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: Software-defined Data Center (SDDC)
Bureau/Office: Bureau of Indian Affairs, Office of Information Management Technology (OIMT)
Date: April 16, 2021
Point of Contact
Name: Richard Gibbs
Title: Associate Privacy Officer
Email: Privacy_Officer@bia.gov
Phone: (505) 563-5023
Address: 1011 Indian School Rd NW, Albuquerque, New Mexico 87104

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 software-defined data center (SDDC) serves as a virtual hosting architecture that enables Infrastructure-as-a-Service (IaaS) capabilities. The SDDC provides the Bureau of Indian Affairs (BIA) the following services for its customers:

- Deliver software-defined services – program software to deliver virtual applications/services,
- Policy-based provisioning – deliver applications based on pre-approved authorization by business owner, and
- Automated operations management – program software to automate operations and maintenance processes.

C. What is the legal authority?

Departmental Regulations, 5 U.S.C. 301; The Paperwork Reduction Act of 1994, 44 U.S.C. 3501; The Clinger-Cohen Act, 40 U.S.C. 11101, et seq.; Federal Information Security Modernization Act of 2014, 44 U.S.C. 3541 et seq.; Government Paperwork Elimination Act, 44 U.S.C. 3504; The E-Government Act of 2002 (Pub. L. 107-347); the Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; The Snyder Act of 1921 (Pub. L. 67-85); Indian Reorganization Act of 1934 (Pub. L. 73-383); OMB Circular A-130, Management of Federal Information Resources; Executive Order 13571, *Streamlining Service Delivery and Improving Customer Service*, April 11, 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 CSAM?

☐ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*
☒ No. SDDC is undergoing registration in CSAM.

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	Not Applicable	Not Applicable	Not Applicable

SDDC will serve as a hosting environment for BIA and external Federal agency customers. Hosted applications and systems will be identified in the SDDC record in CSAM. Each hosted application and system will be covered by separate PIAs conducted specifically for the application or system that collects, uses, stores, processes, disposes of or discloses personally identifiable information (PII).

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

SDDC is not a Privacy Act system of record. However, records in SDDC are maintained under DOI-47: “HSPD 12 –Logical Security Files (Enterprise Access Control Service/EACS), 72 FR

11040, March 12, 2007, consisting of login records to access the SDDC by system administrators, which may be viewed at https://www.doi.gov/privacy/doi-notices.

Due to the nature of the SDDC as a hosting infrastructure, there may be applications and systems hosted in SDDC that may collect, maintain or process PII and are under the control and ownership of each system owner, information owner, or Privacy Act system manager who are responsible for meeting the requirements of the Privacy Act for the collection, maintenance and sharing of their agency records including publishing systems of records notices and addressing requests for notification, access or amendment under the Privacy Act.

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.

☒ Other: *Specify the PII collected.*

Username, Source IP Address. Due to the nature of the SDDC as a hosting infrastructure, there may be applications and systems hosted in SDDC that may collect, maintain or process PII and are under the control and ownership of each system owner, information owner, or Privacy Act system manager who are responsible for completing a PIA to assess privacy risks, implementing privacy controls, and protecting individual privacy. Please see each applicable PIA for the hosted applications and systems in SDDC for types of PII contained in systems and evaluation of privacy risks. DOI PIAs are available on the DOI PIA website: https://www.doi.gov/privacy/pia.

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*

SDDC contains PII data sourced from Active Directory via a Lightweight Directory Access Protocol (LDAP) Query (specifically Username), as well as Source IP Addresses.

The applications and systems hosted in SDDC may collect, maintain or process PII from various sources. The information in these systems is under the control and ownership of each system owner, information owner, or Privacy Act system manager who are responsible for completing a PIA to assess risks to individual privacy. Please see each applicable PIA for the hosted applications and systems in SDDC for types and sources of PII contained in the systems. DOI PIAs are available on the DOI PIA website: https://www.doi.gov/privacy/pia.

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

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

Information is retrieved via Identity Management Services, which does an LDAP Query from Active Directory.

The applications and systems hosted in SDDC may collect, maintain or process PII through various methods. The information in these systems is under the control and ownership of each system owner, information owner, or Privacy Act system manager who are responsible for completing a PIA to assess risks to individual privacy. Please see each applicable PIA for the hosted applications and systems in SDDC for types and methods of collecting PII. DOI PIAs are available on the DOI PIA website: https://www.doi.gov/privacy/pia.

