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: Albuquerque Data Center (ADC) Access Control Management System (ACMS)
Bureau/Office: Bureau of Indian Affairs, Office of Information Management Technology
Date: February 8, 2024
Point of Contact
Name: Richard Gibbs
Title: Indian Affairs 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 Bureau of Indian Affairs (BIA), Office of Information Management Technology (OIMT) completed a Privacy Threshold Analysis (PTA) August 23, 2022, that indicated a Privacy Impact Assessment (PIA) must be completed. This PIA is being completed to comply with the Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C. §3551 to §3559), the E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101), and Privacy Act of 1974.

The ADC currently provides hosting services to information systems for the Bureau of Indian Affairs (BIA), Bureau of Indian Education (BIE), Bureau of Trust Fund Administration (BTFA), Indian Health Services (IHS), and the Department of Health and Human Services (HHS). Under the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, Guide for Developing Security Plans for Federal Information Systems, the ADC is a physical security boundary with the main purpose of providing physical/environmental and other related security controls (SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations) for information systems and applications within the ADC.

The ADC Access Control Management System (ADC ACMS) boundary consists of the system infrastructure components of Physical Access Control (PAC) and Physical Access Monitoring (PAM). The ADC ACMS is comprised of proximity card readers, closed-circuit television (CCTV) security surveillance system, and management software.

The ADC ACMS uses two Identiv commercial off-the-shelf (COTS) products, the Velocity Badging and Velocity Vision systems. The Velocity Badging software controls, monitors, and provides audit trail functionality for all authorized ingress and egress activities for external doors and interior corridors of the ADC. For this process to take place, the badging system stores and processes a minimal amount of information on each person requiring a badge for access to areas within the ADC. Velocity Vision is a CCTV security surveillance system that manages and monitors the ADC and stores still pictures, video and video logs of individuals entering or exiting the ADC. There is no audio component with the CCTV surveillance camera system.

The ADC ACMS Identiv software component uses the Bison System Access Management (BSAM) system to manage access to the system. BSAM is the DOI-wide authoritative source for all identities and the primary solution for Identity Lifecycle Management (ILM). BSAM supports ILM requirements by providing a standard set of enterprise workflows that manage DOI identities from the time a new employee or contractor walks in the DOI door until they depart the DOI, and everything in between. BSAM is used to establish, activate, modify, review, disable user accounts. System administrators utilize user identification, Domain managed Service Account passwords, and audit logs to ensure appropriate permissions and access levels are enforced to ensure separation of duties is in place. Velocity Console uses Single-Sign On combined with a configuration that limits the workstations that can connect to the Velocity System. Console Admin Users login to the workstation on the network using their PIV Card.

AD authentication for User access is covered under the DOI Enterprise Hosted Infrastructure (EHI) Privacy Impact Assessment. For additional information on User authentication please see the EHI PIA on the DOI Privacy website: https://www.doi.gov/privacy/pia.

C. What is the legal authority?

5 U.S.C. 301; Federal Information Security Act (Pub. L. 104-106, section 5113), Electronic Government Act (Pub. L. 104-347, section 203); Paperwork Reduction Act of 1995 (44 U.S.C. §§3501-3521); Government Paperwork Elimination Act (44 U.S.C. § 3504); Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; Federal Property and Administrative Act of 1949, as amended; the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458,

Section 3001 (50 U.S.C. 435b); Executive Order 9397; Federal Property Regulations, July 2002; and Presidential Memorandum on Upgrading Security at Federal Facilities, June 28, 1995.

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: The ADC is a physical security boundary responsible for providing Physical/Environmental (PE) controls and other related security controls (NIST SP 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations") for information systems and applications within the ADC.

E. Is this information system registered in the Governance, Risk and Compliance platform?

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

UII Code: 010-000002493; System Security and Privacy Plan for Albuquerque Data Center (ADC) Access Control Management System (ACMS).

☐ 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.*
Identiv Velocity enrollment station	Associates a personal identity verification (PIV) card to the individual who will be using the card for physical access to the ADC.	Yes	The enrollment station collects Federal personnel and Federal contractor name, title, work phone, work email, and supervisor's name and work phone number, Federal contractor contract number.
Identiv Velocity Badging Software - Door and badge reader access control system	Controls and monitors ADC external and interior corridor doors by providing automated physical access control, monitoring, and auditing.	No	Information stored on the PAC is limited to badging card number.
Identiv Vision - CCTV system managing ADC security cameras	Manages CCTV surveillance cameras and stores still pictures, video, and video logs.	Yes	Captures Federal personnel, Federal contractor, and visitor video images. Video images and/or video logs could be associated with visitor logs to obtain a visitor's name and employer that has entered the ADC.
Visitor Management (paper based)	Logs temporary access to the ADC by visitors.	Yes	Visitor name, organization, phone number, name of Federal employee serving as an escort, date/time in/out.

