US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/03/2025

OPDIV:

NIH

Name:

NCI IMPAC II Extensions

PIA Unique Identifier:

P-7921344-187613

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.

Information for Management, Planning, Analysis, and Coordination (IMPAC) II EXTENSIONS (I2E) system is maintained, hosted, and supported by National Cancer Institute (NCI)’s Center for Biomedical Informatics and Information Technology (CBIIT). The system is a suite of modules that electronically track extramural grant applications from receipt, through peer review, approval, and the award of funds to researchers and organizations outside the National Institute of Health (NIH). I2E also integrates the NCI’s extramural grants process with the NIH’s eRA IMPAC II extramural grants process.

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

The system contains confidential grant application data, and serves the NCI Extramural Grants Management Community. The system contains the following types of personally Identifiable Information (PII): Name, Email Address, Phone Numbers, and Mailing Address. The PII is imported from two source systems. eRA (not an acronym) and the NIH Business Intelligence System (NBIS). Both eRA and NBIS maintain their own privacy impact assessments (PIA).

Users log in to this system using the NIH Identity, Credential, and Access Management (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. IAM Services collects unique user credentials and stores them in an encrypted format. 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.

Information for Management, Planning, Analysis, and Coordination (IMPAC) II EXTENSIONS (I2E) system is maintained, hosted, and supported by National Cancer Institute (NCI)'s Center for Biomedical Informatics and Information Technology (CBIIT). The system is a suite of modules that electronically track extramural grant applications from receipt, through peer review, approval, and the award of funds to researchers and organizations outside the National Institute of Health (NIH). I2E also integrates the NCI's extramural grants process with the NIH's eRA IMPAC II extramural grants process.

The system contains confidential grant application data, and serves the NCI Extramural Grants Management Community. The system contains the following types of personally Identifiable Information (PII): Name, Email Address, Phone Numbers, and Mailing Address. The PII is imported from two source systems. eRA (not an acronym) and the NIH Business Intelligence System (NBIS). Both eRA and NBIS maintain their own privacy impact assessments (PIA).

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. IAM Services collects unique user credentials and stores them in an encrypted format. 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
Mailing Address
Phone Numbers

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?

50,000-99,999

For what primary purpose is the PII used?

The system contains PII information on grantees and NCI staff involved that are involved in the grants business process and is used by NCI to perform grant management.

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

NA

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

Public Health Service Act. (42 U.S.C. 241, 242, 248, 281, 282, 284, 285a-285q, 287, 287b, 287c, 289a, 289c, and 44 U.S.C. 3101).

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, Electronic Research Administration

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

Identify the sources of PII in the system.

Government Sources

Other HHS OpDiv

Identify the OMB information collection approval number and expiration date

NA

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.

I2E is not the source system. eRA and NBIS, as the source systems, maintain their own PIAs, including processes to notify individuals that their PII will be collected.

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.

I2E is not the source system. eRA and NBIS, as the source systems, maintain their own PIAs, including opt-out processes.

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

I2E is not the source system. eRA and NBIS, as the source systems, maintain their own PIAs, including processes to notify and obtain consent when major changes occur to the source systems.

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.

I2E is not the source system. eRA and NBIS, as the source systems, maintain their own PIAs, including processes to resolve individual's concerns.

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

There is no process for periodic reviews. I2E is not the source system. eRA and NBIS, as the source systems, maintain their own PIAs, including processes for periodic reviews of PII.

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: The system owner reviews and approves access requests based on job functions and minimum access needed.

Technical Controls: Access to the system is controlled by NIH log-in which authenticates the user prior to granting access. Access level and permissions are controlled by the system and based on user, role, organizational unit, and status of the report. All servers have been configured to remove all unused applications and system files and all local account access except when necessary to manage the system and maintain integrity of data.

Physical Controls: The servers reside in the Center for Information Technology (CIT) Computer Room where policies and procedures are in place to restrict access to the machines. This includes guards at the front door and entrance to the machine room.