

# Morris K. Udall and Stewart L. Udall Foundation



## Privacy Impact Assessment

For

## MKUSEF

Reviewed by: Sara Moeller, Senior Agency Official for Privacy

## **Udall Foundation Privacy Impact Assessment MKUSEF – Agencywide System**

### **Abstract**

The Morris K. Udall and Stewart L. Udall Foundation (Udall Foundation) uses a single information technology (IT) system to facilitate its programmatic and administrative work. This system has numerous subcomponents and applications that collect, process, analyze, store, disseminate, and destroy Personally Identifiable Information (PII) and Business Identifiable Information (BII). Additionally, the agency maintains a small number of analog (paper) records that collect, process, analyze, store, disseminate, and destroy PII and BII. The PIA was conducted because the MKUSEF system has the potential to store PII within its physical and cloud environments.

### **Overview**

The Morris K. Udall Foundation was established by the U.S. Congress in 1992 as an independent executive branch agency to honor Morris K. Udall's lasting impact on this Nation's environment, public lands, and natural resources, and his support of the rights and self-governance of Native Americans and Alaska Natives. In 2009, Congress enacted legislation to also honor Stewart L. Udall for his half century of distinguished national leadership in environmental and Native American policy. The agency is known today as the Morris K. Udall and Stewart L. Udall Foundation (Udall Foundation) and is headquartered in Tucson, Arizona. The Udall Foundation is authorized to provide educational programs, funding, and collaboration and conflict resolution services related to the environment, Native American and Alaska Native health care issues, and Tribal public policy issues.

To perform its mission, the agency must collect and use a variety of PII/BII. This includes data that are necessary for the agency to meet its mission and statutory obligations (for example, personal information from scholarship applicants and agreement information for various conflict resolution services). Additionally, the agency must collect PII/BII to ensure its administrative teams can perform their functions. These functions include, but are not limited to, finance and payroll, human resources management, operations, and information technology.

The Udall Foundation operates a hybrid agency-wide information system made up of custom applications, shared drives, Microsoft 365 GCC, commercial off-the-shelf tools, and physical and virtual servers, all categorized as FISMA Moderate, as well as paper records that contain PII and BII. Records within this system are managed according to the General Records Schedule and the Agency Records Schedule. The agency utilizes category labeling software to appropriately label PII/BII based on keywords.

### **I. Authorities and Other Requirements**

#### **a. What specific legal authorities and/or agreements permit and define the collection**

**of information by the project in question?**

The authority for the Udall Foundation's collection of PII/BII comes from various statutes, regulations, Executive Orders, and other authorities, including 5 U.S.C. § 552, Freedom of Information Act; 5 U.S.C. § 552a, Privacy Act; 20 U.S.C. §§ 5601–5609, Morris K. Udall and Stewart L. Udall Foundation; 40 U.S.C. § 1401, Clinger-Cohen Act; Title 41 U.S.C. Public Contracts; 44 U.S.C. Chapter 35, Paperwork Reduction Act; 44 U.S.C. 3541 et seq., Federal Information Security Modernization Act of 2014; 36 CFR Part 1600, Public Availability of Documents and Records; Executive Order 9397, as amended by 13478, relating to Federal Agency Use of Social Security Numbers; 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; Presidential Memorandum, Building a 21st Century Digital Government, May 23, 2012; and OMB Circular A-130, Managing Information as a Strategic Resource.

**b. Has a system security plan been completed for the information system(s) supporting the project?**

A first draft of the system security plan was completed on April 30, 2026. The authority to Operate for the system was granted on April 16, 2026, and expires on April 30, 2029. Due to the collection of PII/BII, the system is categorized as Moderate under the Federal Information Processing Standards Publication 199.

**II. System Description**

The Udall Foundation uses an agency-wide system with subcomponents and applications to optimize the efficiency and effectiveness of the agency's programmatic and business processes. Within the hybrid system, the agency operates custom applications, shared drives, Microsoft 365 GCC, and numerous commercial off the shelf (COTS) products. The system includes physical servers located at multiple locations as well as virtual servers. The agency also maintains some paper records.

Records on the system are managed in accordance with the General Records Schedule and Agency Records Schedule. An example of a typical PII lifecycle includes contact lists for an environmental conflict resolution project. In this case, a program manager will collect names and emails of project participants so that they can schedule meetings and distribute necessary documents. This contact list is retained on a specified project drive in a specific folder, and access to the list is limited to team members on the project who have a need to know the contact list. Folder access is set up by the IT team using a folder access form that is signed by the supervisor and system owner. Throughout the project, the contacts are continuously updated on an as needed basis, and after the conclusion of the project, the list is deleted in accordance with the General Records Schedule.

Users may connect to the system using government furnished equipment, including a

Issued: 9/23/2026

laptop and mobile phone. The agency uses multiple layers of authentication and security to manage access to the system. Additionally, access to system areas is permission-based, with access being dependent on the individual's job duties and responsibilities. Only Udall Foundation employees and contractors are given user accounts, and guest accounts are not used. The IT team performs continuous diagnostics and monitoring, logging, and numerous other activities to monitor the system for suspicious activity. The IT team also continuously performs patching and vulnerability mitigation to ensure continued system security. Physical (paper) records are maintained by individuals and filing cabinets with locks are used to secure the records. These physical records are maintained in the Udall Foundation's offices where access is controlled through fobs and keys.

### a. Status of the Information System

Indicate whether the information system is a new or existing system. (*Choose one*)

☐ This is a new information system.

☐ This is an existing information system with changes that create new privacy risks.