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)*

Records pertaining to physical security and access to ADC are covered under the INTERIOR/DOI-46, Physical Security Access Files, 85 FR 3406 (January 21, 2020); modification published at 86 FR 50157 (September 7, 2021). Records pertaining to accessing Departmental networks, information systems, and e-mail services are maintained 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), which may be viewed at https://www.doi.gov/privacy/doi-notices.

☐ 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

☒ Other: Identiv Velocity System Administrator: Username and full name.

Federal Employee and Federal Contractor: Official phone number, duty station address, official title of employee or contractor, type of appointment, contract number, supervisor name and work phone number, time or location of entry or exit, an auto-generated PAC number, and video image.

Visitor: The BIA OIMT Visitor sign-in sheet records visitor name, signature, business organization, business phone number, purpose of visit, and date/time in/out and video image.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☒ DOI records
☐ Third party source
☐ State agency
☐ Other: *Describe*

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

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

Federal Employees and Federal Contractors complete an OIMT Access Request Form to request access to the ADC. The Access Request Form collects employee and contractor name, position/title, work phone, supervisor name, supervisor work phone number. Video images are captured from CCTV surveillance cameras within the ADC.

Visitors complete the paper BIA-OIMT Visitor Sign-in Sheet. The sign-in sheet collects the visitor's name, signature, business organization, business phone number, purpose of visit, date, and time in/out. Video images are captured from CCTV surveillance cameras within the ADC.

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

PII collected and maintained is used to ensure only authorized personnel and visitors with proper authorization and identification are permitted entry into the ADC. PII is used to support physical access control, intrusion detection and video surveillance functions to ensure the safety and security of ADC staff and visitors.

PII, including CCTV video, may be used to assist the BIA Office of Justice Services, U.S. Secret Service, Department of Homeland Security Federal Protective Service, and the Office of

Inspector General agencies for investigation of emergency response situations or the violation, enforcement or implementation of a statute, rule, regulation, or license.

PII, including CCTV video, may be used to assist security guard staff at the entrance to Indian Affairs (IA) managed facilities to associate visitor images to control visitor logs in support of investigation of emergency response situations or the violation, enforcement or implementation of a statute, rule, regulation, or license.

PII, including CCTV video, may be used by Employee Relations or Contracting Officers for personnel attendance verification and personal-related incidents.

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.*

Systems Administrators (authorized employees only) manage user access, review, and analyze user account information (name, username, login dates, access attempts, etc.) against operating system and security events when reporting inappropriate or unusual activity to designated DOI officials. IA Division of Information Security and Data Operations Center (collectively known as security office personnel), system administrators, and contracted security guard staff at the ADC facility, have different defined levels of access to the data within the system, depending on their access rights. Security office personnel and security guard staff have view only access to the data, this includes video footage and proximity card logs. Security office personnel and security guard staff are given this access for the purposes of providing a monitoring system with the overarching goal of providing a robust, responsive 24/7 site-wide physical security program that ensures the reliability and safety of the facility. ADC System administrators are the only individuals that have 24/7 read (view), write, and export access to the data that is used by the ADC ACMS. System administrators are given this level of access to maintain, repair, and patch vulnerabilities, which helps to ensure that the ADC ACMS remains a reliable tool for the security office personnel and security guard staff to provide the comprehensive security program the ADC facility needs.

PII, including CCTV video, may be shared with the BIA Office of Justice Services for investigation of emergency response situations or the violation and enforcement of a statute, rule, regulation, or license.

PII is periodically reviewed by authorized BIA personnel charged with auditing requirements associated with physical access to the ADC.

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

ADC ACMS data may be used by other DOI Bureaus and Offices for criminal investigation purposes, when given proper authorization and approval by DOI and/or IA leadership.

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

Data may be shared with other Federal agencies, such as the Federal Bureau of Investigation, Department of Homeland Security, or other agency if required for reporting or investigative purposes due to suspected criminal activity, potential insider threat, or violation of law or policy, but only with proper DOI and/or BIA approval. IA may share information with external agencies and organizations as authorized by the Privacy Act and outlined in the routine uses section of the published INTERIOR/DOI-46, Physical Security Access Files, system of records notice (SORN), INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) and INTERIOR/DOI-50, Insider Threat Program SORNs.

