## Appendix A: DI-4001 PIA Form

## 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:** Permits for Archeological Investigations – NPS-32

**Date:** 2/8/2018

**Bureau/Office:** National Park Service

**Bureau/Office Contact Title:** Departmental Consulting Archeologist

**Point of Contact**
Email: DCA@NPS.gov
First Name: Stanley
M.I.: C
Last Name: Bond
Phone: 304-535-3123
Address Line 1: 1849 C Street NW MS7508 MIB
Address Line 2:
City: Washington
State/Territory: DC
Zip: 20240

## Section 1. General System Information

**A. Is a full PIA required?**

*This is a threshold question. Indicate whether the system collects, maintains, uses or disseminates information about members of the general public, Federal employees, contractors, or volunteers. If the system does not contain any information that is identifiable to individual (e.g., statistical, geographic, financial), complete all questions in this section and obtain approval and required signatures in Section 5. The entire PIA must be completed for systems that contain information identifiable to individuals, including employees, contractors and volunteers.*

☒ 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?**

*Describe the purpose of the system and how it relates to the program office's and Department's mission. Include the context and background necessary to understand the purpose, the name of the program office and the technology, project or collection being assessed.*

The Regions of the National Park Service (NPS) maintain the Permit for Archeological Investigations Application system of records. The purpose of the system is to provide a Regional Director with information to approve or deny requests for archeological investigations in a park unit within that region. The system also assists park staff to monitor the activity to ensure that the permitted activity does not interfere with the enjoyment of the park by visitors and that the natural and cultural resources of the park are protected.

**C. What is the legal authority?**

*A Federal law, Executive Order of the President (EO), or DOI requirement must authorize the collection and maintenance of a system of records. For Privacy Act systems, the response should reflect the information provided in the authority section of the Privacy Act system of records notice.*

The Archaeological Resources Protection Act of 1979
(16 U.S.C. 470aa-mm; 43 CFR 7); The Antiquities Act of 1906
(P.L. 59-209; 34 Stat. 225; 54 U.S.C. 320302-320303; 43 CFR 3); and the appropriate Bureau-specific statute such as The Reclamation Act, The National Park Service Organic Act, The National Wildlife Refuge System Administration Act, or The Federal Land Policy and Management Act.

**D. Why is this PIA being completed or modified?**

*Indicate why the PIA is being conducted. For example, the system is being significantly modified or two systems are being merged together.*

- ☒ 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?**

*The completed PIA, associated system of records notice(s), and any other supporting artifacts must be entered into the CSAM system for each registered system or application.*

☐ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

☒ No

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

*Enter "None" if no subsystems or applications are hosted. For General Support Systems (GSS) be sure to include all hosted major applications, minor applications, or other subsystems, and describe the purposes and types of PII if any. Privacy risks must be identified and adequately addressed for each hosted application or subsystem identified in the GSS PIA. A separate PIA should be conducted for each hosted application or subsystem that contains PII to ensure privacy implications are assessed. In any case, the GSS PIA must identify all hosted applications, describe the relationship, and reference or append the PIAs conducted for the hosted applications. The GSS PIA and associated PIAs must be reviewed and approved by all officials as appropriate; and all related PIAs, SORNs and supporting artifacts must be entered into CSAM.*

There are no minor systems or subsystems that are hosted on this system.

| **Subsystem Name** | **Purpose** | **Contains PII** *(Yes/No)* | **Describe** *If Yes, provide a description.* |
|---|---|---|---|
| **N/A** | **N/A** | N/A | **N/A** |

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

*A Privacy Act SORN is required if the information system or electronic collection contains information about individuals that is retrieved by name or other unique identifier. Provide the DOI or Government-wide Privacy Act SORN identifier and ensure it is entered in CSAM for this system. For new SORNS being developed, select "Yes" and provide a detailed explanation. Contact your Bureau Privacy Officer for assistance identifying the appropriate Privacy Act SORN(s).*