(*Check all that apply.*)

| Changes That Create New Privacy Risks                     |  |                        |  |                                    |  |
|-----------------------------------------------------------|--|------------------------|--|------------------------------------|--|
| a. Conversions                                            |  | d. Significant Merging |  | g. New Interagency Uses            |  |
| b. Anonymous to Non- Anonymous                            |  | e. New Public Access   |  | h. Internal Flow or Collection     |  |
| c. Significant System Management Changes                  |  | f. Commercial Sources  |  | i. Alteration in Character of Data |  |
| j. Other changes that create new privacy risks (specify): |  |                        |  |                                    |  |

☒ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

☐ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

### b. Information in the System

Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. (*Check all that apply.*)

| Identifying Numbers                           |                                     |                     |                                     |                      |                                     |
|-----------------------------------------------|-------------------------------------|---------------------|-------------------------------------|----------------------|-------------------------------------|
| a. Social Security (including last 4 digits)* | <input checked="" type="checkbox"/> | f. Driver's License | <input checked="" type="checkbox"/> | j. Financial Account | <input checked="" type="checkbox"/> |

| Identifying Numbers                                                                                                                                                                                                                                                                                                      |   |                       |   |                          |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|-----------------------|---|--------------------------|---|
| b. Taxpayer ID                                                                                                                                                                                                                                                                                                           | ✓ | g. Passport           | ✓ | k. Financial Transaction | ✓ |
| c. Employer ID                                                                                                                                                                                                                                                                                                           | ✓ | h. Alien Registration | ✓ | l. Vehicle Identifier    |   |
| d. Employee ID                                                                                                                                                                                                                                                                                                           | ✓ | i. Credit Card        | ✓ | m. Medical Record        | ✓ |
| e. File/Case ID                                                                                                                                                                                                                                                                                                          | ✓ |                       |   |                          |   |
| n. Other identifying numbers, including numbers assigned by Program/Office personnel in lieu of using a name or other identifying data (specify): Vendor ID, Applicant ID                                                                                                                                                |   |                       |   |                          |   |
| *Explanation of the business need to collect, maintain, or disseminate the Social Security number, including truncated form: Social security numbers are collected only as needed to perform program and administrative functions. For example, this information is collected from award recipients to process payments. |   |                       |   |                          |   |

| General Personal Data                                        |   |                     |   |                             |   |
|--------------------------------------------------------------|---|---------------------|---|-----------------------------|---|
| a. Name                                                      | ✓ | h. Date of Birth    | ✓ | o. Financial Information    | ✓ |
| b. Maiden Name                                               | ✓ | i. Place of Birth   | ✓ | p. Medical Information      | ✓ |
| c. Alias                                                     | ✓ | j. Home Address     | ✓ | q. Military Service         | ✓ |
| d. Sex                                                       | ✓ | k. Telephone Number | ✓ | r. Criminal Record          | ✓ |
| e. Age                                                       | ✓ | l. Email Address    | ✓ | s. Physical Characteristics | ✓ |
| f. Race/Ethnicity                                            | ✓ | m. Education        | ✓ | t. Mother's Maiden Name     | ✓ |
| g. Citizenship                                               | ✓ | n. Religion         | ✓ |                             |   |
| u. Other general personal data (specify): Tribal affiliation |   |                     |   |                             |   |

| Work-Related Data                     |   |                                                                    |   |                                        |   |
|---------------------------------------|---|--------------------------------------------------------------------|---|----------------------------------------|---|
| a. Occupation                         | ✓ | e. Work Email Address                                              | ✓ | i. Business Associates                 | ✓ |
| b. Job Title                          | ✓ | f. Salary                                                          | ✓ | j. Proprietary or Business Information | ✓ |
| c. Work Address                       | ✓ | g. Work History                                                    | ✓ | k. Procurement / contracting records   | ✓ |
| d. Work Telephone Number              | ✓ | h. Employment Performance Ratings or other Performance Information | ✓ |                                        |   |
| l. Other work-related data (specify): |   |                                                                    |   |                                        |   |

| Distinguishing Features/Biometrics |   |                          |  |                   |   |
|------------------------------------|---|--------------------------|--|-------------------|---|
| a. Fingerprints                    | ✓ | f. Scars, Marks, Tattoos |  | k. Signatures     | ✓ |
| b. Palm Prints                     |   | g. Hair Color            |  | l. Vascular Scans |   |

| Distinguishing Features/Biometrics                     |   |              |  |                          |  |
|--------------------------------------------------------|---|--------------|--|--------------------------|--|
| c. Voice/Audio Recording                               | ✓ | h. Eye Color |  | m. DNA Sample or Profile |  |
| d. Video Recording                                     | ✓ | i. Height    |  | n. Retina/Iris Scans     |  |
| e. Photographs                                         | ✓ | j. Weight    |  | o. Dental Profile        |  |
| p. Other distinguishing features/biometrics (specify): |   |              |  |                          |  |

| System Administration/Audit Data                     |   |                        |   |                      |   |
|------------------------------------------------------|---|------------------------|---|----------------------|---|
| a. User ID                                           | ✓ | c. Date/Time of Access | ✓ | e. ID Files Accessed | ✓ |
| b. IP Address                                        | ✓ | f. Queries Run         | ✓ | f. Contents of Files | ✓ |
| g. Other system administration/audit data (specify): |   |                        |   |                      |   |

| Other Information (specify) |
|-----------------------------|
|                             |
|                             |

**c. Describe how the accuracy of the information in the system is ensured.**

Information is manually reviewed and updated through standardized scheduled and ad-hoc procedures specifically designed to improve enterprise data quality.