PII, including CCTV video, may be used to assist the U.S. Secret Service, Department of Homeland Security Federal Protective Service, and Office of Inspector General agencies for investigation of emergency response situations or the violation, enforcement or implementation of a statute, rule, regulation, or license.

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

PII is shared with state or local agencies for investigation of emergency response situations or the violation, enforcement or implementation of a statute, rule, regulation, or license as authorized and described in the routine uses published in the INTERIOR/DOI-46, Physical Security Access Files, system of records notice (SORN), INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) and INTERIOR/DOI-50, Insider Threat Program SORNs.

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

Contract security guard staff monitor IA-controlled entrances, and verify the identities of employees, visitors, and other individuals who access these facilities.

☐ 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.*

Federal employees and contractors can decline to provide the identifying information required for registration in the ADC ACMS or Visitors can decline to complete the OIMT Access Request Form for entry to the ADC; however, failure to do so can result in denial of entry.

Individuals are notified before entering the ADC by clearly posted signs that they will be under CCTV surveillance. Individuals can choose not to enter the secured area.

In some cases, such as for use of visual recordings, individuals who enter on Federal properties and public areas do not have a reasonable expectation of privacy. Some DOI controlled areas may have signs posted that inform individuals of surveillance activities, but in many cases, notice may not be provided, or consent obtained for images captured.

☐ 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.*

Federal employees and employed contractors requesting access to the ADC must submit an *ADC Access Card Request Form* approved by their supervisor. Temporary visitors must complete the *BIA-OIMT Visitor Sign-in Sheet*. A Privacy Act Statement (PAS) is included on these forms. A privacy notice is posted on the entry door to the ADC next to the notice to individuals that the facility is under 24/7 camera surveillance. The PAS provides detailed information on the authority and purpose of collecting PII, how PII is used and with whom the PII is shared, the applicable routine uses under the INTERIOR/DOI-46 SORN, and the voluntary nature of the collection, as well as impacts for not providing information.

☒ Privacy Notice: *Describe each applicable format.*

Privacy notice is provided through publication of this privacy impact assessment and the published INTERIOR/DOI-46, Physical Security Access Files, 85 FR 3406 (January 21, 2020); modification published at 86 FR 50157 (September 7, 2021), which may be viewed at https://www.doi.gov/privacy/doi-notices.

A sign is posted at the entry to the ADC informing individuals the facility is under video surveillance.

A Privacy Notice is provided to individuals through a posted sign at the entrance to the facility and within the facility, and copies will be made available upon request. The notice includes legal authorities for collecting information, the purpose of the collection and uses of the information, how and to whom it is shared outside of the Department, and how the provision of information is voluntary and that visitors may decline to provide information and how that may prevent them from entering the facility.

☒ 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.).

Records maintained by the ACMS are primarily retrieved by identifiers such as name and image; date, time or location of entry or exit; and PAC number or date.

Authorized personnel retrieve data manually during auditing processes or incident management activities. Records may be retrieved by employee name, image if associated with a name, employment contact information such as work phone number, work address, official title of Federal employee or Contractor, type of employment appointment, contract number, and supervisor name; date/time or location of entry or exit; PAC number.

I. Will reports be produced on individuals?

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

The ACMS has limited reporting capabilities. ADC ACMS system administrators may generate reports upon request by authorized BIA officials in response to security breach investigations or to any other authorized investigative agency, including state and local law enforcement; other Federal agency customers, and to individuals authorized in Interagency Agreements. Reports on individuals will include name, time, and location of access; however, there may be times where employee ingress or egress times are requested for administrative or investigative purposes. Video recordings of incidents may be produced for investigative purposes and may be generated by authorized Security staff for law enforcement entities such as, but not limited to, the BIA Office of Justice Services, U.S. Secret Service, Department of Homeland Security Federal Protective Service, and Office of Inspector General.

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. System administrators and the information system owner have access to these activity reports.

☐ No

Section 3. Attributes of System Data

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

Data is collected from visiting federal agency personnel that are hosted in the ADC needing physical access to common areas, administrative areas, and equipment. ADC Sponsors sign the OIMT Visitor Sign-in Sheet, verify the accuracy and completeness of provided data.

Visitor identity is collected directly from the individual and verified by photo identification, which is presumed to be accurate at the time presented by the individual requesting access to the ADC.

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.

Federal employees, Federal contractors, and visitors can seek records about themselves that are maintained in this system of records. And if the individual believes the records are not accurate can request corrections or the removal of material from the record by writing to the System Manager identified in the INTERIOR/DOI-46, Physical Security Access Files SORN. These rights and request requirements are outlined in the DOI Privacy Act regulations at 43 CFR Part 2, Subpart K.

