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: DOI Azure General Support System (GSS)
Bureau/Office: Office of the Chief Information Officer
Date: October 2, 2023
Point of Contact
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: Teri_Barnett@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?

DOI Azure General Support System (GSS) is an enterprise-wide cloud-based Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) that is managed by the Enterprise Services Division (ESD), Office of the Chief Information Officer (OCIO). The DOI Azure GSS provides access control and user authentication for various Department of the Interior (DOI) applications,

including the Microsoft Office O365 suite of applications. The DOI Azure GSS enables bureaus and offices to quickly build, test, deploy, and manage their applications and services to support their mission and business needs.

DOI Azure GSS consists of a core component, Microsoft Azure Active Directory, which serves as the Department's identity management and authentication system. Microsoft Azure Active Directory is a FedRAMP-approved cloud service provider and is regularly reviewed to ensure that all applicable security controls are in place. Similar to DOI's on-premise (on-prem) Enterprise Hosted Infrastructure (EHI) boundary that hosts the Enterprise Directory Services (EDS), DOI Microsoft Azure Active Directory provides cloud-based authentication, security, domain name services (DNS), and synchronization services for the Department and bureaus and offices utilizing Microsoft Azure Active Directory services.

The personally identifiable information (PII) collected in the DOI Azure GSS is used in the creation and administration of DOI user accounts to authenticate users and provide access to DOI information and systems and ensure the security of DOI assets. Most of the PII in the DOI Azure GSS resides in the DOI Microsoft Azure Active Directory and consists of username, work email address, work phone number, work address, and job title required for system administration purposes. This information is constantly synchronized through a one-way interface with the DOI AD credentials from EHI on-prem to the Microsoft Azure Active Directory Cloud.

At the request of a bureau/office supervisor, a DOI Azure System Administrator can create and send an invitation to create external user accounts in the DOI Microsoft Azure Active Directory portal for collaborative purposes. External guest user accounts will not be on the DOI domain, but will only receive access to approved and authorized specific shareable content, which they will access using their non-DOI external email that they provided. More details relating to this process can be found in the Microsoft O365 Cloud PIA on the DOI Privacy page. External users will provide first and last name, as well as official email address. These external user accounts provide access to individual Applications within DOI's Microsoft Azure, on an as-needed basis. All requests for external guest accounts in the DOI Microsoft Azure Active Directory will be received and approved by DOI IT services before provisioning. External user accounts are not temporary and exist until they are removed. Access restrictions are set for guest accounts allowing access to only the specific bureau/office resource within the DOI Microsoft Azure Active Directory. PII from DOI Azure GSS and Microsoft Azure Active Directory is shared with authorized OCIO personnel for account management purposes. However, PII may also be shared with DOI human resources (HR) staff or law enforcement organizations for investigations of potential insider threat, violations of law, regulations or policy, or any illegal activities.

The DOI Azure GSS has various logs, including Microsoft Azure Active Directory logs and audit and sign-in logs, which have internet protocol (IP) address information. The IP addresses are only accessible by authorized privileged users via an administrative dashboard. IP addresses only identify organizational demarcation and do not identify authorized users.

Hosted systems in DOI Azure GSS may collect PII. Systems hosted within DOI Azure GSS must obtain and maintain a separate authority to operate (ATO). In addition, privacy requirements of Bureau/Office customer developed applications hosted on DOI Azure GSS are not included within the DOI Azure GSS Privacy Impact Assessment (PIA). The scope of this PIA will cover PII collected within the DOI Azure GSS and Microsoft Azure Active Directory. Bureaus and offices are responsible for ensuring the applications and systems that use Microsoft Azure Active Directory for access meet the privacy requirements, including conducting a separate PIA to address any privacy risks for use of the system and implementing adequate controls to protect individual privacy.