**d. Is the information covered by the Paperwork Reduction Act?**

|   |                                                                                                                                                                                                                                                                                                                                                                                                    |
|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ✓ | <p>Yes, the information is covered by the Paperwork Reduction Act.<br/> <i>Provide the OMB control number:</i></p> <p>OMB control number 3320-0003, Environmental Conflict Resolution Participant Questionnaires;<br/>           OMB control number 3320-0006, Training Services Participant Questionnaire;<br/>           OMB control number 3320-0011, Alumni Survey – Eligibility Criteria.</p> |
|   | No, the information is not covered by the Paperwork Reduction Act.                                                                                                                                                                                                                                                                                                                                 |

**e. Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. (Check all that apply.)**

| Technologies Used Containing PII/BII Not Previously Deployed |   |                                               |   |
|--------------------------------------------------------------|---|-----------------------------------------------|---|
| a. Smart Cards                                               |   | c. Biometrics                                 | ✓ |
| b. Caller-ID                                                 | ✓ | d. Personal Identity Verification (PIV) Cards | ✓ |

| Technologies Used Containing PII/BII Not Previously Deployed |                                                                                                          |
|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| e. Other (specify):                                          |                                                                                                          |
|                                                              | There are not any technologies used that contain PII/BII in ways that have not been previously deployed. |

### III. Information Collection Description

#### a. Identify the information the project collects, uses, disseminates, or maintains.

PII in the system is from Federal, State, and Local government employees and contractors, small businesses, Tribal entities, and members of the public. This information is collected so that the Udall Foundation can perform its mission and key administrative and operational activities. This information includes, but is not limited to, names, emails, social security numbers, credit card numbers, financial information, addresses, dates of birth, telephone numbers, medical information, military service, salary information, contracting and procurement records, photographs, video recordings, and signatures.

Users may create new information and records using the data on the system and in paper records. For example, annual reports about Education program award recipients are created using the information provided by applicants, as well as narrative information created by the Education program team. Employee information is also combined and processed in support of numerous administrative tasks like payroll.

There are two external systems that the IT system receives data from. The first system, Pay.gov, provides payment information through a secure, certificate-based web service to the Udall Foundation after users submit payment details for training registration. The second system, G-Invoicing, provides agreement and contract data through a secure, certificate-based web service. Both connections involve automated, encrypted exchanges of limited information that are used strictly for financial processing and program administration.

FD Online and Integrity are utilized by our employees on their government-issued devices; however, these platforms do not directly connect to the agency's system. Additionally, we leverage data from several external government systems—including GSA's financial systems, FedSEP, MSPB's appeal portal, GAO's appeal portal (EPDS), Sam.gov, Collect.gov, and Max.gov—to support our programmatic and administrative functions. These systems serve as sources from which relevant information is extracted and integrated into our workflows, ensuring compliance and operational efficiency.

#### b. What are the sources of the information and how is the information collected for

**the project?**

Sources of information are employees and users of the system who create, add, store, and upload information, as well as members of the public, organizations, and businesses who are submitting information to the agency. Users may upload information about themselves or other individuals (for example, contact information for a project partner). Information on the system may also come from other agencies, such as financial and personnel data and reports from the agency's payroll and HR shared service provider.

**c. Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.**

Information from commercial sources, contractors, and publicly available sources may be incorporated into the system when necessary for the agency to conduct its work. For example, publicly available points of contact for Federally recognized Tribes may be used to create email distribution lists, and data from contractors may be included if it supports program or administrative functions. Any materials generated from this information will be appropriately marked as PII or BII, as required, to ensure proper handling and compliance with agency policies.

**d. Privacy Impact Analysis: Related to Characterization of the Information**

**Privacy Risk:** The system collects a wide variety of PII/BII (e.g., SSNs, financial data, medical information, work records). Without explicit ties between each data type and the program's statutory mission, there is a risk of unclear justification for sensitive information and over-collection due to broad use across programs.

**Mitigation:** The agency's General Counsel advises program leadership on the applicable statutory or business need for different activities. The Senior Agency Official for Privacy (SAOP) is also a part of the review team for new projects and acquisitions so that they can be aware of what new PII or BII is being collected, if any, and the need for that information. Finally, the SAOP provides annual Privacy training to staff to clarify the need for purpose specification in the collection of PII/BII.

**Privacy Risk:** The system includes broad capabilities, shared drives, custom apps, and multiple COTS tools. This can lead to storing information longer than needed because many workflows rely on shared drives and creating documents that contain incidental or excessive PII.

**Mitigation:** Employees are required to complete a Privacy Impact Assessment prior to the collection of new PII or BII. As part of this assessment, the proposed data collection metrics are examined and the SAOP inquires with the users if they feel that the amount of PII or BII proposed for collection is excessive. Additionally, the

Issued: 9/23/2026

SAOP regularly reviews the system and physical records to determine if PII or other applicable records have been retained past their destruction date, and engages the records owners on their obligations.

**Privacy Risk:** The system will receive and store data from several sources, including employees, applicants for awards, Parks in Focus® participants and their parents or guardians, shared service providers, current and prospective contractors and vendors, employees of Federal and state agencies, and Tribal entities. This may lead to confusion about how individuals may update their information, and what will be done with their information.

**Mitigation:** Privacy notices will be provided to individuals who are giving their information, and the agency will post its PIAs and Systems of Records Notice on its public-facing website. These documents will reside on the agency's privacy page, which also provides individuals with contact information for the privacy program should they have a request related to their PII.

**Privacy Risk:** Because users rely on manual uploads and processes for storage of PII, as well as multiple contributors being responsible for accessing PII, there is a risk that this information may not be kept up to date or may become inaccurate.

**Mitigation:** As part of the annual privacy training, the SAOP reminds users of the need to keep PII/BII up to date and accurate, and reviews documents to ensure this is occurring. When completing PIAs for new collections, teams are also required to consider and document how they will ensure data quality of PII/BII and implement these procedures. Finally, the SAOP, in their role as Agency Records Official, oversees annual destruction of records that have reached their disposition dates to aid with the deletion and destruction of outdated PII/BII.