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

The intended use of the PII collected is for authentication of users to access SDDC in support of the OIMT mission as the BIA's virtual hosting architecture that enables IaaS capabilities for its customers.

There may be numerous applications and systems hosted in SDDC that collect, maintain or process PII and are under the control and ownership of each system owner, information owner, or Privacy Act system manager. Please see each applicable PIA for the hosted applications and systems in SDDC for the purpose and uses of PII. DOI PIAs are available on the DOI PIA website: https://www.doi.gov/privacy/pia.

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.*

Information may be shared with BIA employees acting in their official capacity in the performance of official functions related to monitoring access to the system.

The applications and systems hosted in SDDC are under the control and ownership of each customer and any sharing of PII is at the discretion of the customer.

☐ 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.*

The applications and systems hosted in SDDC may collect PII. Each Federal Agencies' hosted applications and systems will have a separate PIA and information sharing agreement identifying what information may be shared between Indian Affairs and the hosted Federal Agency. Other Federal customer agencies will have access to data for their own employees and contractors. Federal customer agencies have control over their own records, have published their own system of records notices, and are responsible for managing their own records and for meeting the disclosure requirements of the Privacy Act. DOI information may be shared with other Federal agencies as authorized by a routine use outlined in the DOI-47: "HSPD 12 –Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040, March 12, 2007, consisting of login records to access the SDDC by system administrators, which may be viewed at https://www.doi.gov/privacy/doi-notices. User information related to security monitoring, violations or potential threats may be shared with Federal agencies as required by law.

☐ 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 BIA contractors providing Information Technology support services for routine maintenance, future system enhancements, and day-to-day technical support.

The applications and systems hosted in SDDC may collect PII. Each of the hosted applications and systems will have a separate PIA identifying whether information may be shared with BIA contractors.

☐ 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.*

Employees have the option of not providing information on forms during the application and onboarding process. Privacy Act Statements on these forms inform the individual that providing the information is voluntary and that the consequences of not providing the information may have an impact on the individual's employment eligibility and selection.

The SDDC hosts a variety of systems used by Federal government agencies. Any system hosted by the SDDC that includes PII must have a separate PIA to assess and address the relevant privacy risks specific to the system and opportunities for individuals to consent to the collection or use of their PII.

☐ 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.*

A Privacy Act Statement (PAS) is included on the onboarding forms (e.g., OF 306, Declaration for Federal Employment) which provide the Authority, Purpose, Routine Uses, and Disclosure for collecting the information.

☒ Privacy Notice: *Describe each applicable format.*

Privacy notice is provided through publication of this privacy impact assessment (PIA) and the published DOI-47: "HSPD 12 –Logical Security Files (Enterprise Access Control

Service/EACS), 72 FR 11040; March 12, 2007, which may be viewed at https://www.doi.gov/privacy/doi-notices.

☒ Other: *Describe each applicable format.*

Users are presented with a DOI security warning banner 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 in SDDC are primarily retrieved by Username and Source IP.

The SDDC hosts a variety of systems used by Federal government agencies. The retrieval of data is specific to each individual system which are addressed on a system-by-system basis for all systems hosted on the SDDC. The collection, maintenance and retrieval of PII are under the control and ownership of each system owner, information owner, or Privacy Act system manager who are responsible for meeting the requirements of the Privacy Act for the collection, maintenance and sharing of their records including publishing systems of records notices and addressing requests for notification, access or amendment under the Privacy Act. Any system hosted by the SDDC that includes PII will have a separate PIA prepared that will include specific details on data retrieval.

I. Will reports be produced on individuals?

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

Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system. Audit logs capture account creation, modification, disabling, and termination; logon date and time, number of failed login attempts, files accessed, user actions or changes to records. Audit logs also collect information on system users such as username. Access to these activity reports is limited to system administrators and the information system owner.

☐ 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. Users are responsible for ensuring the accuracy of the data associated with their user accounts. Data is checked for accuracy during the account creation process.

The SDDC hosts a variety of systems used by Federal government agencies. Each Federal agency that has a system hosted on SDDC is responsible for collecting, maintaining and ensuring the accuracy of their own data. BIA is responsible for the security, integrity and reliability of the SDDC, but cannot verify the accuracy of the data provided by clients for their own use. The SDDC and all data entered into the applications and systems hosted on the SDDC is subject to appropriate information security controls. These controls will ensure that sensitive information is protected from any undue risk of loss or alteration.

B. How will data be checked for completeness?

Data is checked for completeness during the account creation process. Users are responsible for ensuring the completeness of the data associated with their user accounts.