C. What is the legal authority?

5 U.S.C. 301, Departmental Regulations; 44 U.S.C. Chapter 35, Paperwork Reduction Act; 40 U.S.C. 1401, Clinger-Cohen Act; 44 U.S.C. 3541 et seq., Federal Information Security Modernization Act of 2014; OMB Circular A-130, *Managing Information as a Strategic Resource*; Executive Order 13571, *Streamlining Service Delivery and Improving Customer Service*, April 11, 2011; Presidential Memorandum, *Security Authorization of Information Systems in Cloud Computing Environments*, December 8, 2011; and *Presidential Memorandum, Building a 21st Century Digital Government*, May 23, 2012.

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 the Governance, Risk, and Compliance platform?

☒ Yes:

UII Code: 010-000002539
System Security and Privacy Plan Name: DOI Azure 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.*
Microsoft Azure Active Directory	This system is used to authenticate DOI users and external guests for access to agency applications and information	Yes	Usernames and official contact information of the authorized user

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)*

- DOI Microsoft Azure Active Directory records 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)
- HSPD-12 PIV user account data is covered under GSA/GOVT-7, HSPD-12 USAccess, 80 FR 64416 (October 23, 2015)

The DOI Microsoft Azure Active Directory provides user authentication and access to numerous hosted applications or systems managed by DOI bureaus and offices, some of which may contain records subject to the Privacy Act of 1974 that may be covered under the applicable published Government-wide, DOI-wide or bureau/office SORNs.

DOI SORNs may be viewed on the DOI SORN website 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

☒ Personal Cell Telephone Number
☒ Personal Email Address
☒ Other: *Specify the PII collected.*

PII collected from the DOI Microsoft Azure Active Directory on employees is synced with Active Directory (AD) consisting of an employee's official contact information, including username, work email address, work phone number, work address, and job title for account management purposes. In some cases, employees may use personal phone number or email address as their work contact information. External users provide their name and official email address to create a guest user account.

The following PII data elements will be used to identify and authenticate user access and actions within DOI Azure GSS using AD: Username, password hash values, HSPD-12 authentication, official email address and phone number, duty station city and state, supervisor name, Personal Identity Verification (PIV) Certificate, User Principal Name (UPN), Supervisor email, Supervisor name, and Update date.

AD user account information includes names, passwords, and login time, data, and locality, which is used to authenticate user access and actions within DOI Microsoft Azure Active Directory. This information is constantly synchronized through interface with AD.

The DOI Azure GSS contains various logs, including Azure Active Directory logs and audit logs and sign-in logs, which have IP address information. These IP addresses are only accessible via an administrative dashboard by authorized privileged users. DOI Microsoft Azure Active Directory provides user access to numerous applications and systems, which may collect, use, process or store PII. DOI separately assessed the PII handling activities and addressed the identified privacy risks of theses individual systems and applications. Please see the PIAs for these individual systems and applications on the DOI PIA website at https://www.doi.gov/pia.

The data owners for the bureau/office systems and applications that are accessed by external users are responsible for working with their bureau/office Associate Privacy Officers (APOs) to identify the PII types collected, evaluate the privacy risks, and ensure DOI and Federal privacy requirements are met.

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*

Application Owners are responsible for data management of their site's content and for consulting with their bureau APO to identify privacy risks related to the data and site activities.

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

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

DOI Azure GSS uses Microsoft Azure Active Directory via the AD Federation Service (ADFS) to authenticate user accounts for access to all hosted applications. ADFS is an identity access solution that provides client computers with access to protected internet-facing applications or services. DOI Microsoft Azure Active Directory user data is provided by interface with the On-prem Active Directory from EHI, which is in a separate system boundary. Microsoft Azure Active Directory continuously updates data across the DOI domains for these hosted applications.

☒ Other: *Describe*

DOI Azure uses AD via ADFS to authenticate daily driver user accounts for all hosted applications. DOI Azure Active Directory user data is provided by interface with the "On-prem Active Directory (via Azure AD connect)," which is in a separate system boundary. DOI Microsoft Azure Active Directory continuously updates data across the DOI domains. The DOI Microsoft Azure Active Directory domain also has several cloud-only "guest" user accounts. However, these accounts are mostly created with an external, non-DOI email address. No additional details are required. The Microsoft Azure Active Directory system-administrator accounts are created to manage and monitor the system and these accounts are strictly controlled with proper approvals.

