

Privacy Impact Assessment Form

v 1.43

Status Form Number Form Date

Question

Answer

1 OPDIV: **NIH**

2 PIA Unique Identifier:

2a Name: **NCI Graduate Student Recruiting**

- 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

Program Application System

3a Identify the Enterprise Performance Lifecycle Phase of the system.

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

POC Name

POC Organization

POC Email

POC Phone

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

11 Describe the purpose of the system.

The GSRP Application System is a web-based application operated by the NCI Center for Cancer Training (CCT). 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

Referee information:

- Name
- Institution
- Job Title
- Position/Role (e.g. dissertation advisor)
- Address
- Phone
- E-mail
- Letter of recommendation for applicant

Reviewer, NCI Principal Investigator, and Administrator Information:

- Name
- Degrees
- Employer
- Position Title
- Address
- Phone
- E-mail
- Research Topic, Research Target, Research Approach (reviewer only)

Information is used as follows:

- Contact information is used to contact the applicant about the status of their application.
- Demographic information is used to construct a summary overview of the composition of the applicant pool. Applicants may provide gender, race/ethnicity, date of birth, and place of birth voluntarily.
- Current visa status may be used by CCT and NIH staff for travel purposes.
- Education and transcripts are used by GSRP administrators and reviewers to evaluate current and past academic performance.

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 operated by the NCI Center for Cancer Training (CCT). It is designed to allow application to the NCI Graduate Student Recruiting Program and evaluation of these applications.

- Applicants are required to provide contact and citizenship information, educational background (including transcripts), a personal statement of research and career goals, a curriculum vitae, research interests, an abstract of research to be presented at the GSRP conference, and an indication of how they heard about the GSRP. Additionally, they must request letters of recommendation through the application website by providing email addresses for those from whom letters will be requested.
- Referees may upload the requested letters of recommendation.
- Administrators assign reviewers to evaluate and score applications, accept/reject applicants based on reviewer z-scores, produce metrics on the applicant pool, and generally manage the application process.
- Reviewers provide a list of research interests which will be used by administrators to match reviewers to applicants. Reviewers evaluate and score applications assigned to them.
- NCI Principal Investigators may view applications for a limited time following the event.

The GSRP Application System limits user access by username and password. Within the system, users have varying levels of permission to edit, submit, review, and evaluate applications.

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.

<input type="checkbox"/> Social Security Number	<input checked="" type="checkbox"/> Date of Birth
<input checked="" type="checkbox"/> Name	<input type="checkbox"/> Photographic Identifiers
<input type="checkbox"/> Driver's License Number	<input type="checkbox"/> Biometric Identifiers
<input type="checkbox"/> Mother's Maiden Name	<input type="checkbox"/> Vehicle Identifiers
<input checked="" type="checkbox"/> E-Mail Address	<input checked="" type="checkbox"/> Mailing Address
<input checked="" type="checkbox"/> Phone Numbers	<input type="checkbox"/> Medical Records Number
<input type="checkbox"/> Medical Notes	<input type="checkbox"/> Financial Account Info
<input type="checkbox"/> Certificates	<input type="checkbox"/> Legal Documents
<input checked="" type="checkbox"/> Education Records	<input type="checkbox"/> Device Identifiers
<input type="checkbox"/> Military Status	<input type="checkbox"/> Employment Status
<input type="checkbox"/> Foreign Activities	<input type="checkbox"/> Passport Number
<input type="checkbox"/> Taxpayer ID	<input type="text" value="Other..."/>
<input type="text" value="Other..."/>	<input type="text" value="Other..."/>
<input type="text" value="Other..."/>	<input type="text" value="Other..."/>

16	Indicate the categories of individuals about whom PII is collected, maintained or shared. <input type="checkbox"/> Employees <input checked="" type="checkbox"/> Public Citizens <input type="checkbox"/> Business Partners/Contacts (Federal, state, local agencies) <input type="checkbox"/> Vendors/Suppliers/Contractors <input type="checkbox"/> Patients Other <input type="text"/>
17	How many individuals' PII is in the system? <input type="text" value="<100"/>
18	For what primary purpose is the PII used? <p>The GSRP Application System will disclose PII as follows:</p> <ul style="list-style-type: none">• 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.• Aggregate demographic information may be provided to reviewers, administrators, and NCI Principal Investigators to provide a profile of the applicant pool.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research) <input type="text" value="None"/>
20	Describe the function of the SSN. <input type="text" value="N/A"/>
20a	Cite the legal authority to use the SSN. <input type="text" value="N/A"/>
21	Identify legal authorities governing information use and disclosure specific to the system and program. <input type="text"/>
22	Are records on the system retrieved by one or more PII data elements? <input checked="" type="radio"/> Yes <input type="radio"/> 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: <input type="text" value="09-25-0158"/> Published: <input type="text"/> Published: <input type="text"/> <input type="checkbox"/> In Progress

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.

24 Is the PII shared with other organizations? Yes No

24a Identify with whom the PII is shared or disclosed and for what purpose.

Within HHS

- Other Federal Agency/Agencies
- State or Local Agency/Agencies
- Private Sector

24b Describe any agreements in place that authorizes the information sharing or disclosure (e.g. Computer Matching Agreement, Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).

24c Describe the procedures for accounting for disclosures

<p>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.</p>	<p>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.</p>
<p>26 Is the submission of PII by individuals voluntary or mandatory?</p>	<p><input checked="" type="radio"/> Voluntary <input type="radio"/> Mandatory</p>
<p>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.</p>	<p>Application to the program is voluntary. If a candidate applies, certain information is optional including gender, race/ethnicity, birth place, and birth date.</p>
<p>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.</p>	<p>Functionality is available to email applicants in the system. In the event that disclosure and/or data uses change, applicants can be emailed and provided a link to the updated privacy statement.</p> <p>Applicants will be made aware of the privacy statement when applying and will be alerted that optional demographic information may be shared in aggregate form to provide a profile of the applicant pool. Application to the program is voluntary. However, for the CCT to process an application, required fields must be collected. By providing the information, the applicant is giving consent for the information to be used as stated on the website.</p> <p>The privacy statement (accessible from all application pages) details how collected information will be used. It notifies individuals that "the primary use of information collected via the National Cancer Institute's (NCI) Center for Cancer Training (CCT) online forms is to evaluate an applicant's qualifications for research training at NCI at the National Institutes of Health (NIH). Information may be used during admission consideration; in preparing appointment paperwork; and to provide data for training program evaluation. Information will be disclosed to investigators, members of advisory committees, CCT staff, and contractors working on our behalf. Additional disclosures may be made to law enforcement agencies concerning violations of law or regulation."</p>
<p>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.</p>	<p>Detailed in SOR. In addition, there is a "Contact Us" feature on the website that can be used.</p>

<p>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.</p>	<p>Automated audit trails are monitored on all server-based systems deployed at IMS. All of the UNIX/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 UNIX/Linux workstations and the Windows servers. This log will be maintain and checked for evidence of attempted unauthorized access to the Contractor's LAN.</p> <p>Computer center staff performs weekly security checks of the computer center resources using a vulnerability scanner.</p>										
<p>31 Identify who will have access to the PII in the system and the reason why they require access.</p>	<table border="1"> <tr> <td><input checked="" type="checkbox"/> Users</td> <td>Part of their job function.</td> </tr> <tr> <td><input checked="" type="checkbox"/> Administrators</td> <td>Part of their job function.</td> </tr> <tr> <td><input checked="" type="checkbox"/> Developers</td> <td>On an as-needed basis to perform their job function.</td> </tr> <tr> <td><input type="checkbox"/> Contractors</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Others</td> <td></td> </tr> </table>	<input checked="" type="checkbox"/> Users	Part of their job function.	<input checked="" type="checkbox"/> Administrators	Part of their job function.	<input checked="" type="checkbox"/> Developers	On an as-needed basis to perform their job function.	<input type="checkbox"/> Contractors		<input type="checkbox"/> Others	
<input checked="" type="checkbox"/> Users	Part of their job function.										
<input checked="" type="checkbox"/> Administrators	Part of their job function.										
<input checked="" type="checkbox"/> Developers	On an as-needed basis to perform their job function.										
<input type="checkbox"/> Contractors											
<input type="checkbox"/> Others											
<p>32 Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.</p>	<p>Linux system administrators and database administrators have access to the PII for backup and restore purposes. Both are required to have security clearances and complete yearly training for security and privacy concerns. Additionally, GSRP administrators (including developers), reviewers, and NCI Principal Investigators may access PII. Administrators can create user accounts for other administrators and can approve requests by reviewers or NCI Principal Investigators to access limited PII on applications.</p>										
<p>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.</p>	<p>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 PII.</p>										
<p>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.</p>	<p>System managers, operators, and NCI personnel must complete yearly security awareness and training programs. GSRP administrators are instructed on the importance of providing only necessary access to individuals. GSRP administrators must review requests from NCI Principal Investigators before access is granted.</p>										

35 Describe training system users receive (above and beyond general security and privacy awareness training).	GSRP 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?	<input checked="" type="radio"/> Yes <input type="radio"/> 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 the NIH Records Control Schedule contained in NIH Manual Chapter 1743, Appendix 1 - "Keeping and Destroying Records" (HHS Records Management Manual, Appendix B-361), item 4000-E-3. Refer to the NIH Manual Chapter for specific disposition instructions.
38 Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	<p>The IMS computer center consists of two co-location facilities. One is located in Baltimore MD and the other is located 60 miles away in Sterling VA. Both of these facilities are SAS-70 type II certified facilities which provide 24x7 security and monitoring for physical entry and environmental hazards. The internal IMS network is protected at all entry points by firewalls and intrusion detection devices.</p> <p>IMS has Standard Operating Procedures (SOPs) governing the storage and transmission of all data types including PII. Transmission of data outside of the data center is secured using standard SSL or HTTPS based protocols. IMS has developed a data transfer facility utilizing the HTTPS protocol that allows for secure transfer data between the client and IMS. The storage of data that is deemed sensitive must be commensurate with the level of Confidentiality, Availability and Integrity required as specified in a PIA or other assessment document. Physical controls such as user/group authorization, encryption of data at rest, and weekly security/virus scans are employed in the data center to ensure continued data security while at IMS. All IMS employees are required to read, agree to, and sign a confidentiality agreement at the time of employment. They must also complete yearly security trainings. Additionally, employees that act as gate keepers to the data center such as network and database administrators are required to have security clearances while performing their job.</p> <p>IMS continually monitors all of its systems for anomalies which could indicate a security breach or other issue with the systems. SOPs and a disaster recovery plan are in place that detail actions system administrators and other responsible parties must take in the event of a security incident, unplanned downtime or disaster. Also, IMS does weekly system scans with a vulnerability scanner to ensure all systems are patched to an acceptable level.</p>
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

	Technologies	Collects PII?
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)	<input type="checkbox"/> Web beacons	<input type="radio"/> Yes <input type="radio"/> No
	<input type="checkbox"/> Web bugs	<input type="radio"/> Yes <input type="radio"/> No
	<input checked="" type="checkbox"/> Session Cookies	<input type="radio"/> Yes <input checked="" type="radio"/> No
	<input type="checkbox"/> Persistent Cookies	<input type="radio"/> Yes <input type="radio"/> No
	Other... <input type="text"/>	<input type="radio"/> Yes <input type="radio"/> No

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

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

REVIEWER QUESTIONS: The following section contains Reviewer Questions which are not to be filled out unless the user is an OPDIV Senior Officer for Privacy.

Reviewer Questions	Answer
--------------------	--------

1 Are the questions on the PIA answered correctly, accurately, and completely?	<input type="radio"/> Yes <input type="radio"/> No
--	---

Reviewer Notes

2 Does the PIA appropriately communicate the purpose of PII in the system and is the purpose justified by appropriate legal authorities?	<input type="radio"/> Yes <input type="radio"/> No
--	---

Reviewer Notes

3 Do system owners demonstrate appropriate understanding of the impact of the PII in the system and provide sufficient oversight to employees and contractors?	<input type="radio"/> Yes <input type="radio"/> No
--	---

Reviewer Notes

4 Does the PIA appropriately describe the PII quality and integrity of the data?	<input type="radio"/> Yes <input type="radio"/> No
--	---

Reviewer Notes

Save

Reviewer Questions		Answer	
5	Is this a candidate for PII minimization?	<input type="radio"/> Yes <input type="radio"/> No	
Reviewer Notes	<input type="text"/>		
6	Does the PIA accurately identify data retention procedures and records retention schedules?	<input type="radio"/> Yes <input type="radio"/> No	
Reviewer Notes	<input type="text"/>		
7	Are the individuals whose PII is in the system provided appropriate participation?	<input type="radio"/> Yes <input type="radio"/> No	
Reviewer Notes	<input type="text"/>		
8	Does the PIA raise any concerns about the security of the PII?	<input type="radio"/> Yes <input type="radio"/> No	
Reviewer Notes	<input type="text"/>		
9	Is applicability of the Privacy Act captured correctly and is a SORN published or does it need to be?	<input type="radio"/> Yes <input type="radio"/> No	
Reviewer Notes	<input type="text"/>		
10	Is the PII appropriately limited for use internally and with third parties?	<input type="radio"/> Yes <input type="radio"/> No	
Reviewer Notes	<input type="text"/>		
11	Does the PIA demonstrate compliance with all Web privacy requirements?	<input type="radio"/> Yes <input type="radio"/> No	
Reviewer Notes	<input type="text"/>		
12	Were any changes made to the system because of the completion of this PIA?	<input type="radio"/> Yes <input type="radio"/> No	
Reviewer Notes	<input type="text"/>		
General Comments	<input type="text"/>		
OPDIV Senior Official for Privacy Signature	<input type="text"/>	HHS Senior Agency Official for Privacy	<input type="text"/>