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: NPS Cloud Hosting I
Bureau/Office: National Park Service, Information Resources Management Directorate
Date: November 15, 2022
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 Services (NPS) Cloud Hosting I is managed by the NPS Information Resources Management Directorate and provides infrastructure, software and platform hosting services supporting mission-related applications used by the NPS. Cloud Hosting I provides hosting infrastructure, software, and platform services to applications and systems which may

collect, store, disseminate, or dispose of Personally Identifiable Information (PII) of employees, contractors, volunteers, or members of the public. Applications and systems using Cloud Hosting I services are responsible for conducting and publishing the applicable Privacy Impact Assessments (PIAs) which are available for review on the Department of the Interior (DOI) PIA website at https://www.doi.gov/privacy/pia.

The NPS Cloud Hosting I provides a virtual cloud backup solution for the Enterprise Data Center (EDC) and storage repositories that facilitate creation, storage, sharing, and collaborative work for all types of electronic files which may include documents, forms, reports, correspondence, briefing papers, committee and meeting minutes, contracts, grants, leases, permits, audits, manuals, studies, promotional materials, compliance information and other confidential information. File rights can be further delineated to view only and edit/delete and allows staff to share information with business colleagues as needed. Users may store all types of electronic files including text, graphical, audio, or video files. There is a potential that large amounts of PII may be included in the documents stored. Each user/office program, application, or system utilizing Cloud Hosting I infrastructure is responsible for ensuring proper use of PII and for meeting privacy and security requirements within their organization.

Active Directory (AD) account information for user access authenticates to the Enterprise AD, which is assessed separately in the Enterprise Hosted Infrastructure PIA viewable at https://www.doi.gov/privacy/pia. Cloud Hosting I does not own or manage PII, however, the user community accesses services supported or administered by Cloud Hosting I that contain PII. It is the responsibility of the office or individual using Cloud Hosting I services to protect the information collected, used, maintained, or disseminated on Cloud Hosting I.

C. What is the legal authority?

- Government Organization and Employees, Departmental Regulations (5 U.S.C. 301)
- Paperwork Reduction Act of 1995 (44 U.S.C. 3501)
- Government Paperwork Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504)
- E-Government Act of 2002 (Public Law 107-347)
- Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004

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:

UII Code: 010-000002506
System Security and Privacy Plan (SSPP) Name: NPS Cloud Hosting I System Security and Privacy Plan

☐ 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.*
None			

The systems for which Cloud Hosting I provides infrastructure, software or platform hosting are not covered under this PIA or the Cloud Hosting I SSPP and are not designated as minor systems or subsystems of the Cloud Hosting I or its security boundary for privacy or cybersecurity risk and compliance management purposes. For each of these systems, the respective program management team is responsible for managing security and privacy risks for the applicable system and required to establish a security boundary, PIA, and SSPP distinct from Cloud Hosting I though they may coordinate or inherit select controls from Cloud Hosting I at Cloud Hosting I Program Management team discretion. Cloud Hosting I is not responsible for managing the data or system specific controls for these systems.

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

☒ Yes

Active Directory (AD) records are covered by INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040, March 12, 2007; modification published 86 FR 50156, September 7, 2021.

The Cloud Hosting I provides storage repositories that facilitate creation, storage, sharing, and collaborative work for all types of electronic records that may include PII. These records are under the control and ownership of each system owner, information owner, or Privacy Act

system manager who is responsible for meeting the requirements of the Privacy Act for the collection, maintenance and sharing of their records including publishing systems of records notices (SORNs) and addressing requests for notification, access, or amendment under the Privacy Act. The records within the applications and systems hosted by Cloud Hosting I may be covered by numerous government-wide, Department-wide or NPS SORNs, which may be viewed at https://www.doi.gov/privacy/sorn.

☐ No

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

☐ Yes
☒ No
Cloud Hosting I does not collect information from the public; however, Cloud Hosting I provides hosting services to applications and systems which may collect information from members of the public. Please see the applicable PIA for reference to the appropriate OMB Control Number for the hosted applications and systems.