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

PII is used in the creation and administration of DOI user accounts to authenticate and manage user access to DOI information and systems and ensure the security of DOI assets. DOI Azure GSS provides access control and user authentication for DOI applications and other resources across the DOI environment using the provided information.

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.*

PII is shared with authorized ESD personnel for the creation and administration of DOI user accounts and to provide access control and user authentication for services, applications, and other resources across the DOI environment using the provided information.

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

User account information is replicated in all bureau/office locations and between bureau/office domain controllers for the purpose of access enforcement, which allows DOI users the ability to view or access hosted applications and other services.

PII may be shared with DOI HR staff or law enforcement organizations for referrals or investigations of potential insider threat, violations of law, regulations or policy, or any illegal activities.

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

Other Federal agencies do not have direct access to the DOI Azure GSS or any hosted applications. However, officials at other Federal agencies will have access to the information that is shared on Applications through an approved guest account as external users.

PII data may also be shared with federal law enforcement organizations for referral or investigation purposes when there is an indication of potential violation of law, regulation, or policy. Some information may be shared with other Federal agencies as authorized pursuant to the routine uses contained in the INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), GSA/GOVT-7, HSPD-12 USAccess, or other applicable SORNs. Please view SORNs on the DOI SORN website at https://www.doi.gov/privacy/sorn.

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

Tribal, state, or local agencies do not have direct access to the DOI Azure GSS or any hosted applications. Information may be shared with Tribal, state, or local agencies as authorized pursuant to the routine uses contained in the INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), GSA/GOVT-7, HSPD-12 USAccess, or other applicable SORNs.

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

Microsoft is a Cloud Service Provider (CSP) that will manage the DOI Azure GSS environment. Per contractual obligations, they have no authorization to review, audit, transmit, or store DOI data. Information may be shared with contractors who perform services or otherwise support DOI activities related to the DOI Azure GSS, and as authorized pursuant to the routine uses contained in the DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), GSA/GOVT-7, HSPD-12 USAccess, and other applicable SORNs.

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

Third party organizations do not have direct access to the DOI Azure GSS or any hosted applications. Data in hosted applications may be manually shared with other third parties as authorized and necessary to meet legal or mission requirements, or in the course of conducting official business.

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 network and may be unable to perform their duties.

External guest users voluntarily provide their name and email address when requesting access to DOI assets at the time of account creation. External guest users may decline to provide their information; however, a guest account will not be created, and they will not be given access to DOI assets if declined

☐ 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.*

New users are provided a Privacy Act statement during onboarding when they are issued PIV credentials. In some cases, users may request a new or updated account be created within the DOI domain through an automated form within the DOI Access system which contains a Privacy Act statement. DOI Access is the Department's user credentialing system for individuals who require access to DOI networks, information systems and regular facility access. Cloud-only "Guest" account users are provided a Privacy banner.

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through publication of this PIA and the DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), and GSA/GOVT-7, HSPD-12 USAccess, SORNs. DOI bureaus and offices may also provide notice through the publication of PIAs and SORNs associated with their hosted systems and applications as applicable.

☒ Other: *Describe each applicable format.*

A DOI Security Warning Banner is provided to DOI Azure GSS network users at the login screen and when accessing the DOI network that informs them they are accessing a DOI system, that they are subject to being monitored, and there is no expectation of privacy during use of the system.

☐ None

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

Data can be retrieved by employee or username, email, workstation name, and AD group. Data can be retrieved with these identifiers if the end user seeks to view their profile and update information, in instances when that is possible. In addition, these retrievers may be used to look up user identity for the focus point of logs.

I. Will reports be produced on individuals?

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

Audit logs are collected by Azure GSS and contain details relating to the use of the platform, including username, application being accessed, IP address, and account name. Audit logs are accessible by system administrators and are used for security protocols or system requirements.

