US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/28/2025

OPDIV:

NIH

Name:

Office of Portfolio Analysis Tools Suite

PIA Unique Identifier:

P-5288278-270946

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?

Yes

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 Office of Portfolio Analysis (OPA) Tools Suite are National Institutes of Health (NIH) tools developed to provide access to and analyze biomedical information. This system furthers the NIH and OPA's goal of accelerating biomedical research. It does so by providing access to improved methods of data-driven decision making to evaluate and prioritize current, as well as emerging, areas of research that will advance knowledge and improve human health. This suite includes a set of internal-only tools to support NIH staff and also contains three public-access tools: World RePORT, iCite, and the CoronaVirus Disease 2019 (COVID-19) module.

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

The Office of Portfolio Analysis (OPA) Tools Suite contains awarded grants, grant applications, publications, clinical trial and patent information. The tools suite contains the following Personally Identifiable Information (PII): Principal Investigator (PI) name, email and research/funding affiliation. Grant application information is available to NIH extramural staff who have been approved by their IC (Institutes and Centers) coordinator for access to the data. All other data sources are available

through public forums inside and outside of NIH.

Users log in to this system 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.

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

The Office of Portfolio Analysis (OPA) Tools Suite are National Institutes of Health (NIH) tools developed to provide access to and analyze biomedical information. This system furthers the NIH and OPA's goal of accelerating biomedical research. It does so by providing access to improved methods of data-driven decision making to evaluate and prioritize current, as well as emerging, areas of research that will advance knowledge and improve human health. This suite includes a set of internal-only tools to support NIH staff and also contains three public-access tools: World RePORT, iCite, and the CoronaVirus Disease 2019 (COVID-19) module.

The Office of Portfolio Analysis (OPA) Tools Suite contains awarded grants, grant applications, publications, clinical trial and patent information. The tools suite contains the following Personally Identifiable Information (PII): Principal Investigator (PI) name, email and research/funding affiliation. Grant application information is available to NIH extramural staff who have been approved by their IC (Institutes and Centers) coordinator for access to the data. All other data sources are available through public forums inside and outside of NIH.

Users log in to this system 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.

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

Yes

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

Name
E-Mail Address
Research/Funding affiliation

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

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

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

This information exists for end users to look up. This is public contact information published by authors and researchers in order to reach out to them about their work. The emails and addresses are public data related to their places of employment, and we are gathering them from other public sources, collating, and displaying them.

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

This information can be used as a tool to discern between two similar individuals when grouping their work.

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

5. U.S.C. 301; 42 U.S.C. 217a, 241,282(b)(6), 284a, and 288. 48 CFR Subpart 15.3 and Subpart 42.15.

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

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

09-25-0225, NIH Electronic Research Administration (eRA)

09–25–0036Extramural Awards and Chartered Advisory Committees (IMPAC 2),Contract Information

Identify the sources of PII in the system.

Government Sources

Within OpDiv

Foreign

Identify the Federal Sources

Media/Internet

Private Sector

Identify the OMB information collection approval number and expiration date

OMB # 0925-0001 Expiration Date:1/31/2026

OMB # 0925-0002 Expiration Date: 1/31/2026

OMB # 0925-0361 Expiration Date: 1/31/2026

OMB # 0925-0689 Expiration Date: 4/30/2025"

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

HHS affiliates must agree to terms of use and request an account individually.

Describe the procedures for accounting for disclosures.

There is currently no accounting for disclosures as these follow under the need to know exemption.

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

OPA Tools is not the source system. The source systems: eRA, PubMed, and ClinicalTrials.gov maintain their own processes for notification of individuals. All three maintain their own PIAs.

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.

OPA Tools is not the source system. The source systems: eRA, PubMed, and ClinicalTrials.gov maintain their own processes for opt-out options. All three maintain their own PIAs.

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

OPA Tools is not the source system. The source systems: eRA, PubMed, and ClinicalTrials.gov maintain their own processes for obtain consent when a major change occurs. All three maintain their own PIAs.

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.

OPA Tools is not the source system. The source systems: eRA, PubMed, and ClinicalTrials.gov maintain their own processes to resolve concerns for individuals PII. All three maintain their own PIAs.

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

OPA Tools is not the source system. The source systems: eRA, PubMed, and ClinicalTrials.gov maintain their own processes for periodic reviews of PII. All three maintain their own PIAs.

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.

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.

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).

NA

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 (DAA-0443-2013-0004-0001)
Official case files of construction, renovation, endowment and similar grants.
Disposition: Temporary. 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 cut-off;

Item 02-005 (DAA-0443-2019-0008)
Official Case Files of Applications and Awards, Appeals, and Litigation Records for Grants, Cooperative Agreements, and Other Transaction Activities
Disposition: Temporary. Cut off annually following completion of final award-related activity that represents closing of the case file (e.g., end of project period, completed final peer review, litigation or appeal proceeding concluded). Destroy 30 years after cut-off;

Item 02-003 (DAA-0443-2013-0004-0003)
Animal welfare assurance files.
Disposition: Temporary. Cut off annually following closing of the case file. Destroy 4 years after cut-off; and,

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

Item 04-401, Research Support for Certificates of Confidentiality - Support Documentation (DAA-0443-2017-0001-0001), Cut off annually at expiration of Certificate of Confidentiality. Destroy 6 years after cutoff.

Item 04-402, Research Support for Certificates of Confidentiality - Issued Certificates of Confidentiality (DAA-0443-2017-0001-0002), Cut off annually after all of the individually identifiable data from the research project have been destroyed, used, or otherwise are no long remaining in the NIH intramural program. Destroy 3 years after cutoff.

Item 04-403, Research Support for Certificates of Confidentiality - Issued Certificates of Confidentiality - For Extramural and Outside Research (DAA-0443-2017-0001-0003), Cut off annually at expiration of the Certificate of Confidentiality. Destroy 6 year(s) after cutoff.

Item 04-404, Research Support for Certificates of Confidentiality- Denied Certificates of Confidentiality (DAA-0443-2017-0001-0004),
Cut off annually at notification of denial. Destroy 3 year(s) after cutoff.

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

Administrative Controls: User access is set up and restricted based on least privilege and role based permissions. Access and permissions are approved by the system owner.

Technical Controls: Access to the system is restricted by NIH IAM. IAM authenticates and

authorizes 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.

Physical Controls: Access is managed through Amazon Web Services (AWS). AWS servers are maintained in an AWS Data Center. Access is restricted to areas specified by employee permissions. These permissions are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. Visitors of the data center are escorted by AWS personnel when in the building.

Identify the publicly-available URL:

https://worldreport.nih.gov
https://icite.od.nih.gov
https://covid19.opa-tools.od.nih.gov
Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

Yes

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

Yes