Section 2. Summary of System Data

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

☒ 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:

A wide variety of PII data is potentially included in applications and systems hosted by Cloud Hosting I. Cloud Hosting I utilizes the EHI for authentication and may contain username, user principal name (UPN), work email address, work phone number, work address, title of DOI employee and contractor, and related organizational information required for system administration. Hosted applications and systems may store relational databases, unstructured data, and electronic files including text, graphical, audio, or video files, which may include documents, forms, reports, correspondence, briefing papers, committee and meeting minutes, contracts, grants, leases, permits, audits, manuals, studies, promotional materials, compliance information, and other documents within the Cloud Hosting I domain. There is a potential that large amounts of PII may be included in the data and documents stored. Information about individuals may include, but is not limited to, names, email addresses, telephone numbers, Social Security numbers (SSNs), dates of birth, financial information, employment history, educational background, correspondence, or comments from members of the public, and other information related to a specific mission purpose. Applications, websites, and forms may collect various types of PII or information on user behaviors. System and data owners are also responsible for implementing access controls and working with the bureau Associate Privacy Officer (APO) to ensure appropriate authority for the collection, issuance of an appropriate privacy notice, and assessment of privacy risks.

Cloud Hosting I provides cloud hosting services to applications and systems within the DOI environment. Please see the applicable PIA for the cloud hosted applications and systems for the types of PII and an evaluation of the privacy risks.

Cloud Hosting I uses DOI AD information (e.g., username, password, business contact information, security question answers, UPN, and user id), Personal Identification Verification (PIV) credentials, and security questions and answers to authenticate user identity and to assign

permissions to users. This information is collected and managed by DOI AD and not by Cloud Hosting I.

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*

Cloud Hosting I provides cloud hosting services to applications and systems within the DOI environment, therefore, there are numerous sources of PII collected. Please see the applicable PIA for the hosted applications and systems for the sources of PII collected by these applications and systems.

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

Cloud Hosting I provide cloud hosting services to applications and systems within the DOI environment, therefore, there may be numerous methods for collecting PII. Please see the applicable PIA for the hosted applications and systems for the formats and methods of PII collection for the applicable applications and systems.

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

Cloud Hosting I's intended use of PII is entirely in support of confidentiality, integrity, and availability of data and information for mission support systems and applications. Cloud Hosting I's purpose is to provide the cloud hosting infrastructure, including cloud storage area network and database servers. Cloud Hosting I's intended use of PII is solely to provide secure cloud storage of PII collected, managed, and used by the hosted systems in support of NPS and DOI

missions. Please see the applicable PIA for the hosted applications and systems for the intended use of PII collected for the applicable applications and systems.

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

☒ Within the Bureau/Office
Cloud Hosting I provides cloud hosting services to applications and systems within the DOI environment. Cloud Hosting I only provides information sharing with authorized NPS personnel supporting the hosted applications and systems and indirectly to users of these applications and systems. Please see the applicable PIA for the hosted applications and systems for the sharing of PII collected by these applications and systems.

☒ Other Bureaus/Offices
Cloud Hosting I provides cloud hosting services to applications and systems within the DOI environment. Cloud Hosting I only provides information sharing with authorized DOI personnel supporting the hosted applications and systems and indirectly to users of these applications and systems. Please see the applicable PIA for the hosted applications and systems for the sharing of PII collected by these applications and systems.

In case of a security event, information may be shared with DOI or the DOI Computer Incident Response Center (DOI-CIRC). Information is also shared with DOI to establish user accounts during the onboarding process.

☒ Other Federal Agencies
Cloud Hosting I provides cloud hosting services to applications and systems within the DOI environment. Cloud Hosting I does not share PII with other Federal agencies; however, the hosted applications or systems may participate in information sharing with other Federal agencies. Please see the applicable PIA for the hosted applications and systems for the sharing of PII collected by these applications and systems.

☒ Tribal, State or Local Agencies
Cloud Hosting I provides cloud hosting services to applications and systems within the DOI environment. Cloud Hosting I does not share PII with other Tribal, State or local agencies; however, the hosted applications or systems may participate in information sharing with other Tribal, State or local agencies. Please see the applicable PIA for the hosted applications and systems for the sharing of PII collected by these applications and systems.