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

Permits for Archeological Investigations - NPS 32

☐ No

**H. Does this information system or electronic collection require an OMB Control Number?**
*The Paperwork Reduction Act requires an OMB Control Number for certain collections of information from ten or more members of the public. If information is collected from members of the public, contact your Bureau Information Collection Clearance Officer for assistance to determine whether you need to obtain OMB approval. Please include all OMB Control Numbers and Expiration Dates that are applicable.*

☒ Yes: *Describe* OMB No. 1024-0037 Exp. Date (07/31/2017)

☐ No

## Section 2. Summary of System Data

**A. What PII will be collected? Indicate all that apply.**
*Identify all the categories of PII that will be collected, stored, used, maintained or disseminated. Describe any additional categories of PII not already indicated, as well as any new information that is created (for example, an analysis or report), and describe how this is done and the purpose of that information.*

☒ Name
☐ Citizenship
☐ Gender
☐ Birth Date
☐ Group Affiliation
☐ Marital Status
☐ Biometrics
☐ Other Names Used
☐ Truncated SSN
☐ Legal Status
☐ Place of Birth
☐ Religious Preference
☐ Security Clearance
☐ Spouse Information
☐ Financial Information
☐ Medical Information
☐ Disability Information
☐ Credit Card Number
☐ Law Enforcement
☒ Education Information
☐ Emergency Contact
☐ Driver's License
☐ Race/Ethnicity
☐ Social Security Number (SSN)
☐ Personal Cell Telephone Number
☐ Tribal or Other ID Number
☐ Personal Email Address
☐ Mother's Maiden Name
☐ Home Telephone Number
☐ Child or Dependent Information
☒ Employment Information
☐ Military Status/Service
☐ Mailing/Home Address
☐ Other: *Specify the PII collected.* handle (forum username)

The information to be collected by an application for a Permit for Archeological Investigations is specified in regulations for the Archaeological Resources Protection Act. (43 CFR 7)

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

*Include all sources of PII collected. For example, information may be collected directly from an individual through a written form, website collection, or through interviews over the phone or in person. Information may also come from agency officials and employees, agency records, from a computer readable extract from another system, or may be created within the system itself. If information is being collected through an interface with other systems, commercial data aggregators, or other agencies, list the source(s) and explain why information from sources other than the individual is required.*

- [x] Individual
- [ ] Federal agency
- [ ] Tribal agency
- [ ] Local agency
- [ ] DOI records
- [ ] Third party source
- [ ] State agency
- [x] Other: *Describe* PII is obtained from individuals who are applying for a Permit for Archeological Investigations. The individual may be representing an institution of higher learning, a commercial company, or a governmental agency.

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

*Indicate all the formats or methods for collecting PII that will be used. If the system receives information from another system, such as a transfer of financial information or response to a background check, describe the system from which the information originates, how the information is used, and how the systems interface.*

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

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

*Describe the intended uses of the PII collected and maintained in the system and provide a detailed explanation on how the data will be used. The intended uses must be relevant to the purpose of the system; for Privacy Act systems, uses must be consistent with the published system of records notice.*

The primary purpose of the system is to assist Federal agencies in identifying qualified and competent archeological research projects; monitoring fieldwork; and ensuring that all field records and copies of reports are submitted to the land manager and material objects are appropriately curated.

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

*Indicate all the parties, both internal and external to DOI, with whom PII will be shared. Identify other DOI offices with assigned roles and responsibilities within the system, or with whom information is shared, and describe how and why information is shared. Also, identify other federal, state and local government agencies, private sector entities, contractors or other external third parties with whom information is shared; and describe any routine information sharing conducted with these external agencies or parties, and how such external sharing is compatible with the original purpose of the collection of the information. If sharing is pursuant to a Computer Matching Agreement, provide an explanation. For Privacy Act systems, describe how an accounting for the disclosure is maintained.*

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

Any NPS employee acting in his or her individual official capacity can view PII data that is recorded on an application for a Permit for Archeological Investigations.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*
Application information may be shared with other offices, programs, and bureaus participating in joint research projects.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*
Application information may be shared with other Federal agencies participating in joint research projects.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*
Application information may be shared during tribal consultations concerning potential impact on tribally associated cultural resources.

