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: One General Services System (OneGSS)
Bureau/Office: National Park Service, Information Resources Management Directorate
Date: September 28, 2021
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) OneGSS is the wide area network (WAN) that provides an interconnecting backbone to support a number of business-related and mission-related applications used by the NPS. OneGSS is managed by the NPS Information Resources Management Directorate, and supports the NPS employee, contractor and volunteer community across all NPS regions, programs, and park units. OneGSS includes servers, workstations, networking devices (routers, firewalls, switches, and intrusion detection systems), storage devices, backup devices, and print devices. OneGSS provides several services to the user community to enhance productivity and provide security for the information stored, processed, and transported over the WAN. OneGSS services include malware protection, Voice Over IP (VOIP) services, systems management services, backup processes, Active Directory and group policy structures, and vulnerability scanning services.

OneGSS Active Directory (AD) account information for user access authenticates to the Enterprise AD, which is assessed separately in the Enterprise Hosted Infrastructure privacy impact assessment viewable at https://www.doi.gov/privacy/pia. OneGSS does not specifically contain personally identifiable information (PII) however the user community accesses a number of services which may contain PII that are connected to OneGSS. It is the responsibility of the application, office or individual using OneGSS services to protect the information collected, used, maintained, or disseminated on OneGSS. These services include office automation software such as Microsoft Office, Adobe products, BisonConnect (Microsoft 365 for Government) and Geographical Information System and other products that provide access to the Department of the Interior's (DOI) applications which support Human Resource, Payroll, Finance, Personnel Security, and other functions for NPS.

OneGSS provides 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, 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. There is a potential that large amounts of PII may be included in the documents stored. Each user/office program utilizing these OneGSS infrastructure is responsible for ensuring proper use of OneGSS and for meeting privacy and security requirements within their organization.

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: 010-000002651, NPS General Support 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			

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

☒ Yes:

Government personnel records are covered by OPM/GOVT-1, Government Personnel Records, 77 FR 79694, December 11, 2012, modified 80 FR 74815, November 30, 2015.

Active Directory records are covered by DOI-47, Logical Security Files, 72 FR 11040, March 12, 2007. Other program and user activities that may be subject to the Privacy Act are covered by various government-wide, Department-wide and NPS SORNs which are found at https://www.doi.gov/privacy/sorn.

☐ No

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

☐ Yes: *Describe*
☒ No

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
☒ 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
☒ Race/Ethnicity

☒ Other:

All these types of PII could potentially be included by users of the OneGSS. OneGSS contains username, work email address, work phone number, work address, title of DOI employee and contractor, and related organizational information required for system administration. Users may store all types of 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 on drives within the OneGSS domain. There is a potential that large amounts of PII may be included in the 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. Forms may collect various types of PII or information on user behaviors. Form owners are also responsible for implementing access controls and working with their bureau APO to ensure appropriate authority for the collection, privacy notice is provided, and privacy risks are addressed.

OneGSS provides hosting infrastructure services to applications and systems within the OneGSS environment. Please see the applicable privacy impact assessments (PIAs) for the hosted applications and systems for the types of PII and an evaluation of the privacy risks.

OneGSS uses DOI AD information (e.g., username, password, business contact information, security question answers, user principal name, 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 OneGSS.

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*

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

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

DOI AD/Enterprise Services Network provides information and services for the purpose of authenticating users and managing access. Initial information is collected by Human Resources (HR) or the Contracting Officer Representative (COR) from individuals during the on-boarding process to establish user accounts. As part of this process, the individual is instructed to complete the required security, privacy and records training and document it in the DOI Learning Management System (LMS); subsequently, this is an annual requirement. Upon completion of the training, the individual forwards a copy of the Certificate of Completion to update the completion field(s) in the LMS. HR or the COR then creates a request which notifies the AD team to create the network account(s) for OneGSS. This information is managed in DOI AD and is not collected by OneGSS.

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

The primary use of PII is to establish and manage user accounts to enable and maintain authorized access to the OneGSS to accomplish the business-related and mission-related applications used by NPS. After establishment of user accounts with username and password, users are required to use PIV credentials to access the OneGSS and DOI network resources. The information is also used to specify a username, user account and temporary password which the user is prompted to change at first use. The security questions and answers authenticate user identity for password reset requests.

