06.1 HHS Privacy Impact Assessment (Form) / NIH OD Research and Training Opportunities System (RTO) (Item)

Primavera ProSight

Form Report, printed by: Alves, Steve, **Aug 24, 2012**

PIA SUMMARY

1

The following required questions with an asterisk (*) represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget (OMB) and public posting in accordance with OMB Memorandum (M) 03-22.

Note: If a question or its response is not applicable, please answer ''N/A'' to that question where possible. If the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of personally identifiable information (PII). If no PII is contained in the system, please answer questions in the PIA Summary Tab and then promote the PIA to the Senior Official for Privacy who will authorize the PIA. If this system contains PII, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

2 Summary of PIA Required Questions

**Is this a new PIA?*

No

If this is an existing PIA, please provide a reason for revision:

PIA Validation

**1. Date of this Submission:*

Aug 24, 2012

**2. OPDIV Name:*

NIH

**4. Privacy Act System of Records Notice (SORN) Number (If response to Q.21 is Yes, a SORN number is required for Q.4):*

09-25-0014, 09-25-0158, and 09-25-0108

**5. OMB Information Collection Approval Number:*

0925-0299

**6. Other Identifying Number(s):*

N/A

**7. System Name (Align with system item name):*

NIH OD Research and Training Opportunities System (RTO)

**9. System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:*

Point of Contact Information	
POC Name	Steve Alves

**10. Provide an overview of the system:*

The Office of Intramural Training & Education (OITE) administers a variety of programs and initiatives to recruit and develop individuals who participate in research training activities on the NIH's main campus in Bethesda, Maryland, as well as other NIH facilities around the country. To facilitate its recruitment function, the OITE maintains the NIH Research and Training Opportunities (RTO) Web site, http://www2.training.nih.gov, which includes applications and related forms for a range of intramural research training programs. The application system includes a back-end database that functions as a centralized repository of information regarding program applicants. Collection of the information in this system is authorized under sections 241, 242l, 282(b)(10), 282(b)(13), 284(b)(1)(c), and 284(b)(1)(K) of title 42 of the United States Code (USC), and Part 61, Subpart A and Part 63 of title 42 of the Code of Federal Regulations (CFR). The primary use of this information is to evaluate applicants' qualifications for research training at the NIH.

**13. Indicate if the system is new or an existing one being modified:*

Existing

**17. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system?*

TIP: If the answer to Question 17 is ''No'' (indicating the system does not contain PII), only the remaining PIA Summary tab questions need to be completed

and submitted. If the system does contain PII, the full PIA must be completed and submitted. (Although note that "Employee systems," – i.e., systems that collect PII "permitting the physical or online contacting of a specific individual … employed [by] the Federal Government – only need to complete the PIA Summary tab.)

Yes

17a. Is this a GSS PIA included for C&A purposes only, with no ownership of underlying application data? If the response to Q.17a is Yes, the response to Q.17 should be No and only the PIA Summary must be completed.

No

**19. Are records on the system retrieved by 1 or more PII data elements?*

Yes

**21. Is the system subject to the Privacy Act? (If the response to Q.19 is Yes, the response to Q.21 must be Yes and a SORN number is required for Q.4)*

Yes

**23. If the system shares or discloses PII, please specify with whom and for what purpose(s):*

FDA investigators, staff, and administrators involved in the recruitment/selection of trainees may be given access to the applicant databases. Access is otherwise restricted to authorized NIH investigators, staff, and administrators.

**30. Please describe in detail: (1) The information the agency will collect, maintain, or disseminate (clearly state if the information contained in the system ONLY represents federal contact data); (2) Why and for what purpose the agency will use the information; (3) Explicitly indicate whether the information contains PII; and (4) Whether submission of personal information is voluntary or mandatory:*

The electronic application system collects information, including PII, necessary to evaluate the qualifications of individuals who seek intramural research training opportunities at the NIH. These fields include the following: name, month and day of birth, e-mail address, mailing address, telephone numbers, citizenship status, visa status, institutional affiliations, courses completed and grades earned, grade point average (GPA), academic major, publications, a resume or curriculum vitae, contact information for up to 3 references, cover letter/personal statement, scientific research interests. Candidates also have the option of voluntarily responding to questions regarding gender, race/national origin, and disability (RNO). RNO data are made available to authorized NIH users in aggregate form only.

