US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/30/2025

OPDIV:

NIH

Name:

Division of Communication and Outreach (DCO) System

PIA Unique Identifier:

P-7882826-366564

The subject of this PIA is which of the following?

Minor Application (child)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

No

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

The National Institutes of Health (NIH) Office of the Director (OD) Office of Extramural Research (OER) Division of Communications and Outreach (DCO) provides support and services for OER communications with extramural research community. DCO accomplishes that via software and services, including third party resources (web services/sites), that are used for and not limited to website and application development, communications, training, and information technology support.

All DCO systems and applications work independently of each other, with no interconnections. The DCO systems and applications are for internal use and no access or links to the software/services are made available to the public or NIH staff (with the exclusion of DCO staff).

Describe the type of information the system will collect, maintain (store), or share.

The system does not collect, maintain or share any type of sensitive PII. However, unique usernames and passwords are used to access some of DCO systems and applications.

DCO team members only can access these systems and applications, including third party applications. DCO systems and applications maintain their own privacy risk assessments. The third-party applications are covered by vendor privacy policy and agreement.

Users log in to some DCO systems and applications using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, including all legal authorities documented. The purpose of IAM Services is to authenticate and authorize all users and computers in a Windows domain type network; assigning and enforcing information security policies for all computers and installing or updating software. The IAM Services collect unique user credentials and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.

However, users log in to other systems and applications using unique username and password.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The NIH OD/OER/DCO provides support and services for OER communications with extramural research community. DCO accomplishes that via software and services, including third party resources (web services/sites), that are used for and not limited to website and application development, communications, training, and information technology support.

All DCO systems and applications work independently of each other, with no interconnections. The DCO systems and applications are for internal use and no access or links to the software/services are made available to the public or NIH staff (with the exclusion of DCO staff).

The system does not collect, maintain or share any type of sensitive PII. However, unique usernames and passwords are used to access some of DCO systems and applications.
DCO team members only can access these systems and applications, including third party applications. DCO systems and applications maintain their own privacy risk assessments. The third-party applications are covered by vendor privacy policy and agreement.

Users log in to some DCO systems and applications using the NIH IAM Services which maintains its own unique PIA on record, including all legal authorities documented. The purpose of IAM Services is to authenticate and authorize all users and computers in a Windows domain type network; assigning and enforcing information security policies for all computers and installing or updating software. The IAM Services collect unique user credentials and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.

However, users log in to other systems and applications using unique username and password.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Username and password

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees
Business Partner/Contacts (Federal/state/local agencies)

How many individuals' PII is in the system?

<100

For what primary purpose is the PII used?

The PII is solely used to gain access to the DCO System's applications.

Describe the secondary uses for which the PII will be used.

N/A

Identify legal authorities governing information use and disclosure specific to the system and program.

5 U.S.C. 552a, 15 U.S.C. Chapter 7, 40 U.S.C. Section 1441, 44 U.S.C. chapter 35

Are records on the system retrieved by one or more PII data elements?

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Within the OpDiv

Non-Government Sources

Other

Identify the OMB information collection approval number and expiration date

N/A. The system does not solicit information.

Is the PII shared with other organizations?

No

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Privacy notices/warnings are posted on NIH systems to users logging into government systems hosting NIH websites. Those systems can only be accessed by NIH authorized staff/personnel. The third-party applications are covered by vendor privacy policy and agreement.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

There is no option for users to opt-put of the collection of their PII. Users who opt out delivering their PII will not be able to access DCO's systems/applications.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

Systems and applications under DCO have their own privacy policy. Users are responsible for their own information. The systems and applications' privacy notices should explain how users will be contacted if there is a major change.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

Users can contact the system and application directly if they had concerns or believe their PII has been inappropriately used or obtained.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

The NIH information technology (IT) Privacy Program requires systems to implement privacy reviews and controls throughout the development life cycle, and to incorporate review of privacy controls into the annual assessment schedule of controls on all systems, networks and interconnected systems.

Identify who will have access to the PII in the system and the reason why they require access.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Only authorized NIH staff/personnel will have access to the systems and applications, including the third party tools.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Determinations are made based on role-based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

According to NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security awareness training. Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials.

Describe training system users receive (above and beyond general security and privacy awareness training).

N/A

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

Item 02-001: Official Case Files of Construction, Renovation, Endowment and Similar Grants. Cut off annually following completion of final grant-related activity that represents closing of the case file (e.g., project period ended). Destroy 20 years after cutoff (DAA)-0443-2013-0004-0001).

Item 02-002: Official case files of funded grants, unfunded grants, and award applications, appeals and litigation records. Cut off annually following completion of final grant-related activity that represents closing of the case file (DAA-0443-2013-0004-0002).

Item 02-003: Animal Welfare Assurance Files. Cut off annually following closing of the case file (DAA-0443-2013-0004-0003).

Item 02-004: Extramural program and grants management oversight records. : Cut off annually. Destroy 3 years after cutoff (DAA-0443-2013-0004-0004).

Item 02-005: Official Case Files of Applications and Awards, Appeals, and Litigation Records for Grants, Cooperative Agreements, and Other Transaction Activities. : Cut off annually following completion of final award-related activity that represents closing of the case file. Destroy 30 year(s) after cutoff (DAA-0443-2019-0008-0001).

Item 02-006: Peer Review Records. Cutoff at the end of the calendar year. Destroy records when 12 years old. Longer retention is authorized if required for business use (DAA-0443-2021-0001-0001).

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Physical Controls: The information technology (IT) hardware used to host protected information is located in a secured datacenter facility. The facility is only open to authorized personnel whose access is monitored by locking doors with badge readers for both ingress and egress. Each discrete ingress and egress event is logged. The facility is under 24-hour surveillance by facilities security for security and environmental hazards.

Technical Controls: IT hardware and software is segregated from default commodity public networks to prevent unauthorized or malicious access. Access controls lists and event logs are maintained and monitored to detect unauthorized, suspicious or malicious activity. Access lists are restricted to approved IT technical personnel. Two factor authentication must be used for access. File integrity and auditing software are employed on hardware.

Administrative Controls: All technical personnel who access IT systems which contain protected information have met background investigation criteria for Public Trust positions. All personnel have taken mandatory security and privacy training classes and annual refreshers. Administrative personnel accessing these systems use privileged and separate accounts for administrative access.