Network Application (AACRN) is to assist the NPS in managing and reporting on the process for adding and maintaining properties, facilities, and programs to the African American Civil Rights Network, which was created with the passage of the African American Civil Rights Network Act of 2017 (Public Law 115-04) to recognize "the importance of the African American Civil Rights movement and the sacrifices made by the people who fought against discrimination and segregation." | Yes | Stores name on the listing for NRIS-NHL if a property is listed in the National Register of Historic Places.<br><br>Stores name and contact information for property point of contact and other persons associated to the Resource, including owner/manager.<br><br>Stores email, work phone number, name of State, |

| | | | |
|---|---|---|---|
| | | | Tribal, and local historic preservation office personnel system users and their association to system activity on the property.<br><br>Stores name, userid, password, email, work phone number of non-NPS users for authentication.<br><br>Stores UPN, first name, last name, email of NPS users. |
| Comprehensive American Battlefield information Network (CABIN) | The purpose of the CABIN system is to support NPS in managing and maintaining the identification, research, evaluation, interpretation, and protection of historic battlefields and associated sites on a national, State, and local level.<br><br>CABIN is a web-based electronic application system to assist NPS to manage projects received grants under the "preservation assistance" provisions of 54 U.S.C. § 308102, where information is maintained on each awarded project to monitor its progress, create reports, and provide audit documentation. | Yes | Stores name and contact information for grantee point of contact and other persons associated to the project, including owner/manager.<br><br>Stores email, work phone number, name of State, Tribal, and local historic preservation office personnel, public and private institutions of higher education, tax id, DUNS no., non-profits contacts and their association to system activity on the property.<br><br>Stores UPN, first name, last name, email of NPS users. |

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

☒ Yes:

Grants records are covered under DOI-89, Grants and Cooperative Agreements (July 28, 2008, 3 FR 43775); modification published 86 FR 50156 (September 7, 2021)

A new NPS-35, Cultural Resources, Partnerships and Science, SORN is being developed to cover the Historic Preservation Tax Incentives System (TaxAct) and the NRIS-NHL. A new NPS-32, Permits for Archeological Investigations, SORN is being developed to cover permits related to archeological investigations.

☐ No

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

☒ Yes:

OMB 1024-0018, Nomination of Properties for Listing in the National Register of Historic Places, 36 CFR 60 and 63, Expiration Date: 3/31/2022
OMB 4040-0004, SF-424 Discretionary Grant form usage for NPS, Expiration Date::12/31/2022

☐ No

## Section 2. Summary of System Data

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

☒ Name
☒ Social Security Number (SSN)
☒ Personal Cell Telephone Number
☒ Tribal or Other ID Number
☒ Personal Email Address
☒ Group Affiliation
☒ Home Telephone Number
☒ Employment Information
☒ Mailing/Home Address
☒ Other:
CRPS 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. Employment information is limited to collection of employer name, group affiliation, title, business email address, phone number, and project information for individuals associated with grants or projects on National Register or other historic preservation properties or under contracts or agreements with NPS or another Federal agency.

NRIS-NHL stores information on the significance of the historic site including associated persons, events, and/or cultural significance, address, site ownership, point of contact information, name and point of contact information of persons or organizations associated to the site, e.g., architect, builder. An NRIS-NHL identification number is generated by the subsystem and used to link records in other subsystems to the NRIS-NHL property.

TaxAct stores building name and address, owner name, home mailing address, personal email, phone number, and social security number or tax id, and associated tax benefit; name, email, and phone number of State, Tribal, or local historic preservation office contact. TaxAct also records NPS Reviewer comments, appeal number, project numbers, and dates and actions such as lack of payment, denials, late or second notices.

CRIS collects information on groups associated with the sites, e.g. architects, Tribal groups, non-profits, and may include first and last name, email, and work phone numbers of points of contact. Stores UPN, first name, last name, userid, password, work phone, role, park, access to sensitive data (controlled unclassified information (CUI)), and email of NPS users and non-badged volunteers, interns and contractors.

HPF stores name and contact information for property point of contact and other persons associated to the site, including subgrantee, contractor, National Environmental Policy Act (NEPA) consulting parties, and easement holders. HPF records name and contact information for State, Tribal, and local historic preservation office personnel system and their association to system activity on the property. HPF links records to the NPS Integrated Resource Management Application (IRMA). The IRMA PIA describes the information collected and shared by the IRMA system.