**31. Please describe in detail any processes in place to: (1) 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 the original collection); (2) Notify and obtain consent from individuals regarding what PII is being collected from them; and (3) How the information will be used or shared. (Note: Please describe in what format individuals will be given notice of consent [e.g., written notice, electronic notice, etc.]):*

Information is collected through a web-based electronic application system. Applicants are presented with a link to the following Privacy Act Notification Act Statement:
"Collection of this information is authorized under sections 241, 242l, 282(b)(10), 282(b)(13), 284(b)(1)(c), and 284(b)(1)(K) of title 42 of the United States Code (USC), and Part 61, Subpart A and Part 63 of title 42 of the Code of Federal Regulations (CFR). The primary use of this information is to evaluate your qualifications for research training at the National Institutes of Health. Additional disclosures may be made to law enforcement agencies concerning violations of law or regulation. Application for this program is voluntary; however, in order for us to process your application, you must complete the required fields." (Electronic Notice)
Applicants who choose to respond to the separate survey regarding gender, race/national origin, age, and disability are presented with a link to the following instructions:
"This survey is used to collect and analyze data involving race, sex, age, disability, and national origin from applicants for employment. The information you provide will be used for statistical purposes only and will not in any way affect you individually. While completion of this form is voluntary, your cooperation is important to help ensure accurate information regarding employment practices. We ask you to answer each of the questions to the best of your ability. Read each item thoroughly before selecting the appropriate response." (Electronic Notice)
There is no process in place currently to notify and obtain consent from the individuals whose IIF is in the system when major changes occur to the system.

**32. Does the system host a website? (Note: If the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of PII)*

Yes

**37. Does the website have any information or pages directed at children under the age of thirteen?*

No

**50. Are there policies or guidelines in place with regard to the retention and destruction of PII? (Refer to the C&A package and/or the Records Retention and Destruction section in SORN)*

Yes

**54. Briefly describe in detail how the PII will be secured on the system using administrative, technical, and physical controls:*

Methods are in place to ensure least privilege (i.e., "need to know" and accountability). Accounts to access application data are issued by authorized representatives from the individual ICs. Access to accounts that give the user greater access (to create "read only" accounts and to accept applicants electronically) is controlled by OITE staff. Also, OITE's Web contractors do not have full administrative rights on development and production servers, and only access specific folders on these servers. Technical Controls in place to minimize the possibility of unauthorized access, use, or dissemination of the data in the system include User Identification, Passwords, Firewall, Virtual Private Network (VPN), Encryption, and Intrusion Detection System (IDS). In December 2010, OITE moved RTO behind Federated Identity Login service (NIH Login). Regarding physical access controls that are currently on the system, the Web, e-mail, and database servers that are maintained in secure NIH buildings at which security guards are posted. Access to the servers is restricted to authorized

CIT/OIT individuals with valid Identification Badges.

In addition, the IT contractors are required to adhere to the security guidelines contained in the DHHS Automated Information Systems Security Program (AISSP) Handbook. Software development is performed on servers maintained by the contractor. Staging is on a shared NIH server residing inside the NIH firewall. Development will occur on specific servers maintained by the NIH Office of Information Technology. All contract employees are subject to a National Agency Check and Inquiry Investigation plus a Credit Check (NACIC).

PIA REQUIRED INFORMATION

1 HHS Privacy Impact Assessment (PIA)

The PIA determines if Personally Identifiable Information (PII) is contained within a system, what kind of PII, what is done with that information, and how that information is protected. Systems with PII are subject to an extensive list of requirements based on privacy laws, regulations, and guidance. The HHS Privacy Act Officer may be contacted for issues related to Freedom of Information Act (FOIA) and the Privacy Act. Respective Operating Division (OPDIV) Privacy Contacts may be contacted for issues related to the Privacy Act. The Office of the Chief Information Officer (OCIO) can be used as a resource for questions related to the administrative, technical, and physical controls of the system. Please note that answers to questions with an asterisk (*) will be submitted to the Office of Management and Budget (OMB) and made publicly available in accordance with OMB Memorandum (M) 03-22.