#### IV. Purpose of the System

Indicate why the PII/BII in the system is being collected, maintained, or disseminated. *(Check all that apply.)*

| Purpose                               |   |                                               |  |
|---------------------------------------|---|-----------------------------------------------|--|
| a. For a Computer Matching Program    |   | h. For administering human resources programs |  |
| b. For administrative matters         | ✓ | i. To promote information sharing initiatives |  |
| c. For litigation                     | ✓ | j. For criminal law enforcement activities    |  |
| d. For civil enforcement activities   |   | k. For intelligence activities                |  |
| e. To improve Federal services online | ✓ | l. For employee or customer satisfaction      |  |
| f. For web measurement and            |   | m. For web measurement and                    |  |

| <b>Purpose</b>                              |   |                                               |   |
|---------------------------------------------|---|-----------------------------------------------|---|
| customization technologies (single-session) |   | customization technologies (multi-session)    |   |
| g. For Education Program administration     | ✓ | n. For National Center Program administration | ✓ |
| o. Other (specify):                         |   |                                               |   |

**Analysis:**

To perform its mission, the agency must collect and use a variety of PII/BII. This includes data that are necessary for the agency to meet its mission and statutory obligations (for example, personal information from scholarship applicants and agreement information for various conflict resolution services). Additionally, the agency must also collect data to ensure its administrative functions can be performed; these functions include, but are not limited to, acquisitions, finance and payroll, human resources management, operations, and information technology. The agency utilizes category labeling software to appropriately label PII/BII based on keywords.

**V. Use of the Information**

The system collects, maintains, and disseminates PII/BII so the Udall Foundation can perform its mission, administer its programs, and carry out essential administrative and operational functions. The information supports multiple functional areas within the agency, including Education programs, National Center program activities, conflict resolution services, finance and payroll, human resources, IT operations, and general agency administration.

Internally, information such as names, email addresses, dates of birth, contact information, education history, photographs, video recordings, signatures, contracting and procurement records, salary information, work history, and other personal and business data are used by agency staff to carry out programmatic and administrative responsibilities. For example, program managers use participant names and email addresses to schedule meetings, distribute documents, assemble project contact lists, and generate reports or other deliverables. Employee information is also combined and processed to support payroll and other HR activities. Records stored within designated project folders are used by specific teams with a need to know, enabling coordination, communication, and the creation of new work products based on collected information.

Information may also come from external partners and may be used to support administrative workflows such as financial processing, personnel management, and compliance reporting. Information from publicly available sources supports program communication and outreach. Information maintained and uploaded by users may also support operational tasks including IT management, system monitoring, and maintaining audit logs for user access.

If Social Security numbers are collected, they are used only when necessary to support administrative processes such as payroll, financial reimbursement or payment, tax reporting, or

Issued: 9/23/2026

verification activities. Only the minimum necessary SSN data is used for these statutory or administrative requirements.

**a. How does the project ensure that the information is used in accordance with stated practices in this PIA?**

The Udall Foundation ensures that information within the system is used in accordance with stated practices through multiple technical, administrative, physical, and policy safeguards. System auditing and logging tools track user activity, including logins, access to project folders, and modifications to records, enabling the agency to identify which users accessed which files and whether the access was appropriate. Role-based access controls limit users to the information necessary for their job duties, with some users granted read-only permissions while others may edit or upload records. Access is granted only after supervisor and system owner approval through the IT-managed access process, and permissions are continuously monitored by IT staff who perform diagnostics, patching, and vulnerability mitigation. Physical records that contain PII/BII are maintained by responsible employees in locked filing cabinets, and access into the offices is controlled.

The Udall Foundation conducts internal reviews of system activity and may request independent audits as needed to ensure compliance with privacy and security requirements. Automated monitoring tools within the system help identify potentially inappropriate access or unusual activity, prompting IT or supervisory review when necessary. These combined controls—auditing, defined roles, access restrictions, and automated monitoring—ensure that PII/BII is handled only in ways consistent with approved uses and privacy protections. The Udall Foundation also conducts regular physical inspections to ensure paper records are appropriately secured.

**b. Retention Requirements**

The information in the system is retained only for as long as required by the applicable General Records Schedule or Agency Records Schedule, or until the business need for the information ceases, ensuring the agency retains the minimum amount of PII or BII necessary to meet programmatic and administrative requirements. Project-specific PII, such as contact lists, is held throughout the life of the project and until no longer needed for program operations, after which it is securely deleted in accordance with the approved disposition instructions. Administrative, financial, HR, and other statutory records are maintained for the retention periods mandated by NARA-approved schedules, and only the specific data elements needed to accomplish the original purpose of the collection are retained. At the end of the retention period or business need, all records are disposed of using secure, approved destruction methods that align with federal records management and privacy requirements.

If the agency intends to collect and retain contact information for a recurring email distribution list—such as National Center training or alumni communications—the distribution list can be retained as long as it is necessary for program or agency operations and will be managed according to approved records schedules. If the distribution list is created for a discrete activity, it should be deleted once the activity concludes and the information is no longer needed. In all cases, retention and disposition of contact information must comply with the applicable General Records Schedule or Agency Records Schedule, and any new collection or use outside the scope of the current PIA may require a separate assessment.

**c. Privacy Impact Analysis: Related to the Uses of Information**

**Privacy Risk:** Because the system relies on shared drives, multiple applications, physical storage, and manual uploads, there is a risk that information could be accessed or used in ways that exceed approved purposes, particularly if users are not fully aware of appropriate handling requirements or if access is not tightly aligned to job duties.

**Mitigation:** The Udall Foundation implements multiple controls to ensure information is handled only in accordance with approved uses, including annual privacy training that reinforces proper handling of PII/BII, role-based access restrictions that limit users to the information needed for their responsibilities, and IT-managed access approvals requiring supervisor and system owner authorization. System auditing tools track logins, file access, and modifications, allowing the agency to identify specific records accessed by each user and detect potential misuse. The Udall Foundation conducts internal reviews and uses automated monitoring tools within the system to alert IT staff to unusual or potentially inappropriate activity. Together, these safeguards support transparency, ensure information is used only for mission-relevant purposes, and allow the agency to restrict or revoke access if improper use is detected.

