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: Office of the Chief Information Officer (OCIO) Local Area Network (LAN) System
Bureau/Office: Office of the Chief Information Officer
Date: June 7, 2022
Point of Contact
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: DOI_Privacy@ios.doi.gov
Phone: (202) 208-1605
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

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

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

B. What is the purpose of the system?

The purpose of the OCIO LAN is to provide local area network, local file and print server, and endpoint management support for Office of the Secretary (OS), Interior Business Center (IBC), Office of the Solicitor (SOL) and Office of Hearings and Appeals (OHA) staff at both core and remote locations. Core locations include Washington DC, Reston VA, Herndon, VA, Arlington, VA, Denver CO, and Boise ID. The OCIO LAN Assessment & Authorization (A&A) supports

operations for the Main Interior Building (MIB), John J Powell Building in Reston, VA, Atrium Building in Herndon, VA, OHA Arlington Headquarters Office, OCIO/IBC Mansfield Campus in Denver, and OS Offices in Boise, ID. The OCIO LAN provides connectivity to electronic messaging systems, the Internet, and the OCIO Data Centers for access to DOI information system resources and applications.

OCIO LAN consists of workstations, local file storage and print devices. OCIO LAN does not collect and maintain sensitive PII. However, users may store PII on the file shares located in their local file storage. Access to OCIO LAN is controlled by DOI's Active Directory (AD) user accounts and group membership managed and provisioned through the Enterprise Hosting Infrastructure/Enterprise Directory Services.

C. What is the legal authority?

5 U.S.C. 301, Department Regulations; 44 U.S.C. Chapter 35, Paperwork Reduction Act; and 40 U.S.C. 1401, Clinger-Cohen Act of 1996.

D. Why is this PIA being completed or modified?

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

E. Is this information system registered in CSAM?

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

UII code: 010-000000340; OCIO LAN 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	None	No	N/A

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

☐ Yes: *List Privacy Act SORN Identifier(s)*
☒ No

OCIO LAN is not a Privacy Act system of records. It does not collect or use personally identifiable information (PII) to directly retrieve records on individuals. OCIO LAN provides local area network, local file and print server, and endpoint management support which consists of workstations, local file storage, and print devices. The PII maintained in the file storage or workstations that OCIO LAN supports are covered by applicable published Government-wide, DOI-wide or DOI bureau/office system of records notices (SORNs). These SORNs may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn.

PIV credentials required to access OCIO LAN and the DOI network are covered under 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).

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
☒ Other: *Specify the PII collected.*

OCIO LAN was not designed to collect PII, however, users may store PII on their file shares. Name, username, workstation name, and AD group information are collected to provide support to users. Access to this system is limited to System Administrators through the use of their PIV credentials.

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*

PIV credentials of System Administrators are used for verification and authentication to access OCIO LAN. OCIO LAN was not designed to collect PII, however, users may store PII on their file shares.

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*

System Administrator's access to OCIO LAN requires authentication through a DOI issued PIV card or network username and password. Access to OCIO LAN is controlled by AD user accounts and group membership managed and provisioned through the Enterprise Hosting Infrastructure/Enterprise Directory Services. OCIO LAN was not designed to collect PII, however, users may store PII on their file shares.

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

OCIO LAN provides local area network, local file and print server, and endpoint management and support for OS, IBC, SOL, and OHA. OCIO LAN was not designed to collect PII, however, users may store PII on their file shares in the performance of their official duties. Limited PII is used to identify authorized users, manage access, and provide support to users.

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

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

OCIO LAN was not designed to collect or share PII, however, PII may be used or shared internally to provide access and support to users. OCIO LAN supports users who may store PII on their file shares. Individual users may share PII with authorized users in the performance of their official duties

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

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

PII may be shared with federal law enforcement organizations for security and investigation purposes.

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

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

Information may be shared with contractors who perform services or support DOI activities related to the OCIO LAN. PII may be shared with contractors supporting DOI to perform system maintenance services.

☐ 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?