Note: If a question or its response is not applicable, please answer "N/A" to that question where possible.

2 General Information

**Is this a new PIA?*

No

If this is an existing PIA, please provide a reason for revision:

PIA Validation

**1. Date of this Submission:*

Aug 24, 2012

**2. OPDIV Name:*

NIH

3. Unique Project Identifier (UPI) Number for current fiscal year (Data is auto-populated from the System Inventory form, UPI table):

**4. Privacy Act System of Records Notice (SORN) Number (If response to Q.21 is Yes, a SORN number is required for Q.4):*

09-25-0014, 09-25-0158, and 09-25-0108

**5. OMB Information Collection Approval Number:*

0925-0299

5a. OMB Collection Approval Number Expiration Date:

Mar 31, 2014

**6. Other Identifying Number(s):*

N/A

**7. System Name: (Align with system item name)*

NIH OD Research and Training Opportunities System (RTO)

8. System Location: (OPDIV or contractor office building, room, city, and state)

System Location:	
OPDIV or contractor office building	NIH
Room	31/B1E35
City	Bethesda
State	Maryland

**9. System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:*

Point of Contact Information	
POC Name	Steve Alves

The following information will not be made publicly available:

POC Title	Program Analyst
POC Organization	Office of Intramural Training & Education, OIR, OD, NIH
POC Phone	301-402-1294
POC Email	alvess@mail.nih.gov

**10. Provide an overview of the system: (Note: The System Inventory form can provide additional information for child dependencies if the system is a GSS)*

The Office of Intramural Training & Education (OITE) administers a variety of programs and initiatives to recruit and develop individuals who participate in research training activities on the NIH's main campus in Bethesda, Maryland, as well as other NIH facilities around the country. To facilitate its recruitment function, the OITE maintains the NIH Research and Training Opportunities (RTO) Web site, http://www2.training.nih.gov, which includes applications and related forms for a range of intramural research training programs. The application system includes a back-end database that functions as a centralized repository of information regarding program applicants. Collection of the information in this system is authorized under sections 241, 242l, 282(b)(10), 282(b)(13), 284(b)(1)(c), and 284(b)(1)(K) of title 42 of the United States Code (USC), and Part 61, Subpart A and Part 63 of title 42 of the Code of Federal Regulations (CFR). The primary use of this information is to evaluate applicants' qualifications for research training at the NIH.

SYSTEM CHARACTERIZATION AND DATA CATEGORIZATION

1 System Characterization and Data Configuration

11. Does HHS own the system?

Yes

11a. If no, identify the system owner:

12. Does HHS operate the system? (If the system is operated at a contractor site, the answer should be No)

Yes

12a. If no, identify the system operator:

**13. Indicate if the system is new or an existing one being modified:*

Existing

14. Identify the life-cycle phase of this system:

Operations/Maintenance

15. Have any of the following major changes occurred to the system since the PIA was last submitted?

No

Please indicate "Yes" or "No" for each category below:	Yes/No
Conversions	No
Anonymous to Non-Anonymous	No
Significant System Management Changes	No
Significant Merging	No
New Public Access	No
Commercial Sources	No
New Interagency Uses	No
Internal Flow or Collection	No
Alteration in Character of Data	No

16. Is the system a General Support System (GSS), Major Application (MA), Minor Application (child) or Minor Application (stand-alone)?

Major Application

**17. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system?*

Yes

TIP: If the answer to Question 17 is ''No'' (indicating the system does not contain PII), only the remaining PIA Summary tab questions need to be completed and submitted. If the system does contain PII, the full PIA must be completed and submitted. (Although note that ''Employee systems,'' – i.e., systems that collect PII ''permitting the physical or online contacting of a specific individual ... employed [by] the Federal Government – only need to complete the PIA Summary tab.)