**VI. Information Sharing and Access**

Indicate with whom the Udall Foundation intends to share the PII/BII in the system and how the PII/BII will be shared. *(Check all that apply.)*

| Recipient                        | <i>How Information will be Shared</i> |               |               |
|----------------------------------|---------------------------------------|---------------|---------------|
|                                  | Case-by-Case                          | Bulk Transfer | Direct Access |
| a. Within the Udall Foundation   | ✓                                     |               | ✓             |
| b. Federal agencies              | ✓                                     |               | ✓             |
| c. State, local, tribal entities | ✓                                     |               |               |
| d. Public                        | ✓                                     |               |               |
| e. Private sector                | ✓                                     |               |               |
| f. Foreign governments           |                                       |               |               |
| g. Foreign entities              |                                       |               |               |
| h. Other (specify):              |                                       |               |               |

| Recipient | <i>How Information will be Shared</i>         |               |               |
|-----------|-----------------------------------------------|---------------|---------------|
|           | Case-by-Case                                  | Bulk Transfer | Direct Access |
|           | The PII/BII in the system will not be shared. |               |               |

Within the Udall Foundation, PII/BII stored in the system may be shared with agency staff who require access to perform programmatic or administrative duties. This includes agency leadership, Education and National Center program personnel, Operations and Finance personnel, information technology contractors, and other employees or contractors with a demonstrated need to know. Information is accessed through permission-based shared drives, custom applications, and Microsoft 365 GCC, with specific access granted only after supervisor and system owner approval through the IT-managed access process. Paper records are accessed via locked filing cabinets with the record owner providing access after a need to know has been verified. Internally, users rely on this information to coordinate program activities, schedule meetings, distribute documents, generate reports, manage payroll and personnel records, process financial transactions, and perform essential operational tasks, with access restricted by defined roles—such as read-only or full editing permissions—to ensure information is used appropriately.

Outside the Udall Foundation, information may be shared as part of normal agency operations with federal agencies, state and local government entities, Tribal entities, and partner organizations when needed to support financial processing, HR services, compliance reporting, program coordination, or collaboration related to Education and National Center program activities. Examples include sharing financial or personnel information with the agency's federal financial services and HR shared service provider. External partners access this information only as necessary to fulfill their operational role, and sharing is limited to the minimum amount of data required for specific purposes. No foreign governments are identified as recipients in the current system description, and external disclosures are conducted in accordance with applicable records schedules, privacy requirements, and the routine uses associated with agency operations.

In cases where a need to know cannot be established, employees will contact their supervisor and the SAOP for further clarification. If the SAOP determines that the information can be shared, this disclosure will be appropriately documented.

**a. Does the Udall Foundation place a limitation on re-dissemination of PII/BII shared with external agencies/entities?**

|   |                                                                                                                         |
|---|-------------------------------------------------------------------------------------------------------------------------|
| ✓ | Yes, the external agency/entity is required to verify with the Udall Foundation before re- dissemination of PII/BII.    |
|   | No, the external agency/entity is not required to verify with the Udall Foundation before re- dissemination of PII/BII. |
|   | No, the Udall Foundation does not share PII/BII with external agencies/entities.                                        |

External sharing of PII/BII by the Udall Foundation is limited to the minimum necessary to support defined operational needs, and recipients are expected to use the information only for the stated purpose consistent with

applicable privacy requirements. If an external organization lacks a clear need-to-know, Udall Foundation employees consult their supervisor and the SAOP before any disclosure. Applicable agreements or contractual terms may include items related to confidentiality, use-limitation, and security obligations; access control procedures; and the Udall Foundation's auditing and monitoring processes that are used to help detect and respond to inappropriate external use.

**b. Indicate whether the system connects with or receives information from any other systems authorized to process or store PII and/or BII.**

|   |                                                                                                                                                                                                                                                                                                                                                       |
|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ✓ | <p>Yes, this system connects with or receives information from other system(s) authorized to process PII and/or BII.<br/>Provide the name of the system and describe the technical controls which prevent PII/BII leakage:</p> <p>Pay.gov and G-invoicing. A secure, certificate-based web service transmits the data to prevent PII/BII leakage.</p> |
|   | No, this system does not connect with or receive information from other system(s) authorized to process PII and/or BII.                                                                                                                                                                                                                               |

**c. Identify the class of users who will have access to the system and the PII/BII. (Check all that apply)**

| Class of Users                            |   |                         |   |
|-------------------------------------------|---|-------------------------|---|
| a. General Public                         |   | c. Government Employees | ✓ |
| b. Contractors                            | ✓ |                         |   |
| d. Other (specify): Partner organizations |   |                         |   |

**Analysis:** Access to the system and its data is limited to government employees, contractors, and partner organizations with no general-public system access. Within the Udall Foundation, users are granted access strictly on a need-to-know basis, and permissions and access are assigned through a managed access process that requires supervisor and system owner approval. Role-based controls restrict users to only the information necessary for their duties, including read-only or editing rights depending on job requirements, while contractors operating under confidentiality and security provisions in their agreements are permitted access only to the data required for their contracted work. Access for partner organizations is strictly limited and governed by established protocols; only authorized individuals are granted access to system data, and distribution lists or similar resources are shared externally solely when necessary for programmatic purposes and in accordance with privacy and security requirements. These measures help ensure that information is used solely for mission-aligned purposes and in accordance with privacy requirements.

**d. Privacy Impact Analysis: Related to Information Sharing and Access**

**Privacy Risk:** Sharing information across multiple functional areas inside the Udall Foundation—particularly through shared drives and manual uploads—creates a risk that users may access or use PII/BII beyond what is necessary for their job duties.

**Mitigation:** Role-based access controls restrict users to the minimum information needed for their responsibilities, and access is granted only after supervisor and system owner approval through the managed access process. System audit logs track which users access specific folders and records, and IT staff regularly review logs and perform continuous monitoring to identify unusual or inappropriate use. Annual privacy training reinforces proper handling requirements, and access can be revoked if improper use is detected. Users also sign the agency’s Acceptable Use Policy prior to being granted access.

**Privacy Risk:** External sharing with federal shared service providers, state or local government entities, Tribal entities, or other entities introduces the risk that information may be re-disseminated without authorization or used for purposes inconsistent with the original collection.