☒ Contractor: *Describe the contractor and how the data will be used.*
Application information will be shared with an expert, consultant, or contractor (including employees of the contractor) of the NPS that performs services requiring access to these records on NPS' behalf.

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

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

*If "Yes," describe the method by which individuals can decline to provide information or how individuals consent to specific uses. If "No," state the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

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

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

The information is necessary to determine whether issuance of a Permit for Archeological Investigations is appropriate.

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

*Describe how notice is provided to the individual about the information collected, the right to consent to uses of the information, and the right to decline to provide information. For example, privacy notice to individuals may include Privacy Act Statements, posted Privacy Notices, privacy policy, and published SORNs and PIAs. Describe each format used and, if possible, provide a copy of the Privacy Act Statement, Privacy Notice, or a link to the applicable privacy policy, procedure, PIA or referenced SORN Federal Register citation (e.g., XX FR XXXX, Date) for review. Also describe any Privacy Act exemptions that may apply and reference the Final Rule published in the Code of Federal Regulations (43 CFR Part 2).*

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

A Privacy Act Statement will be included on the last page of the application.

☐ Privacy Notice: *Describe each applicable format.*

☐ Other: *Describe each applicable format.*

☐ None

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

*Describe how data is retrieved from the system. For example, is data retrieved manually or via reports generated automatically? Are specific retrieval identifiers used or does the system use key word searches? Be sure to list the identifiers that will be used to retrieve data (e.g., name, case number, Tribal Identification Number, subject matter, date, etc.).*

Records within this system can be retrieved by searching a Permit spreadsheet kept by each NPS region. The record may be identified by searching various fields, including the name of the correspondent, the Permit number, or location or year of project, and retrieving the appropriate paper or electronic file in which the PII is stored.

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

*Indicate whether reports will be produced on individuals. Provide an explanation on the purpose of the reports generated, how the reports will be used, what data will be included in the reports, who the reports will be shared with, and who will have access to the reports. Many systems have* *features that allow reports to be generated on data in the system or on user actions within the system.*

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

☒ No

## Section 3. Attributes of System Data

**A. How will data collected from sources other than DOI records be verified for accuracy?**
*Data accuracy and reliability are important requirements in implementing the Privacy Act which requires that agencies only maintain data that is accurate, relevant, timely, and complete about individuals. The information has to have some form of verification for accuracy due to the Privacy Act provisions that require that only relevant and accurate records should be collected and maintained about individuals.*

The PII provided on the application is given voluntarily and accuracy is verified only within the context of granting the Permit.

**B. How will data be checked for completeness?**
*Describe the procedures to ensure data is checked for completeness. To the extent practical, PII should be checked for completeness to ensure accuracy within the context of the use of the data.*

A Permit is only issued after park and regional reviewers are satisfied that the application is complete and accurate and the proposed project supports agency mission and park needs.

**C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).**
*Describe the steps or procedures taken to ensure the data is current and not out-of-date. Where are they documented? For example, are they outlined in standard operating procedures or data models? Data that is not current also affects the relevancy and accuracy of the data. This is particularly true with data warehousing. A data warehouse is a repository of an organization's electronically stored data and is designed to facilitate reporting and analysis. A data warehouse may contain data that is not current which would cause a domino effect throughout the data stores.*

It is the responsibility of the applicant to ensure that the data are accurate; NPS relies on the information provided to it by the individual applicant to ensure the data is current.