The SDDC hosts a variety of systems used by Federal government agencies. Each BIA organization or Federal agency that has a system hosted on the SDDC is responsible for collecting, maintaining and ensuring the completeness of their own data. BIA is responsible for the security, integrity and reliability of the SDDC, but cannot verify the completeness of the data provided by clients for their own use.

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

User account information is provided directly by the user during account creation and can be updated by the user. Users are responsible for the accuracy of their records.

The SDDC hosts a variety of systems used by Federal government agencies. Each Federal agency that has a system hosted on the SDDC is responsible for collecting, maintaining and ensuring the currency of their own data. BIA is responsible for the security, integrity and reliability of the SDDC, but cannot verify the currency of the data provided by clients for their own use.

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

SDDC system usage records are covered by the Departmental Records Schedule 1.4A, Short Term Information Technology Records, System Maintenance and Use Records (DAA-0048-2013-0001-0013), approved by the National Archives and Records Administration (NARA). These records include system operations reports, login and password files, audit trail records and backup files. The disposition is temporary. Records are cut-off when superseded or obsolete and destroyed no later than 3 years after cut-off.

The owners of the hosted applications and systems are responsible for establishing records disposition authorities for their systems on a case-by-case basis.

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

Data disposition follow NARA guidelines and approved Records Schedule for transfer, pre-accession and accession activities to NARA. These activities comply with 36 CFR 1220-1249, specifically 1224 - Records Disposition Programs and Part 1236 - Electronic Records Management, NARA Bulletins and the Office of the Special Trustee for American Indians, Office of Trust Records, which provides records management support to include records management policies and procedures, and development of BIA's records retention schedule. System administrators dispose of DOI records by shredding or pulping for paper records and degaussing or erasing for electronic records in accordance with NARA Guidelines and 384

Departmental Manual 1, and the National Institute of Standards and Technology Special Publication 800-88 Revision 1, Guidelines for Media Sanitization.

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 moderate risk to the privacy of individuals due to the PII contained in SDDC. SDDC has undergone a formal Assessment and Authorization in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and National Institute of Standards and Technology (NIST) standards. SDDC is rated as a FISMA moderate system and requires management, operational, and technical controls established by NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations to mitigate the privacy risks for unauthorized access or disclosure, or misuse of PII that may lead to identity theft, fraud, misuse of credit, and exposure of sensitive information.

The risks associated with the sharing or disclosure of information of hosted systems is minimized by the administrative, physical, and technical controls that are properly defined and enforced are commensurate with the privacy risk level of the hosted systems. The hosted systems operating within the SDDC will be logically separated using micro-segmentation, which is a process of creating secure zones that isolate workloads; separating each hosted entity form each other. Controls over information privacy and security are compliant with NIST 800-53. Testing of security and privacy controls will occur on a regular basis as part of the BIA continuous monitoring program. Additionally, controls are tested anytime a change is made to the SDDC environment. The hosted entities will be responsible for their own PII and have to follow their own procedures in case of a breech.

There is a risk of unauthorized access to the system or data, inappropriate use, or disclosure of information to unauthorized recipients. Access to files is strictly limited to authorized personnel who need access to perform official functions. System and information access are based on the "least privilege" principle combined with a "need-to-know" in order to complete assigned duties. BIA manages SDDC user accounts using the Identity Information System (IIS), a self-contained system that provides workflow and access controls, which includes establishing, activating, modifying, reviewing, disabling and removal of SDDC user accounts. System administrators utilize user identification, passwords, and audit logs to ensure appropriate permissions and access levels are enforced to ensure separation of duties is in place. The audit trail includes the identity of each entity accessing the system; time and date of access, and activities performed; and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular, periodic basis and any suspected attempts of unauthorized access or scanning of the system is reported to IT Security. Annually, employees, complete privacy training which includes the topics of inappropriate use and unauthorized disclosure. Personnel with significant privacy responsibilities must also take role-based privacy training initially and annually, to ensure an understanding of the responsibility to protect privacy. Employees must acknowledge their understanding and responsibility for protecting PII, complying with privacy requirements under the Privacy Act, E-Government Act of 2002, OMB privacy guidance, and DOI privacy policy. They must also acknowledge their understanding that there are consequences for not protecting PII and failing to meet privacy requirements. Physical, operational, and technical controls are in place and other security mechanism have also been deployed to ensure data and system security such as firewalls, virtual private network, encryption, malware identification, intrusion detection, and periodic verification of system user activity. Audit logs are routinely checked for unauthorized access or system problems. Data is encrypted during transmission and at rest. Hardcopy documents containing PII are secured in a locked office, desk drawer or file cabinets when not in use to control access, protect against inappropriate use or disclosure to unauthorized individuals.