**Mitigation:** External disclosures are limited to the minimum data necessary to support operational needs, and when a clear need-to-know cannot be established, employees consult their supervisor and the SAOP before sharing. Agreements or contractual terms with external entities may include confidentiality, use-limitation, access-control, and security requirements to ensure appropriate handling. Privacy notices are also added to documents as appropriate so that recipients are aware of the limitations of use associated with the PII or BII.

**VII. Notice and Consent**

Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

|   |                                                                                                                                                   |                                                                                    |
|---|---------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| ✓ | Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section IX below.               |                                                                                    |
| ✓ | Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: _____. |                                                                                    |
| ✓ | Yes, notice is provided by other means.                                                                                                           | Specify how: Website text prior to submitting application information in a portal. |
|   | No, notice is not provided.                                                                                                                       | Specify why not:                                                                   |

Indicate whether and how individuals have an opportunity to decline to provide PII/BII. For example, if the collection is voluntary, they can decline to provide PII/BII by not submitting any information at all (e.g., voluntary surveys, applications for scholarships).

Issued: 9/23/2026

|   |                                                                           |                                                                                                                        |
|---|---------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| ✓ | Yes, individuals have an opportunity to decline to provide PII/BII.       | Specify how: Individuals may decline by not proceeding with the information collection (application, evaluation, etc.) |
|   | No, individuals do not have an opportunity to decline to provide PII/BII. | Specify why not:                                                                                                       |

Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

|   |                                                                                            |                                                                                                                                      |
|---|--------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
|   | Yes, individuals have an opportunity to consent to particular uses of their PII/BII.       | Specify how:                                                                                                                         |
| ✓ | No, individuals do not have an opportunity to consent to particular uses of their PII/BII. | Specify why not: All data elements are required to process the information collection, so consent must be given to all defined uses. |

Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

|   |                                                                                         |                                                                                                                                                                                                   |
|---|-----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ✓ | Yes, individuals have an opportunity to review/update PII/BII pertaining to them.       | Specify how: Information contained in contact lists is regularly verified with individuals for accuracy. Individuals may also re-submit their data and employees will update records accordingly. |
|   | No, individuals do not have an opportunity to review/update PII/BII pertaining to them. | Specify why not:                                                                                                                                                                                  |

**Analysis:** Notice for the system is provided through Privacy Act statements, website text presented prior to submitting information in online portals, and other program-specific notices, ensuring individuals understand why their information is collected and how it will be used. Individuals who voluntarily submit information—such as Scholarship applicants and National Center project participants—may decline to provide PII/BII by choosing not to proceed with the collection, and consent to all defined uses is inherent in completing required forms because each data element is necessary to process the application or administrative transaction. The Udall Foundation also posts its PIAs and Systems of Records Notices on its public website to promote transparency and inform individuals of their rights and the purpose of each collection. Individuals can review and update their information when it is used in contact lists or other program records, and may re-submit corrected information or work directly with agency staff to update their records. Individuals may also request correction of data pursuant to the agency's Privacy Act regulations at 36 CFR Part 1600, Subpart B. These combined approaches ensure individuals receive clear notice, understand how their information will be used, and have an avenue to correct inaccuracies when needed.

**a. Privacy Impact Analysis: Related to Notice**

**Privacy Risk:** Notice may be inconsistent across different collection channels (e.g., program application portals, forms, and administrative workflows), which could reduce transparency about why information is collected, how it will be used, and how individuals can correct their records.

**Mitigation:** The Udall Foundation provides Privacy Act statements and website notices prior to submission, posts PIAs and applicable Systems of Records Notices on its public site, and offers clear avenues for individuals to review and update information (e.g., verification of contact lists and re-submission of corrected data); annual privacy training and SAOP involvement in new projects reinforce consistent, program-specific notice language. All Privacy Act statements are drafted with the assistance of the General Counsel, which will increase consistency across collection channels and notices.

**Privacy Risk:** Information could be used beyond the purposes stated in the initial notice, especially given shared drives, manual uploads, and broad system capabilities, which may blur the link between collection and mission-aligned use.

**Mitigation:** Use-limitation is enforced through role-based access controls, physical safeguards, supervisor and system owner approvals, audit logging of file access/modifications, automated monitoring for unusual activity, and policies that restrict external sharing to the minimum necessary with documented SAOP review when need-to-know is unclear; retention and destruction practices further limit use beyond the original purpose

**b. Privacy Impact Analysis: Related to Redress**

**Privacy Risk:** Individuals may not always have a direct means to access or correct information about themselves, particularly when data originates from external systems such as payroll or HR shared service providers, or when PII is uploaded by staff as part of program operations (e.g., contact lists, project documentation). This may result in outdated or inaccurate information remaining in the system.

**Mitigation:** The Udall Foundation provides clear avenues for individuals to review and update their information and contact information for the privacy program is on the agency's website. Privacy notices, PIAs, and Systems of Records Notices posted on the agency's website inform individuals of how to request corrections or raise concerns, and annual privacy training reinforces staff responsibilities for data accuracy and proper handling of updated information.

**Privacy Risk:** Individuals may be unaware when their information is used for multiple operational purposes (e.g., program administration, financial processing, HR transactions), creating a risk that information collected for one purpose may be used for another without the individual's knowledge.

**Mitigation:** Use-limitation principles are applied through role-based access controls, physical safeguards, supervisor and system owner approval processes, and detailed notice provided at the point of collection through Privacy Act statements or

program-specific instructions. These notices explain the purpose of the collection and how the information will be used, and the agency's privacy page provides information on redress mechanisms, ensuring individuals understand both the intended use of their data and how to challenge or correct records if necessary.