**D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.**
*Identify all applicable records retention schedules or explain at what development stage the proposed records retention schedule is in. Information system owners must consult with Bureau/Office Records Officers early in the development process to ensure that appropriate retention and destruction schedules are identified, or to develop a records retention schedule for*

*the records contained in the information system. Be sure to include applicable records retention schedules for different types of information or subsets of information and describe if subsets of information are deleted and how they are deleted.*

Permits for Archeological Investigations are permanent, 15-year retention for paper and 3-year retention for electronic. The disposition authority can be found in NPS Records Schedule, DO-11D, Item 1 A.1. The NARA reference citation for the disposition authority is N1-079-08-001, Item 1A1.

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

*Describe policies and procedures for how PII that is no longer relevant and necessary is purged. This may be obtained from records retention schedules, the Departmental Manual, bureau/office records management policies, or standard operating procedures.*

Permanent records that are no longer active or needed for agency use are transferred to the National Archives for permanent retention in accordance with NARA guidelines.

Rejected applications are returned to the applicant.

**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.**

*Describe and analyze the major potential privacy risks identified and discuss the overall impact on the privacy of employees or individuals. Include a description of how the program office has taken steps to protect individual privacy and mitigate the privacy risks. Provide an example of how information is handled at each stage of the information life cycle. Also discuss privacy risks associated with the sharing of information outside of the Department and how those risks were mitigated. Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department.*

The records contained in this system are safeguarded in accordance with 43 CFR 2.226 and other applicable security and privacy rules and policies. During normal hours of operation, paper records are maintained in locked file cabinets under the control of authorized personnel. Computer servers on which electronic records are stored are located in secured DOI controlled facilities with physical, technical and administrative levels of security to prevent unauthorized access to the DOI network and information assets. Access granted to authorized personnel is password-protected, and each person granted access to the system must be individually authorized to use the system. A Privacy Act Warning Notice appears on computer monitor screens when records containing information on individuals are first displayed. Data exchanged between the servers and the system is encrypted. Backup media are encrypted and stored in a locked and controlled room in a secure, off-site location.

## Section 4. PIA Risk Review

**Appendix A – DI-4001 PIA Form**

**A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**
*Describe how the use of the system or information collection relates to the purpose of the underlying mission of the organization. Is the information directly relevant and necessary to accomplish the specific purposes of the system? For Privacy Act systems, the Privacy Act at 5 U.S.C. 552a(e)(1) requires that each agency shall maintain in its records only such information about an individual that is relevant and necessary to accomplish an agency purpose required by statute or by executive order of the President.*

☒ Yes: *Explanation* The PII provided in the application allows reviewers to assess the competency of the applicant and capacity of the company to carry out the research. The contact information allows NPS reviewers to communicate with the applicant.

☐ No

**B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?**
*Does the technology create new data or conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? Is data aggregated in a way that will permit system users to easily draw new conclusions or inferences about an individual? Electronic systems can sift through large amounts of information in response to user inquiry or programmed functions, or perform complex analytical tasks resulting in other types of data, matching, relational or pattern analysis, or reporting. Discuss the results generated by these uses and include an explanation on how the results are generated, whether by the information system or manually by authorized personnel. Explain the purpose and what will be done with the newly derived data. Derived data is obtained from a source for one purpose and then used to deduce/infer a separate and distinct bit of information to form additional information that is usually different from the original source information. Aggregation of data is the taking of various data elements and turning it into a composite of all the data to form another type of data, e.g., tables or data arrays.*

☐ 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?**
*Will the results or new data be placed in individuals' records? Explain in detail the purpose of creating the new data, how it will be used, by whom it will be used, with whom it will be shared, and any resulting effect on individuals.*

☐ Yes: *Explanation*

☒ No

**D. Can the system make determinations about individuals that would not be possible without the new data?**
*Will the new data be used to make determinations about individuals or will it have any other effect on the subject individuals? Explain in detail the purpose of creating the new data, how it will be used, by whom it will be used, with whom it will be shared, and any resulting effect on individuals.*

☐ Yes: *Explanation*

☒ No

**E. How will the new data be verified for relevance and accuracy?**
*Explain how accuracy of the new data is ensured. Describe the process used for checking accuracy. Also explain why the system does not check for accuracy. Describe any technical solutions, policies, or procedures focused on improving data accuracy and integrity of the project.*

There is no new data.