Please indicate "Yes" or "No" for each PII category. If the applicable PII category is not listed, please use the Other field to identify the appropriate category of PII.

Categories:	Yes/No
Name (for purposes other than contacting federal employees)	Yes
Date of Birth	Yes
Social Security Number (SSN)	No

Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	Yes
Personal Phone Numbers	Yes
Medical Records Numbers	No
Medical Notes	No
Financial Account Information	No
Certificates	No
Legal Documents	No
Device Identifiers	No
Web Uniform Resource Locator(s) (URL)	No
Personal Email Address	Yes
Education Records	Yes
Military Status	No
Employment Status	Yes
Foreign Activities	No
Other	Birth date (month and day of birth only), citizenship status, visa status, institutional affiliations, courses completed and grades earned, grade point average (GPA), academic major, publications, a resume or curriculum vitae, contact information for up to 3 references, cover letter/personal statement, scientific research interests. Candidates also have the option of voluntarily responding to questions regarding gender, race/national origin, age, and disability. These data are collected in aggregate.

17a. Is this a GSS PIA included for C&A purposes only, with no ownership of underlying application data? If the response to Q.17a is Yes, the response to Q.17 should be No and only the PIA Summary must be completed.

No

18. Please indicate the categories of individuals about whom PII is collected, maintained, disseminated and/or passed through. Note: If the applicable PII category is not listed, please use the Other field to identify the appropriate category of PII. Please answer "Yes" or "No" to each of these choices (NA in other is not applicable).

Categories:	Yes/No
Employees	Yes
Public Citizen	Yes
Patients	No
Business partners/contacts (Federal, state, local agencies)	No
Vendors/Suppliers/Contractors	Yes
Other	No

**19. Are records on the system retrieved by 1 or more PII data elements?*

Yes

Please indicate "Yes" or "No" for each PII category. If the applicable PII category is not listed, please use the Other field to identify the appropriate category of PII.

Categories:	Yes/No
Name (for purposes other than contacting federal employees)	Yes
Date of Birth	No
SSN	No
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	Yes
Personal Phone Numbers	Yes
Medical Records Numbers	No
Medical Notes	No
Financial Account Information	No
Certificates	No
Legal Documents	No
Device Identifiers	No
Web URLs	No
Personal Email Address	Yes
Education Records	Yes
Military Status	No
Employment Status	Yes
Foreign Activities	No
Other	No

20. Are 10 or more records containing PII maintained, stored or transmitted/passed through this system?

Yes

**21. Is the system subject to the Privacy Act? (If the response to Q.19 is Yes, the response to Q.21 must be Yes and a SORN number is required for Q.4)*

Yes

21a. If yes but a SORN has not been created, please provide an explanation.

INFORMATION SHARING PRACTICES

1 Information Sharing Practices

22. Does the system share or disclose PII with other divisions within this agency, external agencies, or other people or organizations outside the agency?

Yes

Please indicate "Yes" or "No" for each category below:	Yes/No
Name (for purposes other than contacting federal employees)	Yes
Date of Birth	Yes
SSN	No
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	Yes
Personal Phone Numbers	Yes
Medical Records Numbers	No
Medical Notes	No
Financial Account Information	No
Certificates	No
Legal Documents	No
Device Identifiers	No
Web URLs	No
Personal Email Address	Yes
Education Records	Yes
Military Status	No
Employment Status	Yes
Foreign Activities	No
Other	Birth date (month and day of birth only), citizenship status, visa status, institutional affiliations, courses completed and grades earned, grade point average (GPA), academic major, publications, a resume or curriculum vitae, contact information for up to 3 references, cover letter/personal statement, scientific research interests. Candidates also have the option of voluntarily responding to questions regarding gender, race/national origin, age, and disability. These data are collected in aggregate.

**23. If the system shares or discloses PII please specify with whom and for what purpose(s):*

FDA investigators, staff, and administrators involved in the recruitment/selection of trainees may be given access to the applicant databases. Access is otherwise restricted to authorized NIH investigators, staff, and administrators.