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.

Visitor information is checked for completeness by ADC staff as it is entered on the OIMT Visitor Sign-in Sheet.

Federal employees, Federal contractors, and visitors can seek records about themselves that are maintained in this system of records. And if the individual believes the records are not complete can request corrections or the removal of material from the record by writing to the System Manager identified in the INTERIOR/DOI-46, Physical Security Access Files SORN. These rights and request requirements are outlined in the DOI Privacy Act regulations at 43 CFR Part 2, Subpart K.

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 currency of their records.

Federal employees, Federal contractors, and visitors can seek records about themselves that are maintained in this system of records. And if the individual believes the records are not current can request corrections or the removal of material from the record by writing to the System Manager identified in the INTERIOR/DOI-46, Physical Security Access Files SORN. These rights and request requirements are outlined in the DOI Privacy Act regulations at 43 CFR Part 2, Subpart K.

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

Data and information maintained is retained under the appropriate National Archives and Records Administration (NARA) and Department Records Schedule (DRS).

Facilities security and protective service records, which include the BIA-OIMT Visitor sign-in Sheet and the ADC Access Card Request Form, are retained in accordance with DRS DAA-0048-2013-0001, Short-term Administrative Records. Records under this schedule are considered temporary and may be destroyed three years after cut-off. These records encompass administrative functions that are produced and maintained during routine business, and do not reflect government business that is subject to additional preservation. Records are characterized by being necessary for day-to-day operations but not long-term justification of the office's activities. CCTV records are covered under General Records Schedule 5.6, Item 090. These records are Temporary. CCTV records are maintained for 30 days or longer as needed. Retention periods for security violation files relating to investigations referred to administrative or law enforcement organizations may vary depending on the subject matter and Departmental policy.

Information technology records are maintained under the DRS 1.4 Information Technology (IT) (DAA-0048-2013-0001-0013, System Maintenance and Use Records and DAA-0048-2013-0001-0014, System Planning, Design, and Documentation). These records include IT files that are necessary for day-to-day operations but no longer-term justification of the office's activities. The disposition of these records is temporary. Records covered under DAA-0048-2013-0001-0013 have a temporary disposition and will be cut off when superseded or obsolete and destroyed no later than three years after cutoff. Records covered under DAA-0048-2013-0001-0014 have a temporary disposition and will be cut off when superseded by a newer version of upon termination of the system and destroyed three 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?

Data disposition complies with 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 Bureau of Trust Funds Administration, 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 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 risk to the privacy of individuals due to the PII used in the ADC ACMS to manage access to the ADC. The PII includes employee name, username, work email address, work phone number, duty station address, and official title of DOI employees and contractors, the work related PII, such as contact information, duty station, and title, which is not considered sensitive, and video images of personnel and visitors captured from CCTV surveillance cameras within the ADC. The ADC ACMS is rated as Federal Information Security Modernization Act (FISMA) moderate system. The ADC ACMS has undergone a formal Assessment and Authorization and has been granted an authority to operate in accordance with the Federal FISMA and National Institute of Standards and Technology (NIST) standards.

The ADC ACMS has a System Security and Privacy Plan and is part of a Continuous Monitoring program that includes ongoing security and privacy control assessments to ensure controls are implemented and assessed in compliance with policy and standards. Additionally, vulnerability scans are routinely conducted on the ADC ACMS to identify and mitigate any found.

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 is based on the "least privilege" principle combined with a "need-to-know" to complete assigned duties. BIA manages user accounts using the BSAM system. BSAM is the DOI-wide authoritative source for all identities and the primary solution for ILM. BSAM supports ILM requirements by providing a standard set of enterprise workflows that manage DOI identities from the time a new employee or contractor walks in the DOI door until they depart the DOI, and everything in between. BSAM is used to establish, activate, modify, review, disable user accounts. System administrators utilize user identification, PIV, 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. 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 ADC ACMS 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 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. 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. 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. ADC ACMS meets BIA’s information system security requirements, including operational and risk management policies.

There is a risk of maintaining inaccurate information. The ADC ACMS information is reviewed on a periodic basis and verified for accuracy. ADC ACMS administrative personnel review various application and access logs to ensure that old records are either corrected or purged in accordance with NARA guidance. Additionally, Federal employees, Federal contractors, and visitors can seek records about themselves that are maintained in this system of records and if an individual believes the records are not accurate, they can request corrections or the removal of material from the record by writing to the System Manager identified in the INTERIOR/DOI-46, Physical Security Access Files SORN. These rights and request requirements are outlined in the DOI Privacy Act regulations at 43 CFR Part 2, Subpart K.