**F. Are the data or the processes being consolidated?**
*If the data is being consolidated, that is, combined or united into one system, application, or process, then the existing controls should remain to protect the data. If needed, strengthen the control(s) to ensure that the data is not inappropriately accessed or used by unauthorized individuals. Minimum sets of controls are outlined in OMB Circular A-130, Appendix III. The DOI Security Control Standards (based on NIST SP 800-53 and FedRAMP) describe the practice of identification and authentication that is a technical measure that prevents unauthorized people or processes from accessing data. The IT Security A&A process requires a system security plan outlining the implementation of the technical controls associated with identification and authentication.*

☐ 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.**
*Describe the process by which an individual receives access to the information within the system. Explain what roles these individuals have and their level of access. If remote access to the system is allowed or external storage or communication devices interact with the system, describe any measures in place to secure the transmission and storage of data (e.g., encryption and/or two-factor authentication). Do users have "read-only" access or are they authorized to*

*make changes in the system? Also consider "other" users who may not be as obvious, such as the GAO or the Inspector General, database administrators, website administrators or system administrators. Also include those listed in the Privacy Act system of records notice under the "Routine Uses" section when a Privacy Act system of records notice is required.*

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

Summary data are recorded on spreadsheets maintained on NPS servers that can be viewed by authorized users –NPS staff and NPS Regional Directors. Files are kept in locked cabinets.

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DOI as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:
(1) (a) To any of the following entities or individuals, when the circumstances set forth in paragraph (b) are met:
(i) The U.S. Department of Justice (DOJ);
(ii) A court or an adjudicative or other administrative body;
(iii) A party in litigation before a court or an adjudicative or other administrative body; or
(iv) Any DOI employee acting in his or her individual capacity if DOI or DOJ has agreed to represent that employee or pay for private representation of the employee;
(b) When:
(i) One of the following is a party to the proceeding or has an interest in the proceeding:
(A) DOI or any component of DOI;
(B) Any other Federal agency appearing before the Office of Hearings and Appeals;
(C) Any DOI employee acting in his or her official capacity;
(D) Any DOI employee acting in his or her individual capacity if DOI or DOJ has agreed to represent that employee or pay for private representation of the employee;
(E) The United States, when DOJ determines that DOI is likely to be affected by the proceeding; and
(ii) DOI deems the disclosure to be:
(A) Relevant and necessary to the proceeding; and
(B) Compatible with the purpose for which the records were compiled.
(2) To a congressional office in response to a written inquiry that an individual covered by the system, or the heir of such individual if the covered individual is deceased, has made to the office.
(3) To the Executive Office of the President in response to an inquiry from that office made at the request of the subject of a record or a third party on that person's behalf, or for a purpose compatible with the reason for which the records are collected or maintained.
(4) To any criminal, civil, or regulatory law enforcement authority (whether Federal, state, territorial, local, tribal or foreign) when a record, either alone or in conjunction with other information, indicates a violation or potential violation of law – criminal, civil, or regulatory in nature, and the disclosure is compatible with the purpose for which the records were compiled.

(5) To an official of another Federal agency to provide information needed in the performance of official duties related to reconciling or reconstructing data files or to enable that agency to respond to an inquiry by the individual to whom the record pertains.

(6) To Federal, state, territorial, local, tribal, or foreign agencies that have requested information relevant or necessary to the hiring, firing or retention of an employee or contractor, or the issuance of a security clearance, license, contract, grant or other benefit, when the disclosure is compatible with the purpose for which the records were compiled.

(7) To representatives of the National Archives and Records Administration (NARA) to conduct records management inspections under the authority of 44 U.S.C. 2904 and 2906.

(8) To state, territorial and local governments and tribal organizations to provide information needed in response to court order and/or discovery purposes related to litigation, when the disclosure is compatible with the purpose for which the records were compiled.