☐ No

Section 3. Attributes of System Data

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

Data is collected from DOI records and user provided information and is not collected from other sources. Hosted systems in DOI Azure GSS may collect PII. However, the scope of this PIA is limited to PII within DOI Azure GSS, Microsoft Azure Active Directory and the limited PII for privileged account holders for system administration purposes. Any bureau/office hosted systems on the DOI Azure GSS must complete and maintain a separate PIA and ATO as required to meet Departmental and Federal legal and policy requirements. Information to create an external user guest account is obtained directly from the guest user by the responsible official and is deemed accurate at the time it is provided by the user.

B. How will data be checked for completeness?

Users must provide complete information during the onboarding process to establish user accounts in DOI Access and AD. Specific account attributes within the DOI Azure GSS can be updated upon the user's request, which generally includes contact information. The specific user information that is used to create AD user accounts is obtained from DOI Access and cannot be changed. As a function of AD, all data related to user access is continuously synchronized across the entire system and DOI Microsoft Azure Active Directory. Information to create an external user guest account is obtained directly from the guest user by the responsible official and is deemed complete at the time it is provided by the user.

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

Certain updates may take effect via the AD system updates, however; it is up to the individual to update their contact information and update data in any application and/or system that is hosted within the DOI Azure GSS. DOI provides the My Account (https://myaccount.doi.gov) internal site where users can maintain and update their work-related contact information. Users are notified that it is their responsibility to ensure their information is up to date. Individuals may also request access to or amendment of their records by following the procedures outlined in the applicable SORNs. As a function of AD, all data related to user access is continuously synchronized across the entire system and DOI Microsoft Azure Active Directory. Guest accounts generally do not require any data other than the external email. Information to create an external user guest account is obtained directly from the guest user by the responsible official and is deemed current when provided by the user.

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), which has been approved by the National Archives and Records Administration (NARA). The disposition is temporary. Records are cut off when the employee's access has been removed, either because the employee separated, retired, or transferred, or if the user's access is completely changed. In general, Records are destroyed 3 years after cut-off. These records encompass IT files described that are not needed for extended retention. Records are characterized by being necessary for day-to-day operations but no longer-term justification of the bureaus/office's activities. DOI Microsoft Azure Active Directory audit logs contain information relating to system changes, with data elements that include date, service category, status, where the request initiated from, and target information focusing on where the request originated from. This audit log information is stored for 7 days within the Azure Event Hubs and is then exported to Splunk and Cybersecurity and Infrastructure Security Agency's (CISA) Cloud Log Aggregation Warehouse (CLAW) for long term retention, which is 3 years as per CISA's CLAW Information Sharing Agreement. At the expiration of the retention times the audit data is

automatically purged by the system that retains them. As a function of AD, all data related to user access is continuously synchronized across the entire system including DOI Microsoft Azure Active Directory. Therefore, active accounts are retained within the system and the associated records will be retained for the time periods described above when user accounts are deactivated or terminated.

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

Once user accounts are terminated in the system, the records are removed in accordance with the DRS and other applicable bureau/office records retention schedules and destruction policy. Procedures for disposition of the data stored in individual applications will vary by application. Data retention/disposition policies in the hosted application(s) is out-of-scope for this PIA.

The DOI Azure GSS user objects can be set to automatically expire at a given date to ensure that a user does not have access past the period of performance or contract. When the account is disabled, all access to the network and all DOI Azure GSS systems are explicitly denied and all attempts to gain access are logged.

Before purging accounts from the system, a report including the name, termination date, and a completed DI-1941, Documentation of Temporary Records Destruction form must be provided to the OS Records Office (or the bureau Records Officer) before the data is purged.

Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and Departmental 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 privacy risk to individuals due to the information contained in and used by the system, which is mitigated by controls implemented to protect data. PII used to authenticate users is limited to employee name, username, work email address, work phone number, duty station address, and official title of DOI employees and contractors. Work related PII, such as contact information, duty station, and title, is generally not considered sensitive. There is an increased risk for the management of system administrator accounts, which include username, password, and elevated privileges. System permissions and access controls are in place to limit system access to only those authorized individuals with a need to know the information to perform official functions. External guest users PII is limited to first name, last name, and official email address.