☒ Contractor:
NPS may contract with other commercial organizations to provide configuration, operations, and maintenance of Cloud Hosting I or specific infrastructure or platform cloud components. Contractor staff are required to undergo background checks as defined by NPS policy and procedures. Contractor staff access is restricted on a need-to-know basis. Privileged accounts are audited, and authentication and other security and privacy controls are enforced as defined in the

SSPP. This maintenance is critical to protecting the system and the PII contained within the system. Cloud Hosting I's cloud infrastructure and platforms undergoes continuous monitoring by security staff to identify security vulnerabilities.

☒ Other Third-Party Sources
Cloud Hosting I provides cloud hosting services to applications and systems within the DOI environment. Cloud Hosting I only provides information sharing with authorized personnel supporting the hosted applications and systems and indirectly to users of these applications and systems. Cloud Hosting I does not share PII with other third-party sources except as noted above; however, the hosted applications or systems may participate in information sharing with third-party entities. Please see the applicable PIA for the hosted applications and systems for the sharing of PII collected by these applications and systems.

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

☒ Yes

Cloud Hosting I stores or manages PII collected through the cloud hosted applications and systems. Please see the applicable PIA for the hosted applications and systems for consent to uses of PII collected by these applications and systems.

For NPS staff account management, information is collected from the individual during onboarding or generated as DOI records (e.g., email address, UPN, username) during operational activities. While an individual's supervisor or Contracting Officer's Representative completes and submits the required information to create the individual's user account, this information is derived from on-boarding forms. These forms provide the requisite Privacy Act statement that informs the individual that providing the information is voluntary and the consequences of not providing the information may impact employment.

☐ No

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

☒ Privacy Act Statement

Cloud Hosting I stores or manages PII collected through the hosted applications and systems. Please see the applicable PIA for the hosted applications and systems for Privacy Act statements provided when PII is collected by these applications and systems.

For NPS staff, a Privacy Act Statement is included on the onboarding forms (e.g., OF 306, Declaration for Federal Employment and SF-85P, Questionnaire for Public Trust Positions)

which include the requisite information on the Authority, Purpose, Routine Uses, and Disclosure for collecting the information.

☒ Privacy Notice

Cloud Hosting I stores or manages PII collected through the hosted applications and systems. Please see the applicable PIA for the hosted applications and systems for privacy notices provided when PII is collected by these applications and systems.

Cloud Hosting I users can also view how their information will be used in this Cloud Hosting I PIA, and the INTERIOR/DOI-47 SORN, and other government-wide, Department-wide and NPS SORNs which may be viewed at https://www.doi.gov/privacy/sorn.

☐ Other

☐ None

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

Data is retrieved by the hosted applications and systems. Please see the applicable PIA for the hosted applications and systems for the identifiers used by the application or system to retrieve data or information.

Service Desk personnel can retrieve a user's account by their name or username within Cloud Hosting I. This is typically done at the behest of users in order to reset their passwords or to resolve computer and network issues.

I. Will reports be produced on individuals?

☐ Yes

☒ No

Cloud Hosting I does not produce reports on individuals. Please see the applicable PIA for the hosted applications and systems for reports produced on individuals by these applications and systems.

Automated scheduled and ad hoc reports may be generated to audit user activity and determine accounts which need to be disabled due to employee separation. Data will include name, username, activity date/time, location and applications accessed via Cloud Hosting I. Cloud Hosting I administrators have access to these reports. These audit functions are conducted by security information and event management (SIEM) tools owned and operated by DOI under a

separate security boundary and SSPP. Cloud Hosting I does not manage these tools, and they are not included in the scope of this PIA.

Section 3. Attributes of System Data

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

Cloud Hosting I collects data through the hosted applications and systems. Please see the applicable PIA for the hosted applications and systems for methods for verification of accuracy of data collected these applications and systems.

Cloud Hosting I does not collect data from other sources. The user can only access the Cloud Hosting I systems as a valid, authorized AD user with current and accurate credentials, an active PIV card, and a valid user account.

B. How will data be checked for completeness?

Cloud Hosting I provides cloud hosting services for data collected and managed through the hosted applications and systems. Please see the applicable PIA for the hosted applications and systems for methods for verification of completeness of data collected these applications and systems.