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

Information is voluntarily provided by employees in order to obtain access to the DOI network and information systems. Users have the opportunity to consent during the onboarding process and verification of approval to work is required to enforce access controls across the DOI network. If users decline to provide the required information upon employment at DOI, they will not be given access to the government-furnished equipment (GFE) and the network, and may be unable to perform their duties. OCIO LAN was not designed to collect PII, however, users may store PII on their file shares.

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

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

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

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through the publication of this PIA. Users may view the INTERIOR/DOI-47 SORN for use of logical access records on the DOI SORN website at https://www.doi.gov/privacy/sorn.

☒ Other: *Describe each applicable format.*

All of the platforms on the OCIO LAN display a pre-login warning banner that complies with DOI and NIST requirements within the technical capabilities of each platform. Commercial off-the-shelf products installed on workstations also display the pre-login warning banner.

☐ None

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

Files stored on individual workstations or file shares may be searched by file name attributes and keywords. If required, OCIO LAN has the ability to search for unique identifiers leveraging OCIO search tools. Retrieval occurs when resetting passwords, to change permissions, transfer or move accounts, and add/remove workstations or applications that reside on the system using AD data such as name, username, workstation name, and AD group.

I. Will reports be produced on individuals?

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

OCIO LAN may produce audit logs or reports on user activity in accordance with DOI logging requirements. The logged information is used to ensure the security of the system and for investigative actions associated with cyber security incidents.

☐ No

Section 3. Attributes of System Data

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

OCIO LAN data is collected from DOI records, which is obtained from employees as part of the AD process to gain network access. AD processes include supervisor review to ensure employee data is accurate. The OCIO LAN is subject to appropriate information security and privacy controls. These controls will ensure that any sensitive information stored in the file shares or workstations are protected from any undue risk of loss or alteration.

B. How will data be checked for completeness?

The OCIO LAN and all data entered into the systems hosted on the OCIO LAN is subject to appropriate information security and privacy controls. These controls will ensure that sensitive information is protected from any undue risk of loss or alteration. OCIO LAN uses AD, which requires supervisor review to ensure employee data is complete.

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

The OCIO LAN and all data entered into the systems hosted on the OCIO LAN is subject to appropriate information security and privacy controls. These controls will ensure that sensitive information is protected from any undue risk of loss or alteration. OCIO LAN uses AD, which has processes to ensure employee data remains current.

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

Records and data maintained in OCIO LAN are retained in accordance with the Departmental Records Schedule (DRS) - Administrative schedule 1.4.1 – [0013] Short Term IT Records – System Maintenance and Use, approved by the National Archives and Records Administration (NARA). These records include IT files that are not needed for extended retention and necessary for day-to-day operations. Disposition is temporary, the cutoff varies depending on the hosted system and types of records. Destroy no later than 3 years after cut-off.

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

DOI approved disposition of paper records includes shredding, and electronic records are degaussed in accordance with NARA guidelines and DOI policy.

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 individuals due to the use of user accounts to access OCIO LAN. Only limited PII is used to manage user access to ensure the security of the system. There is an additional risk from users storing PII on their personal file shares. All users are subject to Federal law, regulation, and DOI policy to safeguard PII. It is the individual filer's responsibility to follow policy, protect PII, and ensure PII is not inappropriately stored on their personal file share.

There is a risk that PII stored employee laptops or workstations may be accessed by unauthorized persons. Full disk encryption is enabled on all DOI issued devices to protect data at rest. OCIO employees complete training on using their GFE for official business only and to avoid storing their personal information on devices. DOI employees must lock their GFE when unattended in a secure environment and follow DOIs incident reporting procedures in the event of a lost or stolen

device. DOI users are also encouraged to rely on the Department's Microsoft O365 Cloud storage solution for official business. OCIO LAN has undergone a formal Assessment and Authorization and has been granted an authority to operate in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and National Institute of Standards and Technology (NIST) guidelines. OCIO LAN is rated as a FISMA moderate system, which requires strict privacy and security controls to ensure the confidentiality, integrity, and availability of the data in the system.