24. If the PII in the system is matched against PII in one or more other computer systems, are computer data matching agreement(s) in place?

Not Applicable

25. Is there a process in place to notify organizations or systems that are dependent upon the PII contained in this system when major changes occur (i.e., revisions to PII, or when the system is replaced)?

No

26. Are individuals notified how their PII is going to be used?

Yes

26a. If yes, please describe the process for allowing individuals to have a choice. If no, please provide an explanation.

The Privacy Act Notification Statement for the RTO system states, in part, "The primary use of this information is to evaluate your qualifications for research training at the National Institutes of Health. Additional disclosures may be made to law enforcement agencies concerning violations of law or regulation. Application for this program is voluntary; however, in order for us to process your application, you must complete the required fields."

27. Is there a complaint process in place for individuals who believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate?

Yes

27a. If yes, please describe briefly the notification process. If no, please provide an explanation.

Users can select the "Contact us" or "Comments" link and e-mail OITE with questions or to express concerns

28. Are there processes in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy?

No

28a. If yes, please describe briefly the review process. If no, please provide an explanation.

By default, authorized users have access to the most current applicant data (i.e., data submitted during the current application cycle for the program in question). Application cycles vary from program to program; some applications are open for a limted time (e.g., 3-4 months) and others are open year-round. Applications are archived after one year or when the applicant's eligibility expires, at which point the application can only be accessed by OITE staff. An applicant can modify/update his/her application during part or all of the application cycle, depending on the program, or withdraw his/her application at any time before it is archived.

29. Are there rules of conduct in place for access to PII on the system?

Yes

Please indicate "Yes," "No," or "N/A" for each category. If yes, briefly state the purpose for each user to have access:

Users with access to PII	Yes/No/N/A	Purpose
User	Yes	Security, update application information, re-send e-mail request for letter of recommendation to references, check status of letters
Administrators	Yes	Security, recruitment of trainees
Developers	Yes	Security, system maintenance/development
Contractors	Yes	Security, system maintenance/development
Other	No	

**30. Please describe in detail: (1) The information the agency will collect, maintain, or disseminate (clearly state if the information contained in the system ONLY represents federal contact data); (2) Why and for what purpose the agency will use the information; (3) Explicitly indicate whether the information contains PII; and (4) Whether submission of personal information is voluntary or mandatory:*

The electronic application system collects information, including PII, necessary to evaluate the qualifications of individuals who seek intramural research training opportunities at the NIH. These fields include the following: name, month and day of birth, e-mail address, mailing address, telephone numbers, citizenship status, visa status, institutional affiliations, courses completed and grades earned, grade point average (GPA), academic major, publications, a resume or curriculum vitae, contact information for up to 3 references, cover letter/personal statement, scientific research interests. Candidates also have the option of voluntarily responding to questions regarding gender, race/national origin, and disability (RNO). RNO data are made available to authorized NIH users in aggregate form only.

**31. Please describe in detail any processes in place to: (1) 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 the original collection); (2) Notify and obtain consent from individuals regarding what PII is being collected from them; and (3) How the information will be used or shared. (Note: Please describe in what format individuals will be given notice of consent [e.g., written notice, electronic notice, etc.])*

Information is collected through a web-based electronic application system. Applicants are presented with a link to the following Privacy Act Notification Act Statement:
"Collection of this information is authorized under sections 241, 242l, 282(b)(10), 282(b)(13), 284(b)(1)(c), and 284(b)(1)(K) of title 42 of the United States Code (USC), and Part 61, Subpart A and Part 63 of title 42 of the Code of Federal Regulations (CFR). The primary use of this information is to evaluate your qualifications for research training at the National Institutes of Health. Additional disclosures may be made to law enforcement agencies concerning violations of law or regulation. Application for this program is voluntary; however,

in order for us to process your application, you must complete the required fields." (Electronic Notice)
Applicants who choose to respond to the separate survey regarding gender, race/national origin, age, and disability are presented with a link to the following instructions:
"This survey is used to collect and analyze data involving race, sex, age, disability, and national origin from applicants for employment. The information you provide will be used for statistical purposes only and will not in any way affect you individually. While completion of this form is voluntary, your cooperation is important to help ensure accurate information regarding employment practices. We ask you to answer each of the questions to the best of your ability. Read each item thoroughly before selecting the appropriate response." (Electronic Notice)
There is no process in place currently to notify and obtain consent from the individuals whose IIF is in the system when major changes occur to the system.