(9) To an expert, consultant, or contractor (including employees of the contractor) of DOI that performs services requiring access to these records on DOI's behalf to carry out the purposes of the system.

(10) To appropriate agencies, entities, and persons when:

(a) DOI suspects or has confirmed that there has been a breach of the system of records;

(b) DOI has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOI (including its information systems, program, and operations), the Federal government, or national security; and

(c) the disclosure made to such agencies, entities and persons is reasonably necessary to assist in connection with DOI's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

(11) To another Federal agency or Federal entity, when DOI determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in:

(a) responding to a suspected or confirmed breach; or

(b) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

(12) To the Office of Management and Budget (OMB) during the coordination and clearance process in connection with legislative affairs as mandated by OMB Circular A-19.

(13) To the Department of the Treasury to recover debts owed to the United States.

(14) To the news media and the public, with the approval of the Public Affairs Officer in consultation with counsel and the Senior Agency Official for Privacy, where there exists a legitimate public interest in the disclosure of the information, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(15) To State Historic Preservation Offices in states where research took place, that maintains registers of known archeological sites located within the state, including sites on Federal lands. Shared information includes locational data, summary site data, contact information for investigators, and copies of research reports.

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

*Users are normally only given access to certain data on a "need-to-know" basis for information that is needed to perform an official function. Care should be given to avoid "open systems"* *where all information can be viewed by all users. System administrators may be afforded access to all of the data depending upon the system or application. However, access should be restricted when users may not need to have access to all the data. For more guidance on this, refer to the Federal Information Processing Standards [FIPS] Publications in the authorities section. The DOI Security Control Standards (based on NIST SP 800-53 and FedRAMP) describe the practice of applying logical access controls, which are system-based means by which the ability is explicitly enabled or restricted. It is the responsibility of information system owners to ensure no unauthorized access is occurring.*

Only cultural resource specialists and NPS Regional Directors and staff have direct access to files in which applications for a Permit for Archeological Investigations are maintained. Information from the files is shared as necessary.

**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?*

☒ No

**J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?**
*Are there new technologies used to monitor activities of the individual in any way? Access logs may already be used to track the actions of users of a system. Describe any new software being used, such as keystroke monitoring.*

☐ Yes. *Explanation*

☒ No

**K. Will this system provide the capability to identify, locate and monitor individuals?**
*Most systems now provide the capability to identify and monitor individual's actions in a system (e.g., audit trail systems/ applications). For example, audit logs may record username, time and date of logon, files accessed, or other user actions. Check system security procedures for information to respond to this question.*

☒ Yes.

The system can *identify* applicants by their names.

The system can *locate* employers and contact applicants.

The system does not actively *monitor* applicants outside of the archeological investigations.

☐ No

**L. What kinds of information are collected as a function of the monitoring of individuals?**
*The DOI Security Control Standards (based on NIST SP 800-53 and FedRAMP) detail how audit logs should be used for DOI systems. Provide what audit activities are maintained to record system and user activity including invalid logon attempts and access to data. The IT Security A&A process requires a system security plan outlining the implementation of the technical controls associated with identification and authentication of users to the system. Examples of information collected may include username, logon date, number of failed logon attempts, files accessed, and other user actions on the system.*

The system does not actively monitor applicants.

**M. What controls will be used to prevent unauthorized monitoring?**
*Certain laws and regulations require monitoring for authorized reasons by authorized employees. Describe the controls in place to ensure that only authorized personnel can monitor use of the system. For example, business rules, internal instructions, posting Privacy Act Warning Notices address access controls, in addition to audit logs and least privileges. It is the responsibility of information system owners and system managers to ensure no unauthorized monitoring is occurring.*

All authorized users are trained and required to follow established internal security protocols and must complete all security, privacy, and records management training and sign the DOI Rules of Behavior. A Privacy Impact Assessment was conducted on the Permits for Archeological Investigations to ensure that Privacy Act requirements are met and appropriate privacy controls were implemented to safeguard the personally identifiable information contained in the system.