There is a risk that SDDC may collect and share more information than necessary to complete program goals and objectives, or information may be used outside the scope of the purpose for which it was collected. Only the minimal amount of information needed to perform official functions for which the system was designed is collected and maintained in order to provide a service or perform official functions. Authorized personnel with access to the system are instructed to collect the minimum amount of information needed to perform official functions for which the system was designed and are to share information only with individuals authorized access to the information and that have a need-to-know in the performance of their official functions. Employees complete privacy training which includes topics on the collection and unauthorized disclosure of information. Users are advised not to share sensitive data with individuals not authorized access and to review applicable SORN before sharing information. Employees are aware information may only be disclosed to an external agency or third party if there is informed written consent from the individual who is the subject of the record; if the disclosure is in accordance with a routine use from the published SORN and is compatible with the purpose for which the system was created; or if the disclosure is pursuant to one of the Privacy Act exceptions outlined in 5 U.S.C. 552a(b). Before authorizing and granting system access, users must complete all mandatory security, privacy, records management training and sign the DOI Rules of Behavior to ensure employees with access to sensitive data understand their responsibility to safeguard individual privacy. Employees must acknowledge their understanding and responsibility for protecting PII, complying with privacy requirements under the Privacy Act, E-Government Act of 2002, OMB privacy guidance, and DOI privacy policy. They must also acknowledge their understanding that there are consequences for not protecting PII and failing to meet privacy requirements. System access and restrictions are explicitly granted based on the user roles and permissions in accordance with job descriptions and “need-to-know” factors, based on the “least privilege” principle. Access restrictions to data and various parts of the system’s functionality is role-based and requires supervisory approval. Access controls and system logs are reviewed regularly as part of the continuous monitoring program. SDDC meets BIA’s information system security requirements, including operational and risk management policies.

There is risk of maintaining inaccurate information. To mitigate this risk, the Computer Incident Response Team (CIRT) and Division of Information Security (DIS) perform routine monitoring of PII information in Active Directory. Changes to Active Directory are synchronized with the SDDC identity management system to ensure the accuracy of SDDC information.

There may be a risk associated with the collection of information from other DOI systems. To mitigate this risk, SDDC receives its limited PII from Active Directory via a secure, encrypted Lightweight Directory Access Protocol (LDAP) query.

There is a risk that information will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. The Office of

Information Management Technology (OIMT) is responsible for managing and disposing of BIA records in SDDC as the information owner. The OIMT ensures only records needed to support its program is maintained. Information collected and stored within SDDC is maintained, protected, and destroyed in compliance with all applicable Federal laws, Executive Orders, NARA Guidelines, 384 Departmental Manual 1, and operational requirements.

There is a risk that individuals may not have notice of the purposes for collecting their information. This risk is mitigated as individuals are notified of the privacy practices through this PIA and through the published DOI-47: "HSPD 12 –Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040; March 12, 2007, SORN which may be viewed at https://www.doi.gov/privacy/doi-notices. The PIA, SORN, and PAS provide a detailed description of system source data elements and how an individual's PII is used.

In addition to the risk mitigation actions described above, the Bureau maintains an audit trail of activity sufficiently enough to reconstruct security relevant events. The BIA follows the "least privilege" security principle, such that only the least amount of access is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user. Access to the DOI Network requires two-factor authentication. Users are granted authorized access to perform their official duties and such privileges comply with the principles of separation of duties. Controls over information privacy and security are compliant with NIST 800-53. DOI employees must take Information Management Training (IMT) which includes Cybersecurity (FISSA), Privacy, Records Management, and Controlled Unclassified Information before being granted access to DOI information and information systems, and annually thereafter. Personnel with significant privacy responsibilities must also take role-based privacy training initially and annually, to ensure an understanding of the responsibility to protect privacy. DOI personnel also sign the DOI Rules of Behavior. 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.

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 use of the system and data collected is relevant and necessary to the purpose for which SDDC was designed, it supports the OIMT mission as the BIA's virtual hosting architecture that enables IaaS capabilities for its customers.