NPS staff users are responsible for the completeness of the data provided during onboarding and in the user account request form.

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

Cloud Hosting I provides cloud hosting services for data collected and managed through the hosted applications and systems. Please see the applicable PIA for the hosted applications and systems for methods for ensuring data collected by these applications and systems is current.

The NPS Information System Continuous Monitoring Plan (ISCMP) specifies the review, monitoring and assessment frequency of all National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 security and privacy controls to maintain the integrity and accuracy of the data.

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

System administration or AD records are maintained under the Departmental Records Schedule (DRS)-1.4, Short Term Information Technology Files, System Maintenance and Use Records (DAA-0048-2013-0001-0013), and System Planning, Design, and Documentation (DAA-0048-2013-0001-0014). These records include IT files that are necessary for day-to-day operations but no longer-term justification of the bureaus/office's activities. The disposition of these records is

temporary. Records covered under DAA0048-2013-0001-0013 have a temporary disposition and will be cut off when superseded or obsolete and destroyed no later than three years after cut-off. Records covered under DAA-0048-2013-0001-0014 have a temporary disposition and will be cut off when superseded by a newer version or upon termination of the system and destroyed three years after cut-off.

Retention periods vary depending on the user created or manage contents and purpose of the program records. Records created by individual users are retained and disposed of in accordance with applicable Departmental and bureau/office records schedules, or General Records Schedule (GRS) approved by the National Archives and Records Administration (NARA) for each type of record based on the subject or function and records series. However, the Bureau has a number of litigation holds in place which may require the retention of these records past the cut-off date.

NPS records are retained in accordance with the National Park Service Records Retention Schedule which has been approved by NARA (Job No. N1-79-08-01/09) and the DRS for Administration (DRS 1) and Policy (DRS 3). Please see the PIA for the hosted applications and systems for the applicable retentions schedule for the data collected by these applications and systems.

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

The NPS Account Management Procedures specify the procedures and disposition of data collected for Cloud Hosting I accounts. The NPS Exit Clearance process documents the steps and procedures used to remove information when employees and contractors leave the bureau. The records management policies and procedures also govern disposal of information. Procedures for disposition of the data stored in individual applications will vary by program office and needs of the agency. Due to the nature of Cloud Hosting I as a hosting service facility, there may be numerous records schedules with different dispositions applicable to the records created and maintained by users. It is the responsibility of each program office and user that creates or maintains Federal records to maintain and dispose of the records in accordance with the appropriate records schedule and disposition authority that covers their program area. Approved disposition methods for records include shredding or pulping paper records and erasing or degaussing electronic records in accordance with Departmental policy and NARA guidelines.

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.

There is a risk to the privacy of the individuals associated with Cloud Hosting I and the hosted applications that reside in the Cloud Hosting I due to the volume of sensitive PII that may be maintained. Cloud Hosting I is categorized as a Federal Information Security Modernization Act (FISMA) moderate system; however, multiple controls have been implemented to mitigate and substantially lower privacy risks. 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.

Cloud Hosting I allows the user community to access a number of services which may contain PII. Cloud Hosting I is not designed or characterized to support the collection, use, maintenance, or dissemination of PII other than that found in AD. Risk is mitigated by implementing the access controls outlined in the NIST SP 800-53 guidance. Privacy risk to Cloud Hosting I accounts would affect usernames, passwords and security questions and answers. These risks are mitigated by a combination of administrative, physical, and technical controls. Cloud Hosting I has a Moderate system security categorization in accordance with NIST standards and Federal Information Processing Standard (FIPS) 199, and FISMA.

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 SSPP. Risk is also mitigated through system configuration controls that limit or prevent access to privacy information. The Cloud Hosting I SSPP describes appropriate security and privacy controls implemented to safeguard Cloud Hosting I information collection, use, retention, processing, disclosure, destruction, transmittal, storage, and audit logging. It covers access controls, password management, firewalls, segregation of duties, and encryption of database, media, and communications. The SSPP documents the principle of least privilege access for authorized users to perform duties. Federal government information is managed and safeguarded by following NIST, FISMA and DOI security and privacy policies. All access is controlled by authentication methods to validate the authorized user. All DOI employees and contractors are required to complete annual security and privacy awareness training and sign DOI Rules of Behavior. Personnel authorized to manage, use, or operate the system information are required to take additional role-based training annually. For the applications hosted by Cloud Hosting I, the data is under the control of each program official or system owner who is responsible for protecting the privacy rights of the individuals whose information they collect, maintain, and use in each system, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as processing complaints, in consultation with privacy officials.