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 ADC ACMS information owner, the system owner and the assigned records management specialist are responsible for ensuring only those records needed to support its program are maintained. The

ADC ACMS system usage records are covered by the DRS DAA-0048-2013-0001, Short-term Administrative Records, approved by NARA. These records include system operations reports, login 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. Information collected and stored within the ADC ACMS is maintained, protected, and destroyed in compliance with all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

There is a risk that individuals may not have adequate 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 INTERIOR/DOI-46, Physical Security Access Files SORN, 85 FR 3406, (January 21, 2020); modification published at 86 FR 50156 (September 7, 2021) which may be viewed at: https://www.doi.gov/privacy/doi-notices. Additionally, a PAS is included on both the *BIA-OIMT Visitor Sign-in Sheet and ADC Access Card Request Form* used with the ADC ACMS. The PIA, SORN, and PAS provide a detailed description of system source data elements and how an individual's PII is used. Notice of surveillance is also provided via signs posted in the building where there are CCTV cameras.

In addition to the risk mitigation actions described above, the BIA 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 multi-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 SP 800-53. DOI employees must take Information Management and Technology (IMT) Awareness Training, which includes Privacy Awareness Training, Records Management, Section 508 Compliance, and Controlled Unclassified Information (CUI) training 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 the ADC ACMS was designed and supports the mission by managing physical security operations and visitor access to Federally controlled facilities and information systems.

☐ 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. No new data created.

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: Information may be shared with Federal agency points-of-contact (POC) who are using the ADC hosted services. Hosted agencies may request access logs and surveillance footage on their agency's personnel and designated areas in the ADC. Only hosted agency POCs identified in the Interagency Agreement or service level agreement can make these requests with the approval of the ADC Manager.

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

ADC ACMS is a single use information system for controlling physical access within the ADC. While the operator of this system may allow an individual to verify their information manually through visual inspection during PAC creation, Administrative and operator level access is provided using BSAM, which requires supervisor and system owner approval prior to access being granted on a need-to-know basis to perform an official function.

Users are only given access to data based on the "least privilege" principle combined with a "need-to-know" to complete assigned duties. BIA manages user accounts using the BSAM system. BSAM is the DOI-wide authoritative source for all identities and the primary solution for ILM. BSAM supports ILM requirements by providing a standard set of enterprise workflows that manage DOI identities from the time a new employee or contractor walks in the DOI door until they depart the DOI, and everything in between. BSAM is used to establish, activate, modify, review, disable 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.

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 privacy terms and conditions and 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 function of the ADC ACMS is to monitor individuals to meet DOI security policies. The ACMS can identify individuals and monitor them entering and leaving the ADC.

ADC ACMS has the capability to monitor and audit system user actions 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 ADC ACMS is intended to monitor individuals. ADC ACMS provides audit trails which detail the date and time employees gained physical access to the ADC and interior corridors. Audit records contain date, time, access panel number, unique ID of the individual's PAC, as well as the individual's name. ADC ACMS provides video surveillance images and videos that contain time and date stamp that can be correlated with PAC card usage.

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 SP 800-53, and other DOI policies are fully implemented to prevent unauthorized monitoring.

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

Physical security and system administrative personnel have access to the data in the system. System access is protected and requires a PIV card for access. Each person granted access to the system must be trained and individually authorized to use the system. All system users are required to follow established internal security protocols. Service Accounts are tied to Domain Credentials within the System.

ADC ACMS can audit the usage activity in the system. ADC ACMS 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. ADC ACMS assigns roles based on the principles of 'least privilege' and performs due diligence toward ensuring that separation of duties is in place.

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 sufficient to reconstruct security relevant events. The ADC ACMS 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
☒ Multi-Factor Authentication (MFA)
☒ Firewall
☒ Encryption
☒ User Identification
□ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
□ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
□ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The Deputy Associate Chief Information Officer is the Information System Owner. The Information System Owner (ISO), Information System Security Officer (ISSO), and authorized bureau/office system managers are responsible for oversight and management of security and privacy controls and the protection of IA information processed and stored in ADC ACMS. 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 ADC ACMS ISO and ISSO are responsible for the central oversight and management of the ADC ACMS 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 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, within 1-hour of discovery in accordance with Federal policy and established DOI breach reporting 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 reporting any potential compromise to DOI-CIRC and privacy officials.