**N. How will the PII be secured?**
*Discuss how each privacy risk identified was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included. Describe auditing features, access controls, and other possible technical and policy safeguards such as information sharing protocols, or special access restrictions. Do the audit features include the ability to identify specific records each user can access? How is the system audited? For example, does the system perform self audits, or is the system subject to third party audits or reviews by the Office of Inspector General or Government Accountability Office (GAO). Does the IT system have automated tools to indicate when information is inappropriately accessed, retrieved or misused? Describe what privacy and security training is provided to system users. Examples of controls include rules of behavior, encryption, secured facilities, firewalls, etc.*

(1) Physical Controls. Indicate all that apply.

☐ Security Guards
☐ Key Guards
☒ Locked File Cabinets

- [x] Secured Facility
- [ ] Closed Circuit Television
- [ ] Cipher Locks
- [ ] Identification Badges
- [ ] Safes
- [ ] Combination Locks
- [x] Locked Offices
- [ ] Other. *Describe*

(2) Technical Controls. Indicate all that apply.

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

(3) Administrative Controls. Indicate all that apply.

- [ ] Periodic Security Audits
- [x] Backups Secured Off-site
- [x] 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
- [x] 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.**

*Although all employees who have access to information in a Privacy Act system have responsibility for protecting and safeguarding that information, often the information system owner and Privacy Act system manager share the responsibility for protecting the privacy rights of employees and the public. For Privacy Act responsibilities refer to 383 Department Manual Chapters 1-13 and DOI Privacy Act regulations at 43 CFR Part 2. Also, describe how Privacy Act complaints and requests for redress or amendment of records are addressed.*

The information system owner and NPS Privacy officer share the responsibility of protecting the privacy rights of the public and employees. Privacy Act complaints and requests for redress will be handled jointly between these two entities.

**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?**

*This may be the information system owner and Privacy Act system manager, or may be another individual with designated responsibility, or otherwise stipulated by contract or in language contained in an agreement (e.g., Head of the Bureau or Program Manager). There may be multiple responsible officials. Consider a system that contains several databases from different program offices; there may be one information system owner and several Privacy Act system managers. Also, describe who is responsible for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information.*

There are potentially several parties responsible for assuring the proper use of data and reporting potential Privacy Act violations or unauthorized access; the core responsible parties include the NPS Regional Director, park superintendent, Departmental Consulting Archeologist, NPS Privacy officer, and NPS Information Technology Security office (ITSO).

## Section 5. Review and Approval

PIAs for Bureau or Office level systems must be signed by the designated Information System Owner, Information System Security Officer, and Bureau Privacy Officer, and approved by the Bureau Assistant Director for Information Resources as the Reviewing Official. Department-wide PIAs must be signed by the designated Information System Owner, Information System Security Officer, and Departmental Privacy Officer, and approved by the DOI Chief Information Officer/Senior Agency Official for Privacy as the Reviewing Official.

**Information System Owner**

Email: Stanley_C_Bond@NPS.gov
First Name: Stanley M.I.: C Last Name: Bond Title: Departmental Consulting Archeologist
Bureau/Agency: National Park Service Phone: 202-354-2123 Date: 02/08/2018

Signature:

**Information System Security Officer**

Email:
First Name: M.I.: Last Name: Title:
Bureau/Agency: National Park Service Phone: Date:

Signature:

**Privacy Officer**

**Appendix A – DI-4001 PIA Form**

Email: teri_barnett@ios.doi.gov
First Name: Teri M.I.: Last Name: Barnett Title: Departmental Privacy Officer
Bureau/Agency: Office of the Chief Information Officer Phone: 2022081943 Date:

Signature:

**Reviewing Official**

Email: Shane_Compton@nps.gov
First Name: Shane M.I.: Last Name: Compton Title: Associate Director, Information Resources
Bureau/Agency: National Park Service Phone: 2022082433 Date:

Signature: