Save

Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-17302 | Form Date: 10/10/2019 1:00:30 PM

	Question	Answer
1	OPDIV:	NIH
2	PIA Unique Identifier:	P-5029624-466843
2a	Name:	Graduate Student Recruitment Program Application System
3	The subject of this PIA is which of the following?	○ General Support System (GSS) ○ Major Application ◉ Minor Application (stand-alone) ○ Minor Application (child) ○ Electronic Information Collection ○ Unknown
3a	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
3b	Is this a FISMA-Reportable system?	○ Yes ◉ No
4	Does the system include a Website or online application available to and for the use of the general public?	◉ Yes ○ No
5	Identify the operator.	○ Agency ◉ Contractor
6	Point of Contact (POC):	POC Title: Chief Intramural Diversity Workforce Branch POC Name: Dr. Ofelia Olivero POC Organization: NCI Center for Cancer Training POC Email: oliveroo@dc37a.nci.nih.gov POC Phone: 240-276-6890
7	Is this a new or existing system?	◉ New ○ Existing
8	Does the system have Security Authorization (SA)?	◉ Yes ○ No
8a	Date of Security Authorization	Jul 23, 2019

Save

11	Describe the purpose of the system.	The Graduate Student Recruitment Program (GSRP) Application System is a web-based application used by the National Cancer Institute (NCI) Center for Cancer Training (CCT) and run by Information Management Systems Inc, a third party contractor. It is designed to allow application to the NCI Graduate Student Recruiting Program and evaluation of these applications.
12	Describe the type of information the system will collect, maintain (store), or share. (Subsequent questions will identify if this information is PII and ask about the specific data elements.)	Information collected and stored in the GSRP Application System includes the following. Applicant information: • Name • Address (Home, School) • Phone • E-mail • Gender • Race/Ethnicity • Date of Birth • Place of Birth • Citizenship • Current Visa Status • Education (degree, month/year awarded/expected, major, minor, university) • Unofficial Transcripts • Personal Statement of Research and Career Goals • Curriculum Vitae • Research Topic, Research Target, Research Approach • Abstract • How applicant heard about the GSRP • Permission to make application available to NCI investigators if not invited to the event Referee information: • Name • Institution • Job Title • Position/Role (e.g. dissertation advisor) • Address • Phone • E-mail • Letter of recommendation for applicant • Date that Advisor expects applicant will receive PhD • Reason Advisor disagrees with applicant over date PhD degree is expected Reviewer, NCI Principal Investigator, and Administrator Information: • Name • Degrees • Employer • Position Title • Address • Phone • E-mail • Research Topic, Research Target, Research Approach (reviewer only)

Save

13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The GSRP Application System is a web-based application used by the NCI Center for Cancer Training (CCT) and run by Information Management Systems Inc, a third party contractor.
14	Does the system collect, maintain, use or share **PII**?	(•) Yes ( ) No
15	Indicate the type of PII that the system will collect or maintain.	☐ Social Security Number ☒ Date of Birth ☒ Name ☐ Photographic Identifiers ☐ Driver's License Number ☐ Biometric Identifiers ☐ Mother's Maiden Name ☐ Vehicle Identifiers ☒ E-Mail Address ☒ Mailing Address ☒ Phone Numbers ☐ Medical Records Number ☐ Medical Notes ☐ Financial Account Info ☐ Certificates ☐ Legal Documents ☒ Education Records ☐ Device Identifiers ☐ Military Status ☐ Employment Status ☐ Foreign Activities ☐ Passport Number ☐ Taxpayer ID Education History Demographics Curriculum Vitae Letters of Recommendation Personal Statement, Research Interests
16	Indicate the categories of individuals about whom PII is collected, maintained or shared.	☒ Employees ☒ Public Citizens ☐ Business Partners/Contacts (Federal, state, local agencies) ☐ Vendors/Suppliers/Contractors ☐ Patients Other
17	How many individuals' PII is in the system?	500-4,999

Save

18	For what primary purpose is the PII used?	The GSRP Application System will disclose PII as follows: • Referees will have access to minimal PII for applicants who have requested that they provide letters of recommendation. Minimal PII will be displayed to identify the applicant to the referee. • Reviewers will have access to limited PII for those applicants which they are assigned to review for a limited period. Limited PII will include information needed to identify the applicant and facilitate review. • Administrators will have access to PII for all applications. In particular, contact information will be available to reach the applicant. • NCI Principal Investigators will have access to limited PII following review for a limited period. Limited PII will allow the principal investigators to contact an applicant to discuss training opportunities.	
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	Aggregate demographic information may be used to provide a profile of the applicant pool. The information may also be used to compare different cohorts over the years, conducting research/ evaluations to improve the application system as well as the training program.	
20	Describe the function of the SSN.	N/A	
20a	Cite the **legal authority** to use the SSN.	N/A	
21	Identify **legal authorities** governing information use and disclosure specific to the system and program.	• 42 U.S.C. 284(b)(1)(C) authorizes Director to conduct and support research training for which fellowship support is not provided under section 487 and which is not residency training of physicians or other health professionals. • 42 U.S.C. 285a-2 (b) (3) states that the NCI Director shall support appropriate programs of education and training (including continuing education and laboratory and clinical research training).	
22	Are records on the system retrieved by one or more PII data elements?	(•) Yes ( ) No	
22a	Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or identify if a SORN is being developed.	Published:	9-25-0158 (Administration: Records of Applicants and Awardees of the NIH Intramural Research Training Awards Program)
		Published:	
		Published:	
			[ ] In Progress

Save

23	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains ☐ In-Person ☐ Hard Copy: Mail/Fax ☐ Email ☒ Online ☐ Other Government Sources ☒ Within the OPDIV ☐ Other HHS OPDIV ☐ State/Local/Tribal ☐ Foreign ☐ Other Federal Entities ☐ Other Non-Government Sources ☒ Members of the Public ☐ Commercial Data Broker ☐ Public Media/Internet ☐ Private Sector ☐ Other
23a	Identify the OMB information collection approval number and expiration date.	0925-0761 and expiration date 7/31/2022
24	Is the PII shared with other organizations?	○ Yes ◉ No
25	Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.	A link to the Privacy Statement exists on each web page. The Privacy Statement indicates that "application for this program is voluntary; however, in order for the CCT to process an application, the applicant must complete the required fields." For non-required PII, an explanation is provided in the application that indicates that this PII will be provided in aggregate form to provide a profile of the applicant pool.
26	Is the submission of PII by individuals voluntary or mandatory?	◉ Voluntary ○ Mandatory
27	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.	Application to the program is voluntary. If a candidate applies, certain information is optional including, gender, race/ ethnicity, birth place and birth date.
28	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). Alternatively, describe why they cannot be notified or have their consent obtained.	In the event that disclosure and/or data uses change, users are emailed and provided a link to the updated privacy statement.

Save

29	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. If no process exists, explain why not.	There is a “Contact Us” feature on the website that can be used for the individual to send their concern. The contact mailbox is monitored during business hours. Once notified by the individual, a web site administrator can correct the data, delete the data, or otherwise resolve the issue.	
30	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. If no processes are in place, explain why not.	Automated audit trails are monitored on all server-based systems deployed at IMS. All of the Linux workstations and the Windows systems have the ability to track resources as small as a single file. File usage logging will be done for files specified by the HHS organization. Audit records and server logs will be reviewed daily for anomalies. Windows servers log user access and resource usage. An automated reporting tool will be used to analyze the server logs to look for abnormal activity. Automated audit trails also play an important part in governing the access granted to users outside the Contractor’s Local Area Network (LAN). A firewall is in place that logs all incoming and outgoing connections to the LAN. This includes connections to the Linux workstations and the Windows servers. This log will be maintained and checked for evidence of attempted unauthorized access to the Contractor’s LAN. Computer center staff performs weekly security checks of the computer center resources using a vulnerability scanner.	
31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users	Website administrators will have access to PII to review qualifications of applicants and to contact applicants, if necessary.
		☒ Administrators	Linux administrators and database administrators have access to PII for backup and restore purposes.
		☒ Developers	Developers have access to PII to debug user problems.
		☒ Contractors	Only contractors who are website administrators have access to PII to debug user problems and contact applicants in regard to these problems.
		☒ Others	(Reviewers) for reviewing qualifications of applicants
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The contractor that runs this website maintains an Application Support Environment (ASE). As part of the ASE, Linux system administrators and database administrators have access to the	
33	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.	All users are assigned a role when user accounts are created. Both reviewers and NCI Principal Investigators are assigned a role that is used to provide limited access to PII. Administrators are assigned a role that provides full access to PI.	