### VIII. Administrative and Technological Controls

Indicate the administrative and technological controls for the system. *(Check all that apply.)*

|   |                                                                                                                                                                                                                                                                                                                                 |
|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | a. All users signed a confidentiality agreement or non-disclosure agreement.                                                                                                                                                                                                                                                    |
|   | b. All users are subject to a Code of Conduct that includes the requirement for confidentiality.                                                                                                                                                                                                                                |
| ✓ | c. Staff (employees and contractors) received training on privacy and confidentiality policies and practices.                                                                                                                                                                                                                   |
| ✓ | d. Access to the PII/BII is restricted to authorized personnel only.                                                                                                                                                                                                                                                            |
| ✓ | e. Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Current agency logging and continuous monitoring activities monitors, tracks, and records user activity across the system.                                                                                                                      |
| ✓ | f. A security risk assessment has been conducted.                                                                                                                                                                                                                                                                               |
| ✓ | g. The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.<br>Provide date of most recent Assessment and Authorization (A&A): <u>4/16/2026</u><br><input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved. |
| ✓ | h. The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.                                                                                                                                                                                                     |
| ✓ | i. NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).                                                                                     |
| ✓ | j. A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.                                                                                                                                                                             |
| ✓ | k. Contractors that have access to the system are subject to information security provisions in their contracts required by Udall Foundation policy.                                                                                                                                                                            |
|   | l. Other (specify):                                                                                                                                                                                                                                                                                                             |

***Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.***

The Udall Foundation protects privacy and data in the system through layered access controls and administrative safeguards aligned to a strict need-to-know principle. Access to folders, applications, and records is permission-based and granted only after supervisor and system owner approval through the IT-managed access process; users are assigned role-based permissions (such as read-only or edit/upload) that limit them to the minimum information required for their job duties. Accounts are provisioned solely for Udall Foundation employees and contractors—guest accounts

Issued: 9/23/2026

are not used—and users must accept the agency’s Acceptable Use Policy before access is granted. The system employs multiple layers of authentication and security, and connections occur from government-furnished equipment, further reducing the risk of unauthorized access. Physical records are safeguarded through physical access controls, including limited office access and filing cabinets.

Technical controls emphasize prevention, detection, and response. The IT team conducts continuous diagnostics and monitoring, maintains comprehensive audit logging of user logins, file/folder access, and record modifications, and performs ongoing patching and vulnerability mitigation to keep the IT infrastructure secure. Automated monitoring tools help detect unusual or potentially improper access, and audit logs enable the agency to identify which specific records each user accessed and whether such access was appropriate. The system and its subcomponents are categorized FISMA Moderate under FIPS 199, and the agency undergoes an annual FISMA audit, which independently evaluates the effectiveness of its security and privacy controls. These assessments help ensure that administrative, technical, and policy safeguards remain effective and aligned with federal security and privacy requirements.

**a. Provide a general description of the technologies used to protect PII/BII on the system. (Include data encryption in transit and/or at rest, if applicable).**

The system uses a combination of layered security technologies and controls to protect PII/BII, including full-disk and file-level encryption, secure remote access, and multifactor authentication. Encryption is used to protect information both in transit and at rest, ensuring that data remains unreadable if intercepted or accessed improperly, while secure remote-connection technologies safeguard communication channels when users access the system from government-furnished equipment. Multifactor authentication adds an additional protection layer by requiring multiple forms of verification before system access is granted, reducing the likelihood that compromised credentials alone could lead to unauthorized access. These protections work together with the system’s existing access controls, role-based permissions, and continuous monitoring to reduce the risk of unauthorized disclosure and ensure that PII/BII is handled in accordance with federal privacy and security requirements.

**b. Indicate IT system supported activities which raise privacy risks/concerns. (Check all that apply)**

| Activities                                                                           |                          |                                     |                                     |
|--------------------------------------------------------------------------------------|--------------------------|-------------------------------------|-------------------------------------|
| a. Audio recordings                                                                  | <input type="checkbox"/> | c. Building entry readers           | <input checked="" type="checkbox"/> |
| b. Video surveillance                                                                | <input type="checkbox"/> | d. Electronic purchase transactions | <input checked="" type="checkbox"/> |
| e. Other (specify):                                                                  |                          |                                     |                                     |
| There are not any IT system supported activities which raise privacy risks/concerns. |                          |                                     |                                     |

**d. Privacy Impact Analysis: Related to Administrative and Technological Controls**

**Privacy Risk:** Because the system relies on multiple contributors, shared drives, manual uploads, and a hybrid IT environment, there is a risk that PII/BII could be accessed or stored in locations that are not properly restricted, increasing the likelihood of unauthorized access or accidental disclosure.

**Mitigation:** The Udall Foundation uses layered administrative and technological controls to limit this risk, including role-based access controls, supervisor and system owner approval for folder and system access, and multiple authentication requirements. Continuous monitoring, audit logging, and regular review of access records enable the agency to identify inappropriate access, while annual privacy training and enforcement of the Acceptable Use Policy reinforce proper handling and storage practices. The Foundation also uses physical access controls to limit who has access to the office and physical records.

## IX. Privacy Act

Is the PII/BII searchable by a personal identifier (e.g., name or Social Security number)?

- ☒ Yes, the PII/BII is searchable by a personal identifier.  
☐ No, the PII/BII is not searchable by a personal identifier.

- a. **Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a.** *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

The Privacy Act of 1974, defines the term “system of records” means “a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.” 5 U.S.C. § 552a(a)(5).

|   |                                                                                                                                                    |
|---|----------------------------------------------------------------------------------------------------------------------------------------------------|
|   | Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i> |
| ✓ | Yes, a SORN is required and will be submitted to the SAOP on or before December 31, 2026.                                                          |
|   | No, this system is not a system of records and a SORN is not applicable.                                                                           |

**Analysis:** Information in the system about United States citizens and lawfully admitted permanent residents is retrieved by personal identifiers such as name, email address, date of birth, Social Security number (when required for payroll or tax purposes), or other identifying information maintained in program records, administrative files, or project documentation. Because the system stores PII/BII in shared drives, custom applications, Microsoft 365 GCC, and other system components, authorized users retrieve records through permission-based access aligned with their job duties, such as locating participant information for Education

awards or National Center projects, accessing employee data for HR and payroll activities, or reviewing contact lists for project coordination. Retrieval occurs only by users with approved access and is conducted for mission-aligned purposes, and the Udall Foundation has determined that the system constitutes a system of records; therefore, a SORN is required and will be submitted to the SAOP on or before December 31, 2026.