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. 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 for unauthorized purposes or disseminated by personnel authorized to access the system or view records. The system uses DOI SIEM tools and 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 AD, authentication results, and activity report and audit log content.

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 risk that individuals providing information do not have adequate notice on how their PII will be collected or used, or how to seek access to or correction of their records. This risk is mitigated by the publication of this PIA, the PIA for the hosted applications and systems, applicable SORNs that outline the authority, purpose, and uses of information and how individuals can submit requests under the Privacy Act, and Privacy Act statements provided during the onboarding process or during account creation and activation process. The DOI Privacy Program website also contains DOI and NPS privacy officials' contact information and provides guidance to individuals on how to submit requests or complaints under the Privacy Act.

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

The data is relevant and necessary to provide cloud hosting services to enhance productivity and security for the information stored, processed, and managed by applications and system in support of NPS missions. Cloud Hosting I provides cloud hosting services for data collected and managed through the hosted applications and systems. Please see the applicable PIA for the hosted applications and systems for methods for ensuring data collected by these applications and systems is current.

☐ 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. Cloud Hosting I is not intended to be used in any manner that would allow the system to derive new data or create previously unavailable data.

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

Auditors or DOI assessment management group may access the system at least annually or as described in the ISCMP. Individual users will have access to their own data.

Cloud Hosting I provides cloud hosting services for multiple applications and systems. Please see the applicable PIA for the hosted applications and systems for access specific to these applications and systems.

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

Contractors, system administrators, and auditors are granted access in accordance with mission function. Cloud Hosting I uses the principle of least privilege access for authorized users to perform duties. Federal government information is managed and safeguarded by following FISMA, NIST guidelines, and DOI security and privacy policies.

Cloud Hosting I provides cloud hosting services for multiple applications and systems. Please see the applicable PIA for the hosted applications and systems for user access specific to these applications and systems.

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 Cloud Hosting I infrastructure and platforms, 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 Laws, 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 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

☒ No

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

☒ Yes

Cloud Hosting I employs software, networking, infrastructure, and platform component to establish an audit trail of creation, modification of username of the account that changed the record, and the date and time the record was changed. Logs are only accessed by authorized administrative/manager staff.

☐ No

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

Information collected is used to monitor user access (username) and activity (logins, record changes, deletions, additions, date and timestamp) for auditing purposes.

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

Access to Cloud Hosting I components is only provided to necessary authorized employees and is applied on the principle of least privilege to manage access and audit logs. Audit features track user activity and record all changes.

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

(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

(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

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 Deputy Associate Director of Information Resources serves as the Cloud Hosting I System Owner is the official responsible for oversight and management of the security and privacy controls and the protection of the information processed and stored in Cloud Hosting I. The System Owner and NPS APO 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 Cloud Hosting I, in consultation with NPS and DOI Privacy Officials.

For hosted systems, the system owner responsible for oversight and management of the security and privacy controls and the protection of the information processed and stored by and for their respective system(s). These system owners also work with the NPS APO to address privacy

rights and complaints and ensure adequate safeguards for their respective system(s). The applicable system owner is identified in the respective PIA for the system(s).

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 Cloud Hosting I System Owner and Cloud Hosting I 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 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 APO.

For hosted systems, the system owner and information system security officer are responsible for daily operational oversight and management of the security and privacy controls and proper access management for their respective system(s). These system owners are also responsible for reporting to DOI-CIRC and coordinating with the NPS APO and other NPS and DOI officials. The applicable system owner and information security officer are identified in the respective PIA for the system(s).

System administrators and contractors are required to report any potential loss or compromise of Cloud Hosting I or any hosted system to the applicable System Owner, Information System Security Officer and NPS APO.