US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/23/2025

OPDIV:

NIH

Name:

Specialized Scientific Jobs

PIA Unique Identifier:

P-8687115-877227

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 National Cancer Institute (NCI) system, Specialized Scientific Jobs System (SSJ), supports efficient and secure vacancy management. SSJ is designed to allow scientific candidates to apply for positions electronically thus eliminating the need to submit paper applications via the mail. The system supports reference check collection. SSJ also allows for search committee members to rate and rank candidates electronically thus eliminating the need for printing multiple copies of applications to distribute to committee members.

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

The application form requires that the candidate provide: email address, home phone, business phone, degree information, mailing address, and the names and contact information for a predefined number of references. Additionally, the applicant will upload his/her curriculum vitae (CV), bibliography, and qualification statement and vision statement. Reference letters for each candidate will also be collected and stored in the system for reviewers to access.

Applicants use email address and password to authenticate to the system, while NIH employees NIH Identity, Credential, and Access Management Services (IAM), which maintains its own unique PIA on record, with all legal authorities documented. The purpose of the IAM 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 collects unique user credentials and stores them in a encrypted format. The IAM is a 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 National Cancer Institute (NCI) system, Specialized Scientific Jobs System (SSJ), supports efficient and secure vacancy management. SSJ is designed to allow scientific candidates to apply for positions electronically thus eliminating the need to submit paper applications via the mail. The system supports reference check collection. SSJ also allows for search committee members to rate and rank candidates electronically thus eliminating the need for printing multiple copies of applications to distribute to committee members.

The application form requires that the candidate provide: email address, home phone, business phone, degree information, mailing address, and the names and contact information for a predefined number of references. Additionally, the applicant will upload his/her curriculum vitae (CV), bibliography, and qualification statement and vision statement. Reference letters for each candidate will also be collected and stored in the system for reviewers to access.

Applicants use email address and password to authenticate to the system, while NIH employees NIH Identity, Credential, and Access Management Services (IAM), which maintains its own unique PIA on record, with all legal authorities documented. The purpose of the IAM 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 collects unique user credentials and stores them in a encrypted format. The IAM is a 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
Education Records
Names and contact information of references
Resumes/CVs/supporting documents from applicants
Letters of Recommendation from references
Applicant email address and password for authentication

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

Employees
Public Citizens

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

The Personally Identifiable Information (PII) is used primarily to contact candidates. The CV and the letters of recommendations are used to determine qualification of applicants.

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.

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.

SORN OPM/GOV-5 Recruiting, Examining and Placement Records

SORN 09-25-0114 Clinical Research Student Records

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Within the OD

Non-Government Sources

Public

Identify the OMB information collection approval number and expiration date

0925-0761

07/31/2025

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.

There is a Privacy Act-compatible Notice on the website. Each applicant is notified of information practices at NIH during the hiring process.

NCI is currently working to add System of Records Notice 09-25-0114 to the Privacy Act Statement.

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. PII collected is for candidate contact information only. Without collecting this data, we will not be able to contact candidates to provide updates on the status of their applications, contact for interviews, etc.

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

All applicants will be contacted via email if major changes occur to disclosure and/or data uses.

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.

Individuals may contact the application administrator via email to discuss concerns pertaining to PII.

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 not a periodic review of the PII data. The data is only used when NCI is filing a current job vacancy and is destroyed 2 years after the job opening has closed.

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.

Administrators and users may access PII. If an issue occurs in production, developers/contractors may need to gain access to the system containing PII to troubleshoot the issue.

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.

Users in specific positions are allowed to access applicant PII only if they have been given access by the administrator. Developers/Contractors may be given temporary access by the administrator to troubleshoot issues that occur in production.

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.

The NIH Security Awareness Training course is used to satisfy this requirement. 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.

NIH Records Retention Schedule – 06-112, Interview records -Human Resources-Employee Acquisition Records. Destroy 2 years after case is closed by hire or non-selection, expiration of right to appeal a non-selection, or final settlement of any associated litigation, whichever is later (DAA-GRS-2014-0002-0008).

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

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..

Technical Controls: Access to the system is controlled by NIH IAM (for internal NCI users), which authenticates the user prior to granting access. External applicants will also log in with a unique email address and password. Access level and permissions are controlled by the system and based on user, role, and organizational unit. 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.

Physical Controls: The information technology (IT) hardware used to host protected information is 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 facility security for security and environmental hazards.

Identify the publicly-available URL:

https://specializedscientificjobs.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?

No

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