The SDDC hosts a variety of systems used by Federal government agencies. The relevance and necessity of data is an issue that must be addressed on a system-by-system basis for all systems hosted on the SDDC. The system hosted by the SDDC that includes PII will have a separate PIA prepared; these individual system PIAs will include specific details on the relevance and necessity of the use of the data.

☐ 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. SDDC 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. *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*

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

Users are only given access to data on a 'least privilege' principle and 'need-to-know' to perform official functions. BIA manages SDDC user accounts using the IIS, a self-contained system that provides workflow and access controls, which includes establishing, activating, modifying, reviewing, disabling and removal of SDDC user accounts. Federal employee access requires supervisor approval. Contract officer representatives determine the level of access for contractors, which is approved by the information owner. Tribes who have contracted or compacted a government trust function may submit requests for access for tribal members working on a program, which must be approved by the program manager.

The SDDC hosts a variety of systems used by Federal government agencies. User access must be addressed on a system-by-system basis for all systems hosted on the SDDC.

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 required to sign nondisclosure agreements as a contingent part of their employment. They are also required to sign the DOI Rules of Behavior and complete security and privacy training before being granted access to a DOI computer system or network. Information security and role-based privacy training must be completed on an annual basis as a contractual employment requirement. The following Privacy Act contract clauses were included in the contract.

- Federal Acquisition Regulation (FAR) 52.224-1, Privacy Act Notification (Apr 1984)
- FAR 52.224-2, Privacy Act (Apr 1984)
- FAR 52.224-3, Privacy Act Training (Jan 2017)
- FAR 52.239-1, Privacy or Security Safeguards (Aug 1996)

☐ 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*

The purpose of SDDC is not to monitor individuals, however user actions and use of the system is monitored to meet DOI security policies. Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system.

☐ No

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

The SDDC system is not intended to monitor individuals; however, the system has the functionality to audit user activity. Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system. The logs capture account creation, modification, disabling, and termination. Additionally, the system may capture a variety of user actions and information such as usernames, logon date, number of successful and unsuccessful logins, and modifications made to data by different users along with date and time stamps. Firewalls and network security configurations are also built into the architecture of the system and NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, and other DOI policies are fully implemented to prevent unauthorized monitoring.

The SDDC hosts a variety of systems used by Federal government agencies. While it is not anticipated that any systems hosted on the SDDC will have the capability to identify, locate, and monitor individuals, the issue of individual monitoring must be addressed on a system-by-system basis for all systems hosted on the SDDC. As discussed above, any system hosted by the SDDC that includes PII will have a separate PIA prepared. These individual system PIAs will include specific details on individual monitoring.

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

SDDC has the ability to audit the usage activity in the system. Firewalls and network security configurations are also built into the architecture of the system and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, and other DOI policies are fully implemented to prevent unauthorized monitoring. SDDC System Administrators review the use of the system and the activities of users to ensure that the system is not improperly used and to prevent unauthorized use or access. SDDC assigns roles based on the principles of 'least privilege' and performs due diligence toward ensuring that separation of duties is in place.

In addition, all users will be required to consent to DOI Rules of Behavior. Users must complete annual Information Management and Technology (IMT) Awareness Training, which includes Privacy Awareness Training, Records Management and Section 508 Compliance training, and Controlled Unclassified Information (CUI) training before being granted access to the DOI network or any DOI system, and annually thereafter. To ensure personnel have an understanding of their responsibilities for protecting privacy, personnel with significant privacy responsibilities must also take role-based privacy training initially upon employment and annually thereafter.

The use of DOI IT systems is conducted in accordance with the appropriate DOI use policy to ensure systems maintain an audit trail of activity sufficiently to reconstruct security relevant events. The SDDC audit trail will include system user username, logon date and time, number of failed login attempts, files accessed, and user actions or changes to records. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system is reported immediately to IT Security.

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 Associate Chief Information Officer (ACIO) is the Information System Owner for SDDC. The Information System Owner (ISO), Information System Security Officer (ISSO), and authorized bureau/office 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 SDDC. The ISO and the Privacy Act system managers are responsible for addressing any Privacy Act complaints and requests for notification, access, redress, or amendment of records in consultation with the 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 SDDC ISO and ISSO are responsible for the central oversight and management of the SDDC 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 SDDC ISO, ISSO, and bureau and office system administrators 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 that appropriate remedial activities are taken to mitigate any impact to individuals in coordination with DOI Privacy Officials. Program officials and users are also responsible for protecting PII and meeting requirements under the Privacy Act and Federal law and policy, and for reporting any potential compromise to DOI-CIRC and privacy officials.