US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/05/2024

OPDIV:

NIH

Name:

Application Spaces Authorization Boundary

PIA Unique Identifier:

P-5277875-524122

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 Application Spaces Boundary is a lower level boundary that resides within the Monarch General Support System. It is used for applicants who are interested in applying for research training opportunities within National Institute of Allergy and Infectious Diseases (NIAID). Candidates use the systems to submit applications for a postdoctoral positions. It is also used to identify talented students from populations under-represented in the biomedical sciences in the under graduate community. Selected applicants participate in intramural Research training opportunities to gain experience and possible future employment.

The systems complement a separate application process that is maintained by NIAID Office of Research Training & Development (ORTD). Principal Investigators (PI) use these tools to easily access and search through submitted applications in order to contact and then accept candidates for their labs.

Application Spaces Authorization Boundary consists of the following system:

PostDoc and Intramural NIAID Research Opportunities (INRO) Program

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

During registration, applicants enter their personally identifiable information (PII): name, email address, phone number, Citizenship, resume, Associated University or College, Education Records, interested research areas, publications, training, presentations, awards and honors, leadership and outreach experiences as part of the process.

Applicants who are the external users use their own personal registered email on One Time Pin (OTP) system which produces a single use code to log into the external sites for the registration process.

This boundary uses specific login information for NIH users to assign permissions/user roles which is considered Personally Identifiable Information (PII). However, this is done by using the NIH Identity, Credential, and Access Management Services: Identity Management Services (IAM), formerly known as the Active Directory (AD), which combines the identity and authentication tools and capabilities used throughout the NIH enterprise. The IAM has its own approved PIA on record, including all legal authorities documented. 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, with 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 Application Spaces Boundary is a lower level boundary that resides within the Monarch General Support System. It is used for applicants who are interested in applying for research training opportunities within National Institute of Allergy and Infectious Diseases (NIAID). Candidates use the systems to submit applications for a postdoctoral positions. It is also used to identify talented students from populations under-represented in the biomedical sciences in the under graduate community. Selected applicants participate in intramural Research training opportunities to gain experience and possible future employment.

The systems complement a separate application process that is maintained by NIAID Office of Research Training & Development (ORTD). Principal Investigators (PI) use these tools to easily access and search through submitted applications in order to contact and then accept candidates for their labs.

Application Spaces Authorization Boundary consists of the following system:
PostDoc and Intramural NIAID Research Opportunities (INRO) Program .
During registration, applicants enter their personally identifiable information (PII): name, email address, phone number, Citizenship, resume, Associated University or College, Education Records, interested research areas, publications, training, presentations, awards and honors, leadership and outreach experiences as part of the process.

Applicants who are the external users use their own personal registered email on One Time Pin (OTP) system which produces a single use code to log into the external sites for the registration process.

This boundary uses specific login information for NIH users to assign permissions/user roles which is considered Personally Identifiable Information (PII). However, this is done by using the NIH Identity, Credential, and Access Management Services: Identity Management Services (IAM), formerly known

as the Active Directory (AD), which combines the identity and authentication tools and capabilities used throughout the NIH enterprise. The IAM has its own approved PIA on record, including all legal authorities documented. 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, with 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
Phone Numbers
Education Records
Citizenship
Interested research area for Disease/Medical Category
Associated University or College, Publications,
Resume, publications, trainings, awards and honors
leadership and outreach experiences

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

Public Citizens

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

The Personally Identifiable Information (PII) of applicants is used for the purpose of contacting the applicant during the selection process, or to resolve any outstanding question with regards to their application. In addition, the Principal Investigator (PI) may use PII to help determine eligibility, and to evaluate the academic background of the applicant for the purpose of selection consideration.

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

Not Applicable (N/A)

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

42 U.S.C. § 285f

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.

09–25–0158- Administration: Records of Applicants and Awardees of the NIH Intramural Research

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Non-Governmental Sources

Identify the OMB information collection approval number and expiration date

Public

NIH research activities are exempt from an OMB Information Collection Number through Public Law 114-255 - 21st Century Cures Act, Section 2035: Exemption for the National Institutes of Health from the Paperwork Reduction Act requirements.

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.

Users are notified via a welcome screen prior to creating an account to participate in the program for the purpose of selecting suitable candidates.

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 opt-out option. Individuals may decline to give their PII. However, in doing so, they will not be able to participate in the program.

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

A bulk email will be sent to all or select applicants by engaging the development team. Recipients details will be extracted from the system and shared with the coordinators for mass notification. Applicants can also contact the coordinators via email address located in the welcome page.

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 have two methods to contact the program team to resolve an individuals concerns, They can directly email the program coordinators from Office of Research Training & Development (ORTD) outside of the application, which they establish correspondence after the application process is completed or simply contact the program team via the support link located on the welcome page and work through the issues until resolved.

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

Periodic audits are conducted to ensure the data integrity, availability, accuracy and relevancy. The system produces reports for system administrators and stakeholders (coordinators) to review PII information every 6-12 months.

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.

Users, Administrators developers and contractors will be given different roles or access rights based on the task they need to perform. Access is reviewed and approved by the project managers or stakeholders who will determine who gets access to the PII data. In Addition, access is logged and periodic reviews performed for accuracy.

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.

NIH users authenticate using agency approved access management services: Identity Management Services (IAM). Once logged in, each user is a assigned a role based on their current job responsibilities. The Software Engineering Branch (SEB), system owner, and/or business owners has the ability to restrict data access via roles and limited to the functions and information that is essential to the job function.

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. There are five categories of mandatory IT training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Preparedness). 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).

Administrators and Privileged Users require additional Role Based training specific to their roles and responsibilities.

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

No

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

User records are retained and disposed of under the authority of the NIH Intramural Records Schedule, Item I-0003: Records of All Other Intramural Research Projects. These are temporary records, cut off annually at termination of project/program or when no longer needed for scientific reference, whichever is longer. Destroy 7 years after cutoff.
[Disposition Authority: DAA-0443-2012-0007-0003]

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

Administrative Controls: Annual security reviews are conducted for compliance of the security controls in place.

Technical Controls: Access to the system is controlled by NIH log-in and One Time Pin which authenticates the user prior to granting access. Access level and permissions are controlled by the system and based on user, role, organizational unit. All servers have been configured to remove all unused services and local account access except when necessary to manage the servers.

Physical Controls:
Information system is located in a FedRamp certified facility. Physical controls are assessed during certification.

Identify the publicly-available URL:

https://postdoc.niaid.nih.gov/
https://internal.postdoc.niaid.nih.gov/

https://inro.niaid.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?

No

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

null