WEBSITE HOSTING PRACTICES

1 Website Hosting Practices

**32. Does the system host a website? (Note: If the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of PII)*

Yes

Please indicate "Yes" or "No" for each type of site below. If the system hosts both Internet and Intranet sites, indicate "Yes" for "Both" only.	Yes/ No	If the system hosts an Internet site, please enter the site URL. Do not enter any URL(s) for Intranet sites.
Internet	Yes	http://www2.training.nih.gov
Intranet	Yes	
Both	Yes	

33. Does the system host a website that is accessible by the public and does not meet the exceptions listed in OMB M-03-22?

Note: OMB M-03-22 Attachment A, Section III, Subsection C requires agencies to post a privacy policy for websites that are accessible to the public, but provides three exceptions: (1) Websites containing information other than "government information" as defined in OMB Circular A-130; (2) Agency intranet websites that are accessible only by authorized government users (employees, contractors, consultants, fellows, grantees); and (3) National security systems defined at 40 U.S.C. 11103 as exempt from the definition of information technology (see section 202(i) of the E-Government Act.).

Yes

34. If the website does not meet one or more of the exceptions described in Q. 33 (i.e., response to Q. 33 is "Yes"), a website privacy policy statement (consistent with OMB M-03-22 and Title II and III of the E-Government Act) is required. Has a website privacy policy been posted?

Yes

35. If a website privacy policy is required (i.e., response to Q. 34 is ''Yes''), is the privacy policy in machine-readable format, such as Platform for Privacy Preferences (P3P)?

Yes

35a. If no, please indicate when the website will be P3P compliant:

36. Does the website employ tracking technologies?

Yes

Please indicate "Yes", "No", or "N/A" for each type of cookie below:	Yes/No/N/A
Web Bugs	No
Web Beacons	No
Session Cookies	Yes
Persistent Cookies	No
Other	

**37. Does the website have any information or pages directed at children under the age of thirteen?*

No

37a. If yes, is there a unique privacy policy for the site, and does the unique privacy policy address the process for obtaining parental consent if any information is collected?

38. Does the website collect PII from individuals?

Yes

Please indicate "Yes" or "No" for each category below:	Yes/No
Name (for purposes other than contacting federal employees)	Yes
Date of Birth	Yes
SSN	No
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	Yes
Personal Phone Numbers	Yes
Medical Records Numbers	No
Medical Notes	No
Financial Account Information	No
Certificates	No
Legal Documents	No
Device Identifiers	No
Web URLs	No
Personal Email Address	Yes
Education Records	Yes
Military Status	No
Employment Status	Yes
Foreign Activities	No
Other	Birth date (month and day of birth only), citizenship status, visa status, institutional affiliations, courses completed and grades earned, grade point average (GPA), academic major, publications, a resume or curriculum vitae, contact information for up to 3 references, cover letter/personal statement, scientific research interests. Candidates also have the option of voluntarily responding to questions regarding gender, race/national origin, age, and disability. These data are collected in aggregate.

39. Are rules of conduct in place for access to PII on the website?

Yes

40. Does the website contain links to sites external to HHS that owns and/or operates the system?

Yes

40a. If yes, note whether the system provides a disclaimer notice for users that follow external links to websites not owned or operated by HHS.

Yes

ADMINISTRATIVE CONTROLS

1	Administrative Controls

Note: This PIA uses the terms ''Administrative,'' ''Technical'' and ''Physical'' to refer to security control questions—terms that are used in several Federal laws when referencing security requirements.