There is a risk that PII data is collected and stored on a cloud system. Microsoft Azure is a FedRAMP approved cloud service provider and regularly undergoes reviews to ensure that all security controls are in place and operating as intended. DOI Azure GSS provides an enterprise-

wide cloud-based PaaS and IaaS for the Department and bureaus and offices utilizing Microsoft Azure Active Directory services. DOI Azure GSS is rated as a moderate system in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) based upon the type and sensitivity of data and requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive data contained in the system. Prior to granting users access to the DOI network, all users must agree to the DOI Rules of Behavior, as well as the DOI Warning Banner before accessing the system, which includes the consent to monitoring and restrictions on data usage. DOI bureaus and offices with hosted applications may also implement additional controls to protect privacy and DOI information assets.

DOI's user identity management processes include authentication with AD to control and manage access restrictions to authorized personnel on an official need-to-know basis. System administrators utilize user identification, passwords, least privileges, and audit logs to ensure appropriate permissions and access levels. The contract between DOI and Azure does not allow the service provider to review, audit, transmit, or store DOI data, which minimizes privacy risks from the vendor source. All DOI employees and contractors must complete privacy, security and records management awareness training, as well as role-based training where applicable, on an annual basis and sign the DOI Rules of Behavior prior to accessing the system.

The Department utilizes a combination of technical and operational controls to reduce risk in the DOI Azure GSS environment, such as firewalls, encryption, audit logs, least privileges, malware identification, and data loss prevention policies. All DOI employees must have a DOI account and government issued PIV card to access DOI Azure GSS.

As part of the continuous monitoring program, continual auditing will occur on the system to identify and respond to potential impacts to PII information stored within the DOI Azure GSS environment, which will help the agency effectively maintain a good privacy and security posture for the system. The system security and privacy plan will be reviewed annually to ensure adequacy of controls implemented to protect data.

There is a risk that data in the Microsoft Azure Active Directory may be inaccurate. As a function of AD, all data related to user access is continuously synchronized across the entire system and Microsoft Azure Active Directory. In addition, users provide their information at the time of account creation, to confirm accuracy of information and can update any information as appropriate to ensure ongoing accuracy.

There is a risk that data may be inappropriately disclosed, accessed, or used for unauthorized purposes. Access to administrative functions is strictly controlled and can only be granted by Azure Enterprise Managers. DOI complies with the National Institute of Standards and Technology (NIST) and other Federal requirements for data security as part of a formal program of assessment and authorization, and continuous monitoring. All information collected/contained on systems, is only accessible to special privileged administrators and the data is encrypted on the system drives. Scheduled scans of the network are performed to ensure that changes do not occur that would create an exposure or weakness in the security configuration of any Azure equipment. The use of DOI IT systems, including Azure, is conducted in accordance with the

appropriate DOI use policy. IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system are reported immediately to IT Security. PII from DOI Azure GSS and Microsoft Azure Active Directory is shared with authorized DOI personnel for account management purposes. PII may also be shared with DOI HR staff or law enforcement organizations for referrals or investigations of potential insider threat, inappropriate access or use, violations of law, regulations or policy, or any illegal activities.

There is a risk that information in applications may be shared with external users, that guest user accounts will not be properly granted, maintained, or deleted, or that guests will have access to more information than necessary or authorized for an official purpose. These external user accounts are temporary and provide limited access to individual applications within DOI's Microsoft Azure on an as-needed basis for the purpose of conducting Department and/or Bureau mission needs. Guest accounts are given access only to specific functions and applications within the DOI applications. Bureaus and offices utilizing the Azure services are responsible for implementing adequate controls to safeguard PII used or maintained within their environment as appropriate and for managing guest accounts in a secure and auditable manner. Bureaus and offices are informed of their responsibilities.... All requests for external guest accounts in the DOI Microsoft Azure Active Directory must be approved before provisioning. Access restrictions are set for guest accounts allowing access to only the specific bureau/office resource within the DOI Microsoft Azure Active Directory. External users or organizations will have access to the information that is shared in applications through the approved guest account but will not have direct access to the DOI Azure GSS or any non-shared hosted applications. The data owners for the bureau/office applications that are accessed by external users are responsible for working with their APOs to identify the PII types collected, assess the privacy risks, and ensure DOI and Federal privacy requirements are met.