## X. Retention of Information

Indicate whether these records are covered by an approved records retention schedule and monitored for compliance. *(Check all that apply.)*

|   |                                                                                                                                                                       |
|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ✓ | There is an approved record retention schedule.<br>Provide the name of the record retention schedule: General Records Schedule and Udall Foundation Records Schedule. |
|   | No, there is not an approved record retention schedule.<br>Provide the stage in which the project is in developing and submitting a records retention schedule:       |
| ✓ | Yes, retention is monitored for compliance to the schedule.                                                                                                           |
|   | No, retention is not monitored for compliance to the schedule.<br>Provide explanation:                                                                                |

### a. Indicate the disposal method of the PII/BII. *(Check all that apply)*

| Disposal            |   |                |   |
|---------------------|---|----------------|---|
| a. Shredding        | ✓ | c. Overwriting | ✓ |
| b. Degaussing       |   | d. Deleting    | ✓ |
| e. Other (specify): |   |                |   |

### b. Privacy Impact Analysis: Related to Retention

**Privacy Risk:** Because the system retains information for the duration required by the applicable records schedules or until business need ceases, there is a risk that PII/BII may be kept longer than is necessary for the specific purpose for which it was collected, increasing exposure to unauthorized access or unintended use.

**Mitigation:** The Udall Foundation mitigates this risk by strictly aligning retention practices with the General Records Schedule and the Agency Records Schedule, ensuring only the minimum information needed to fulfill mission-aligned purposes is maintained. Records are securely destroyed once retention periods and business needs end, and the SAOP regularly reviews records to ensure excessive or outdated PII/BII is not retained. Employees are instructed to store records containing PII/BII only in approved locations and not in personal folders unless the SAOP approves an exception.

**Privacy Risk:** Longer retention periods increase the likelihood that information becomes outdated, inaccurate, or incomplete, particularly given the system's reliance on manual uploads, shared drives, and multiple contributors. This may reduce data quality and affect program accuracy and administrative decision-making.

**Mitigation:** The Udall Foundation mitigates this risk through scheduled and ad-hoc data reviews, annual privacy training emphasizing data accuracy obligations, and standardized procedures for updating information. As records reach the end of their retention period or business need, they are securely destroyed, preventing the continued storage of stale or irrelevant PII/BII and supporting overall data integrity.

#### XI. NIST Special Publication 800-122 PII Confidentiality Impact Level

Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

|   |                                                                                                                                                                                                       |
|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.                 |
| ✓ | Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.            |
|   | High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |

Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

|   |                        |                                                                                                                                                                                                                                                               |
|---|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ✓ | Identifiability        | Provide explanation: The system stores highly identifying information—including names, dates of birth, email addresses, and, in limited cases, Social Security Numbers—which increases impact because many data elements can directly identify an individual. |
| ✓ | Quantity of PII        | Provide explanation: The system contains PII/BII for employees, contractors, applicants, award recipients, project partners, and others across multiple program areas.                                                                                        |
| ✓ | Data Field Sensitivity | Provide explanation: MKUSEF maintains sensitive data fields such as financial information, medical information, salary records, procurement records, and photographs or video recordings, which carry elevated impact if improperly accessed or disclosed.    |
| ✓ | Context of Use         | Provide explanation: The PII/BII supports mission-critical functions so misuse could directly affect individuals'                                                                                                                                             |

|   |                                       |                                                                                                                                                                                                                                                                                                                  |
|---|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   |                                       | benefits, employment, or participation in agency programs.                                                                                                                                                                                                                                                       |
| ✓ | Obligation to Protect Confidentiality | Provide explanation: Many data elements in the system are protected under federal requirements including the Privacy Act, FISMA, NIST standards, and NARA-approved records schedules.                                                                                                                            |
| ✓ | Access to and Location of PII         | Provide explanation: PII/BII resides across shared drives, custom applications, physical and virtual servers, and Microsoft 365 GCC, and although access is restricted by role and requires supervisor approval, the distributed storage environment increases the potential impact if any access control fails. |
|   | Other:                                | Provide explanation:                                                                                                                                                                                                                                                                                             |

## XII. Misc.

- a. Indicate whether project described in this PIA requires any business process changes.

|   |                                                                                           |
|---|-------------------------------------------------------------------------------------------|
|   | Yes, the project described in this PIA requires business process changes.<br>Explanation: |
| ✓ | No, the project described in this PIA does not require any business process changes.      |

- b. Indicate whether the project described in this PIA requires any technology changes.

|   |                                                                                     |
|---|-------------------------------------------------------------------------------------|
|   | Yes, the project described in this PIA requires technology changes.<br>Explanation: |
| ✓ | No, the project described in this PIA does not require any technology changes.      |

- c. Describe what privacy training is provided to users either generally or specifically relevant to the project.

The SAOP provides real-time (in person and virtual) privacy training annually to all employees, and new employees receive new hire privacy training within the first 90 days of their employment. Both trainings cover key themes from the Privacy Act and E-Government Act, as well as the Federal Information Security and Modernization Act. Contractors who have access to the system are also given training by the SAOP. The SAOP tracks training completion for all employees and contractors who have access to the system, and maintains these records to demonstrate training compliance.

**d. What procedures are in place to determine which users may access the information and how does the project determine who has access?**

Access to information in the system is controlled through a formal, role-based authorization process that requires both supervisor approval and system owner approval before a user is granted access to electronic records. Access to physical records is controlled through physical access controls including fobs and keys. Udal Foundation employees and contractors receive only the minimum level of access needed for their responsibilities. Remote system access is permitted only through secure, encrypted connections and requires multifactor authentication to ensure that data transmission and storage remain protected from unauthorized access. All users are trained on proper handling, storage, and protection of PII/BII, and the agency's internal intranet provides a PII handbook and additional privacy and security guidance to reinforce these requirements and help ensure information is accessed and used appropriately.