Access to OneGSS includes a number of services to the user community to enhance productivity and provide security for the information stored, processed, and transported over the network

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

☒ Within the Bureau/Office
Information may be shared with NPS information resources, human resources, contract management staff or other management staff on a need to know basis. The primary use of PII is to enable and maintain authorized access to OneGSS to accomplish the business-related and mission-related applications used by NPS. Initially, the information is used to specify a username, user account and temporary password which the user is prompted to change at first use. The security questions and answers authenticate user identity for password reset requests.

Access to OneGSS includes a number of services to the user community to enhance productivity and provide security for the information stored, processed, and transported over the network.

☒ Other Bureaus/Offices

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

☐ Other Federal Agencies

☐ Tribal, State or Local Agencies

☒ Contractor
NPS may contract with other commercial organizations to provide configuration, operations, and maintenance of OneGSS or specific network components. 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. OneGSS undergoes continuous monitoring by security staff to identify security vulnerabilities.

☐ Other Third Party Sources

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

☒ Yes
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 COR 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
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
Users can also view how their information will be used in the OneGSS Privacy Impact Assessment, and the DOI-47 Logical Security Files, OPM/GOVT-1, Government Personnel Records, 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.).

Service Desk personnel can retrieve a user's account by their name or username within OneGSS. 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

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 OneGSS. OneGSS administrators have access to these reports.

☐ No

Section 3. Attributes of System Data

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

Data is not collected from other sources. The user can only access the OneGSS system as a valid, authorized Active Directory user with current and accurate credentials, an active PIV card, and a valid OneGSS user account.

B. How will data be checked for completeness?

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).

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)-4.1, 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/offices 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 Schedule, Resource Management and Lands (Item 1), which has been approved by NARA (Job No. N1-79-08-01/09). The disposition of OneGSS records is temporary, destroy/delete 3 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?

The NPS Account Management Procedures specify the procedures and disposition of data collected for OneGSS 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 OneGSS as a GSS, 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 moderate risk to individuals associated with OneGSS and the hosted applications that reside on the OneGSS due to the volume of sensitive PII that may be maintained. OneGSS is categorized as a moderate risk 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.

OneGSS allows the user community to access a number of services which may contain PII. OneGSS is not designed or characterized to support the collection, use, maintenance or dissemination of PII other than that found in AD. There is minimal risk to the privacy of official user information throughout the information lifecycle; user information is authenticated by AD for access to OneGSS. Risk is further reduced by following established guidance from NIST SP 800-53 on access controls. Privacy risk to OneGSS network accounts would affect usernames, passwords and security questions and answers. These risks are mitigated by a combination of administrative, physical and technical controls. OneGSS has a Moderate system security categorization in accordance with NIST standards and Federal Information Processing Standard (FIPS) 199, and the Federal Information Security Modernization Act (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 System Security and Privacy Plan. Risk is also mitigated through system configuration controls that limit or prevent access to privacy information. The OneGSS System Security and Privacy Plan (SSPP) describes appropriate security and privacy controls implemented to safeguard OneGSS 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 OneGSS, 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 or disseminated by personnel authorized to access the system or view records. The system uses audit logs to protect against unauthorized access, changes or use of data. Federal employees and contractors are required to take annual mandated security, privacy, and records management as well as role-based training where applicable and sign the NPS Rules of Behavior prior to accessing the system. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, criminal, civil, and administrative penalties.

There is a risk that erroneous information may be collected. This risk is mitigated by allowing individuals to access and update only their records in the system. For DOI user accounts, this risk is further mitigated by validating information against DOI Active Directory, authentication results, and activity report and audit log content.

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, 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
Data collected is required to provide services to enhance productivity and security for the information stored, processed, and transported over the WAN in support of NPS missions.

☐ 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. OneGSS 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: *Describe*

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.

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. OneGSS 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.

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, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations.

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

OneGSS includes routers, firewalls, and software 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 time-stamp) for auditing purposes.

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

Access to OneGSS 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. *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 Deputy Associate Director of Information Resources serves as the OneGSS 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 OneGSS. The System Owner and System Privacy 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 OneGSS, 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 OneGSS System Owner and OneGSS System Security and Privacy 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, System Security and Privacy 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 System Owner, System Security Officer and System Privacy Officer.