There is a risk that data may be stored longer than necessary. Only the minimal amount of data needed to authenticate users and manage system access is collected or used, and the records are maintained and disposed of under a NARA-approved records schedule. Information collected and stored within DOI Azure is maintained, protected, and destroyed in compliance with NARA and all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

There is a risk that individuals may not receive adequate notice of DOI privacy practices or the extent of the use of their PII data. Notice is provided to individuals through the publication of this PIA and the SORNs for DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) and GSA/GOVT-7, HSPD-12 USAccess, as well as any additional PIAs and SORNs published for hosted bureau and office systems. DOI employees are also provided privacy notice during the onboarding process and must read and acknowledge the Privacy Act Statement provided in DOIAccess, which is the Department's user credentialing system for individuals who require access to DOI networks, information systems and regular facility access.

Authorized external guest users are provided notice at the time of external guest account creation through a Privacy banner. Individuals may update their contact information at any time following established procedures within their organizations and may request access to or amendment of their records by following the procedures outlined in the applicable SORNs.

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*

Data is required for the purposes of hosting any applications on the DOI Azure GSS and providing access to these applications through Microsoft Azure Active Directory to facilitate the work across the Department while meeting the agency's mission and maintaining the appropriate level of security to protect privacy and the DOI network and information assets. Also, DOI Azure GSS provides access to infrastructure portal and allows system administrators to monitor and update attributes to provide optimal services with the appropriate level of security.

☐ 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 since DOI Azure GSS does not generate new 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.*

Data gathered from bureaus/offices is consolidated into the DOI AD, which is used to authorize access to individual users throughout the enterprise and to manage system and application level access. DOI Azure uses data contained within AD (via synchronization), and access is controlled and is only granted to individuals with the correct level of permissions to view the data.

☐ 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*

Users and contractors will have access to their own information, and in some cases a limited subset of other users based on mission, system, and application management needs.

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

Access is controlled through user account management and authentication with DOI's AD system. Only authorized DOI personnel will have access to the system, and that access is based on least privileges to perform job duties. By default, all users, including guest users, only have access to information that they create or add. DOI performs regular audits of the system access and user interactions within the system. Access to all DOI Azure data will be restricted through AD permissions and access controls. An additional restriction is placed on Guest accounts preventing access to a list of users/accounts or PII information. System administrators will have access based on a need to know and mission accomplishment.

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?*

DOI has baseline privacy requirements that must be included in all contracts that involve information technology (IT) products or services that involve the creation, collection, maintenance, use, processing, storage, access, dissemination or disposal of Privacy Act records or personally identifiable information (PII). These requirements are applicable when DOI information is generated, accessed, stored, processed, or exchanged with DOI or on behalf of DOI by a service provider or subcontracted service provider, regardless of whether the information resides on a DOI information system or a service provider/subcontracted service provider's information system.

The standard DOI Privacy Act contract clauses include Federal Acquisition Regulation (FAR) 52.204-21 Basic Safeguarding of Covered Contractor Information Systems; FAR 52.224.1 Privacy Act Notification; FAR 52.224-2 Privacy Act; FAR 52.224-3 Privacy Training; and FAR 52.239-1 Privacy or Security Safeguards. The DOI Azure GSS contract includes the current required FAR Privacy Act clauses and will include the requisite privacy terms and conditions in the next iteration.

☐ 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*

As part of the security monitoring and management of the system, all user actions taken on DOI Azure resources can be reviewed by DOI Azure administrators. This information includes items such as: failed login/access attempts, changes in user permissions, and failed AD services associated with user authentication.