Save

34	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 use NIH applications must attend security awareness training every year. There are four categories of mandatory IT training (Information Security, Counterintelligence, Privacy Awareness, and Records Management). Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials.
35	Describe training system users receive (above and beyond general security and privacy awareness training).	Website administrators are provided a beta site to understand the functions of the system and are shown the methods for creating new administrator accounts and approving investigator accounts. Responsibilities for protecting PII are discussed as part of this training.
36	Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?	(•) Yes ( ) No
37	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.	Records are retained and disposed of under the authority of NIH Records Control Schedule contained in NIH Manual Chapter 1743, Appendix 1 - "Keeping and Destroying Records" (HHS Record Management Manual, Appendix B-361), item 4000-E-3. Records are maintained within NCI for a time of no less than six years after a password is altered or an user account is terminated in accordance with NARA record retention schedule: 3.2.031, System access records; Systems requiring special accountability for access; DAA-GRS-2013-0006-0004 Records are maintained within NCI for one year after the system is superseded by a new iteration or when no longer needed for agency/Information Technology (IT) administrative purposes to ensure a continuity of security controls throughout the life of the system in accordance with NARA record retention schedule: 3.2.010, Systems and data security records: DAA-GRS-2013-0006-0001

Save

38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Administrative Controls: Access requests are managed, validated, and audited by system administrators and scheduled audits are performed to ensure accounts are validated and/or revoked if needed. Technical Controls: For NIH users: Access to the system is controlled by NIH log-in. The 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. For non-NIH users All logical access to the underlying systems is hosted and controlled by a third party, Information Management Services Inc. All servers utilized by this application have been configured to remove all unnecessary applications and system files. Physical Controls: The servers reside in one of the co-location facilities of Information Management Systems Inc., at any given time. The facilities are located in Sterling VA, and Baltimore MD. All facilities have controlled access and are SOC 2 type II audited and have been reviewed by FISMA auditors for compliance with appropriate facility related controls.
39	Identify the publicly-available URL:	https://nci-gsrp.cancer.gov
40	Does the website have a posted privacy notice?	(•) Yes ( ) No
40a	Is the privacy policy available in a machine-readable format?	( ) Yes (•) No
41	Does the website use web measurement and customization technology?	(•) Yes ( ) No

41a Select the type of website measurement and customization technologies is in use and if it is used to collect PII. (Select all that apply)

Technologies		Collects PII?
☐	Web beacons	( ) Yes ( ) No
☐	Web bugs	( ) Yes ( ) No
☒	Session Cookies	( ) Yes (•) No
☐	Persistent Cookies	( ) Yes ( ) No
Other...		( ) Yes ( ) No

42	Does the website have any information or pages directed at children under the age of thirteen?	( ) Yes (•) No

Save

43	Does the website contain links to non- federal government websites external to HHS?	○ Yes ◉ No

General Comments	This module is under the National Cancer Institue Local Network (NCI LAN) General Support System (GSS) whose Universal Unique Identifier (UUID) is 93F1C7DB-B2F0-4282-9FAD-7168D5B63F91.

OPDIV Senior Official for Privacy Signature	Celeste E. Dade-vinson -S Digitally signed by Celeste E. Dade-vinson -S Date: 2019.11.14 12:10:00 -05'00'