SAT/PA collects information on grant applicants, tax ID (which may be SSN), data universal numbering system (DUNS) No., agency/employer points of contact and authorized representatives, and NAGPRA collects applicant and/or institution information, employer ID no., name, company, title, phone, email, patrimony, case no., Tribe and Tribe contacts and activities as well as dates, descriptions, and activity on penalties, violations, allegations, and the associated NPS Reviewer.

Both SAT/PA and NAGPRA collect the Grant ID and documents downloaded from Grants.gov. The OS Grants.gov (hhs.gov) describes the information collected and shared by Grants.gov.

A comment field is available to the NPS staff in each of the applications. A notice to avoid entering PII in the comment field is published with the comment field on the website. The comment field is only available to NPS users, and NPS users must undergoing annual privacy awareness training.

PII for Government Users (NPS employees and other NPS badged contractors and volunteers) is required for authentication, account management and logging purposes. NPS users use their government issued PIV card authenticated through the Enterprise Active Directory (AD). CRPS collects the subsystem user's name, email address, username, and role or access level for authorized users.

Non-NPS users may voluntarily request an account which must be approved by an NPS program manager. The PII required to create a user account includes the individual's name, email address, userid, password, and work phone.

**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:

**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
☒ Other:

Information collected from submission of paper and faxed forms and correspondence received from SHPOs and applicants is entered into the applicable subsystem by NPS staff. Paper and faxed forms and correspondence are secured and managed pursuant to NPS policies and procedures by NPS staff in locked offices and file cabinets until transfer to the National Archives and Records Administration in accordance with the applicable records schedule.

Both SAT/PA and NAGPRA collect the Grant ID and documents downloaded from Grants.gov. The OS Grants.gov (hhs.gov) describes the information collected and shared by Grants.gov.

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

The PII collected is used to track the receipt and processing of applications for NPS certification for Federal income tax incentives for historic preservation, track and process grant applications and results, and to comply with legal and regulatory requirements for cataloging and reporting on cultural resources and historic properties.

PII collected from the non-NPS users for account creation and management is used to authenticate individuals and to enable the individuals to participate in CRPS system process 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 e-mail is sent for account activation, account reset and change alerts.

PII collected from NPS Users will be used by system to securely authenticate individuals to the system, manage user roles and permissions, enable change and audit logging, record actions (e.g. violations, penalties) associated with historic properties or projects.

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

☒ Within the Bureau/Office:

Within the Cultural Resources, Partnership, and Science directorate, staff from the Technical Preservation Services and National Register/National Historic Landmarks divisions and the Chief Appeals Officer use the database system to enter data and track the processing of applications requesting NPS certification.

Limited Tax Act PII (applicant names and addresses only) is shared with the NPS Office of Legislative and Congressional Affairs who use the information to notify Congressional members of certified, completed tax incentive projects in their respective state/district.

Data sharing will be restricted between and within the CRPS based on the user's role and permission assignment.

☐ Other Bureaus/Offices:

☒ Other Federal Agencies:

The federal income tax incentives for historic preservation are administered by the NPS and the Internal Revenue Service (IRS). The Internal Revenue Code (Sections 47 and 170) requires the Secretary of the Interior to provide certain "certifications" to the Secretary of the Treasury regarding the historic significance of a property and whether the rehabilitation preserves its historic character. The IRS is responsible for administering all tax code aspects of the program. The NPS regularly provides copies of the data in the database system to the IRS for its use in administering the TaxAct programs.

☒ Tribal, State or Local Agencies:

The NPS administers its certification of tax incentive applications in partnership with the State, Tribal, and local Historic Preservation Offices (SHPOs). All applications go through the SHPOs, which retain a copy and provide feedback to the NPS. SHPOs may request an account and provide and access PII in CRPS subsystems.

☒ Contractor:

CRPS's contractors provide application development, improvement, and maintenance of CRPS systems. 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.

☒ Other Third-Party Sources:

NPS provides limited information to Congressional members on historic rehabilitation projects in their district requesting NPS certification. This information includes the name and address of applicants applying for the tax incentive benefits.

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

☒ Yes:

Individuals may decline to provide PII when applying for a grant or tax credit, registering or working on a historic property or landmark, or requesting a system user account; however, declining to provide information may impact the ability of NPS to process grant or tax credit applications, register historic properties, authorize system accounts, or communicate with an individual pursuing associated Federal benefits. Failure to provide information may impact a person or organization's participation or employment on historic preservation projects.

For DOI AD Users this information from DOI AD is collected from the individual during onboarding or generated as DOI records (e.g., business phone, UPN) during operational activities. PII is collected from DOI AD users who must use the system to perform the duties of their employee, contract, or volunteer position. DOI AD Users may decline to provide information during the onboarding process; however, this may result in reassignment to another position or a withdrawal of the offer of employment.