☐ No

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

As part of the security monitoring and management of the system, all user actions taken on DOI Azure resources can be reviewed by DOI Azure administrators. This information includes items such as: username, day and time of access, failed login/access attempts, changes in user permissions, and failed AD services associated with user authentication.

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

DOI complies with NIST and other Federal requirements for data security as part of a formal program of assessment and authorization, and continuous monitoring. Microsoft Azure is a FedRAMP approved cloud service provider and regularly undergoes reviews to ensure that all security controls are in place and operating as intended. Continuous scans are performed to ensure that changes do not occur that would create an exposure or weakness in the security configuration of any DOI Azure GSS resources. The use of DOI IT systems, including DOI Azure GSS, is conducted in accordance with the appropriate DOI use policy. IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each entity accessing the system; time and date of access, including activities performed using a system administrator's identification; and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system are reported immediately to IT Security.

Access to administrative functions is strictly controlled and can only be granted by DOI Azure Enterprise Managers. Also, all users must complete IT security and privacy awareness training, as well as role-based training, on an annual basis and before being granted access, and sign the DOI Rules of Behavior.

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*

Additionally, there are physical controls in place at Microsoft Azure, the cloud service provider.

(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*

Microsoft Azure is a FedRAMP approved cloud service provider and regularly undergoes reviews to ensure that all security controls are in place and operating as intended. Some of the controls Azure provides include Microsoft Sentinel, Defender for Cloud, Azure Resource Manager, Application Insights, Azure Monitor, Azure Advisor, Azure Application Gateway with WAF, Azure Firewall, Azure Virtual Network, VPN Gateway, Microsoft Antimalware for Azure cloud, Hardware Security Module, Azure Backup, SQL VM TDE, MFA, Azure Active Directory, Azure Confidential Computing and many other layered configurable security options and the ability to control and customize security to meet the unique requirements of DOI.

(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*

Microsoft Azure is a FedRAMP approved cloud service provider and regularly undergoes reviews to ensure that all security controls are in place and operating as intended. Some of the controls Azure provides include Microsoft Sentinel, Defender for Cloud, Azure Resource Manager, Application Insights, Azure Monitor, Azure Advisor, Azure Application Gateway with WAF, Azure Firewall, Azure Virtual Network, VPN Gateway, Microsoft Antimalware

for Azure cloud, Hardware Security Module, Azure Backup, SQL VM TDE, MFA, Azure Active Directory, Azure Confidential Computing and many other layered configurable security options and the ability to control and customize security to meet the unique requirements of DOI. Network infrastructure is backed up to cross region clouds and can be used to restore, if needed.

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 End User Services Branch Chief, ESD, OCIO, serves as the DOI Azure GSS Information System Owner and the official responsible for oversight and management of the Azure security and privacy controls for the Azure system. The DOI Azure GSS Information System Owner, Information System Security Officer, AD System Manager, and applicable Privacy Act System Managers 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 in Azure. Privacy Act System Managers are responsible for responding to Privacy Act requests and complaints in consultation with DOI Privacy Officials.

Each bureau/office is responsible for ensuring the security of data maintained in individual systems and applications served by the DOI Azure GSS, meeting privacy and security requirements within their organization, providing adequate privacy notice, and responding to requests or complaints for their hosted systems and applications in accordance with Federal laws, regulations, and policy.

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 DOI Azure GSS Information System Owner is responsible for daily operational oversight and management of the system's security and privacy controls, and for ensuring to the greatest possible extent that Azure data is properly managed, and that all system access has been granted in a secure and auditable manner. The DOI Azure GSS Information System Owner and all authorized users are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC, DOI's central incident reporting portal, within 1- hour of discovery in accordance with Federal policy and established procedures. The cloud service provider, Microsoft Cloud Services, has the responsibility to monitor or report loss or compromise of data that may occur through the provision of their services.

Each bureau/office is responsible for ensuring the security of data maintained in individual systems and applications served by the DOI Azure GSS and for meeting privacy and security requirements within their organization, and immediately reporting any potential compromise of data in accordance with Federal and DOI privacy breach response policy.