There is a risk of unauthorized disclosure or that PII may be misused or used for unauthorized purposes. OCIO LAN limits access to only those persons authorized to use the servers and ensures that they can access only resources for which they have authorization. OCIO authorized personnel sign the DOI Rules of Behavior (ROB) and are subject to monitoring in the system and DOI network. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, and criminal, civil, and administrative penalties. DOI employees must complete Information and Management Technology awareness training which includes privacy, cybersecurity, records management, Controlled Unclassified Information (CUI), Section 508, and the Paperwork Reduction Act, and the DOI ROB prior to being granted access to DOI information and information systems, and annually thereafter. Personnel with significant privacy responsibilities, such as law enforcement personnel, must also take role-based privacy training initially and annually, to ensure an understanding of the responsibility to protect privacy.

There is a risk that data on OCIO LAN will be maintained for longer than necessary to support the Department's mission, or that records may not be properly destroyed. This risk is mitigated by managing records in accordance with a NARA-approved records schedule and providing extensive training to users on IT security, Privacy, Records Management and CUI.

There is a risk of inadequate notice for individuals. Notice is provided to users through the publication of this PIA and the DOI-47 SORN and other applicable SORNs that cover PII may reside on the file shares. Users are also provided notice of security monitoring in the warning banner and ROB.

Section 4. PIA Risk Review

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

☒ Yes: *Explanation*

The purpose of the information system is to provide file share services to users to facilitate daily mission and duties.

☐ No

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

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

☒ No

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

☐ Yes: *Explanation*
☒ No

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

☐ Yes: *Explanation*
☒ No

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

Not Applicable. OCIO LAN does not derive new data or create previously unavailable data.

F. Are the data or the processes being consolidated?

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

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

☒ No, data or processes are not being consolidated.

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

☒ Users
☒ Contractors
☐ Developers
☒ System Administrator
☒ Other: *Describe*
The system administrators and the contractors working in the system in an administrative capacity can access the OCIO LAN.

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

OCIO LAN file share system access is based on the least privilege principle, role-based approach for user account authorization and access enforcement. Individuals can only access their own file share. Privilege account holders supporting OCIO LAN are reviewed, authorized, and approved by the System Owner.

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

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

Contractors are involved with the design, development, or maintenance of OCIO LAN. The appropriate contract clauses will be included in the contract.

☐ No

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

☐ Yes. *Explanation*

☒ No

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

☒ Yes. *Explanation*

OCIO LAN uses audit logs which monitor user activities for security purposes.

☐ No

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

All OCIO LAN devices are configured to provide audit warnings, errors, or failures. Audit settings enabled include directory service access, logon events, object access, privilege use, system events, and account management and can be reviewed by designated administrators. OCIO periodically reviews and updates the list of auditable events for the OCIO LAN platforms. OCIO LAN user activity is monitored which includes name, username, logon date, number of failed logon attempts, etc.

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

System administrators can monitor user activity, which requires proper authorization by System Owner. Additionally, infrastructure logs related to privileged functions, administrator activity, authentication and authorization checks, permission changes, data changes and deletions are automatically monitored and analyzed to detect suspicious activity and indicators of inappropriate or unusual activity.

Users must consent to DOI Rules of Behavior and complete Federal Information System Security Awareness, Privacy Awareness and Records Management training, and any required role-based training before being granted access to the DOI network or any DOI system, and annually thereafter.

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*

The physical controls are inherited from Local sites where the users are located. The system inherits those controls which are in compliance with NIST SP 800-53.

(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 Chief, End User Services Branch, Office of the Chief Information Officer serves as the Information System Owner and the official responsible for oversight and management of the OCIO LAN security and privacy controls and the protection of OCIO LAN data processed and stored within the system. The OCIO LAN System Owner and Information System Systems Security Officer (ISSO) are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored. The System Owner is also responsible for addressing any Privacy Act requests for notification, access, amendment, and complaints in consultation with 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 OCIO LAN System Owner is responsible for the daily operational oversight and management of the OCIO LAN security and privacy controls, for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The OCIO LAN System Owner and authorized users are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC, DOI's incident reporting portal, within 1-hour of discovery in accordance with Federal policy and established DOI procedures, and for working with the Departmental Privacy Officer to ensure appropriate remedial activities are taken to mitigate any impact to individuals.