☐ No

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

☒ Privacy Act Statement:

Users are provided a Privacy Act Statement on grant, tax credit, and National Register paper application forms.

☒ Privacy Notice:

Notice is provided through publication of this PIA and the applicable published SORN. A link to a privacy notice will be provided on every screen where PII is collected.

☒ Other:

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.).**

Information in the system may be retrieved by the name of a historic property, by property location, by NPS system-assigned project number, or by using a person's name.

**I. Will reports be produced on individuals?**

☐ Yes

☒ No

Reports are produced on projects or properties but not on individuals.

## Section 3. Attributes of System Data

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

Where possible, PII information is collected directly from the applicant or owner/agent for the project or property using standard application forms. The SHPO is responsible for verifying accuracy of the data before submission of the forms to NPS or entering the data into CRPS. NPS staff review data for accuracy during the relevant data entry, application, certification, or adjudication processes. NPS Program Managers also provide oversight to NPS staff to ensure data accuracy.

**B. How will data be checked for completeness?**

To the extent practicable, data entry validations will be implemented to ensure data integrity and completeness. SHPOs and NPS staff during the data entry, application, certification, or adjudication processes may periodically verify information provided is complete.

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

All applications, registrations, and inventories will be actively managed until close out of the respective processes. Individuals may periodically be contacted to update their information by SHPOs or NPS staff. SHPOs and NPS staff are responsible for maintaining current inventories and to follow up with applicants and owner/agents for the project or property.

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

Records 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. Nl-79-0801). The disposition for CRPS records is permanent and records are transfer 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 National Archives when 3 years old. Digital records will be transferred according to standards applicable at the time. Transfer all other permanent records to NARA 7 years after closure.

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

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 are transferred to the National Archives when 3 years old. Digital records will be transferred according to standards applicable at the time. All other permanent records are transferred to NARA 7 years after closure.

**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.**

The privacy risks to individuals are considered moderate due to the PII collected, and CRPS is classified as a FISMA Moderate system.

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 will be referenced in the System Security and Privacy Plan. Risk is also mitigated through system design and implementation.

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. Access to administrative functions is strictly controlled. System administrators periodically review audit logs to prevent unauthorized monitoring. Users are required to accept rules of behavior when using the system. All users must have an account in the system and user authentication protocols are enforced based on the user's role and permissions, i.e., PIV cards, if applicable. Government Users will be authorized for their role and permissions using a formal process for ensuring least privilege access is maintained before their accounts are created in Role Based Access Control (RBAC) system. Government Users will authenticate to RBAC using the applicable agency identity provider (e.g., Active Directory Federated Services for DOI) and their GSAccess issued PIV card.

There is a risk that unauthorized persons could potentially gain access to the PII on the stored forms or during the form's submission process. Paper, faxed, and email scanned, or printed forms and correspondence are maintained under cabinet lock and key and retained for 7 years and then sent to the National Archive center.

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 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. Contingency plans and procedures will be defined to ensure the ability to recover in the event of improper data disposal.

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, applicable SORNs, privacy notice, and Privacy Act Statements. During the development of this PIA, the NPS identified the need to publish new SORNs for the historic preservation tax incentive records under the TaxAct, NRIS-NHL, and LOOT records. This PIA will be updated when these SORNs are published.

## 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

Information collected is relevant and necessary to comply with legal and regulatory requirements to register and preserve historic places and landmarks, to track grant and tax incentive applications for receipt of federal benefits, and to improve NPS cultural resources management utilizing best-available information.

☐ No

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

☐ Yes

☒ No

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

☐ Yes

☒ No

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

☐ Yes

☒ No

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

Not applicable.

**F. Are the data or the processes being consolidated?**

☐ Yes, data is being consolidated.

☐ Yes, processes are being consolidated.

☒ 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*

**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 based on authorized and assigned roles and permissions. Roles and permissions must be authorized by the appropriate program manager. The permissions will determine what function the user may execute in the system and define what records the user can enter, edit, read, or delete.

System administrators may on occasion be required to view username, permission 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

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, 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 privacy and 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) regarding sensitive data.

☐ 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

CRPS will not be used for monitoring members of the public.

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. 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 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?**

System logging records all attempted access to the system from users and internal processes, including monitoring, maintenance, and audit processes. Data logged includes unique identifiers, usernames, timestamp, event information, source, successful/unsuccessful login attempts, edits to selected data elements.

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

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 Associate Director, Cultural Resources, Partnerships, and Science serves as the 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 CRPS. 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 CRPS, 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 Information System Owner and 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 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.