41. Has the system been certified and accredited (C&A)?

Yes

41a. If yes, please indicate when the C&A was completed:

Jul 30, 2009

41b. If a system requires a C&A and no C&A was completed, is a C&A in progress?

42. Is there a system security plan for this system?

Yes

43. Is there a contingency (or backup) plan for the system?

Yes

44. Are files backed up regularly?

Yes

45. Are backup files stored offsite?

Yes

46. Are there user manuals for the system?

Yes

47. Have personnel (system owners, managers, operators, contractors and/or program managers) using the system been trained and made aware of their responsibilities for protecting the information being collected and maintained?

Yes

48. If contractors operate or use the system, do the contracts include clauses ensuring adherence to privacy provisions and practices?

Yes

49. Are methods in place to ensure least privilege (i.e., ''need to know'' and accountability)?

Yes

49a. If yes, please specify method(s):

OITE's contractors do not have full administrative rights on development and production servers, and only access specific folders on these servers.

**50. Are there policies or guidelines in place with regard to the retention and destruction of PII? (Refer to the C&A package and/or the Records Retention and Destruction section in SORN):*

Yes

50a. If yes, please provide some detail about these policies/practices:

The information collected by the RTO system is collected and maintained in accordance with the following Privacy Act Systems of Records Notices: 09-25-0158, "Administration Records of Applicants and Awardees of the Intramural Research Training Awards Program;" 09-25-0014, "Clinical Research: Student Records;" and 09-25-0108, "Personnel: Guest Researchers, Special Volunteers, and Scientists Emeriti."
The Retention and Disposal section of SORN 09-25-0108 states:
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 2300-320-3(a), which allows records to be destroyed after a maximum period of two years after the individual completes work at NIH. Refer to the NIH Manual Chapter for specific disposition instructions.
The Retention and Disposal section of SORN 09-25-0014 states:
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), items 2300-320-1-13, which allows records to be kept up to a maximum period of ten years. Refer to the NIH Manual Chapter for specific disposition instructions.
The Retention and Disposal section of SORN 09-25-0158 states:
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.

TECHNICAL CONTROLS

1 Technical Controls

51. Are technical controls in place to minimize the possibility of unauthorized access, use, or dissemination of the data in the system?

Yes

Please indicate "Yes" or "No" for each category below:	Yes/No
User Identification	Yes
Passwords	Yes
Firewall	Yes
Virtual Private Network (VPN)	Yes
Encryption	Yes
Intrusion Detection System (IDS)	Yes
Common Access Cards (CAC)	No
Smart Cards	Yes
Biometrics	No
Public Key Infrastructure (PKI)	No

52. Is there a process in place to monitor and respond to privacy and/or security incidents?

Yes

52a. If yes, please briefly describe the process:

When an incident occurs the Office of Information Technology is notified.

PHYSICAL ACCESS

1 Physical Access

53. Are physical access controls in place?

Yes

Please indicate "Yes" or "No" for each category below:	Yes/No
Guards	Yes
Identification Badges	Yes
Key Cards	No
Cipher Locks	No
Biometrics	No
Closed Circuit TV (CCTV)	No

**54. Briefly describe in detail how the PII will be secured on the system using administrative, technical, and physical controls:*

Methods are in place to ensure least privilege (i.e., "need to know" and accountability). Accounts to access application data are issued by authorized representatives from the individual ICs. Access to accounts that give the user greater access (to create "read only" accounts and to accept applicants electronically) is controlled by OITE staff. Also, OITE's Web contractors do not have full administrative rights on development and production servers, and only access specific folders on these servers. Technical Controls in place to minimize the possibility of unauthorized access, use, or dissemination of the data in the system include User Identification, Passwords, Firewall, Virtual Private Network (VPN), Encryption, and Intrusion Detection System (IDS). In December 2010, OITE moved RTO behind Federated Identity Login service (NIH Login). Regarding physical access controls that are currently on the system, the Web, e-mail, and database servers that are maintained in secure NIH buildings at which security guards are posted. Access to the servers is restricted to authorized CIT/OIT individuals with valid Identification Badges.

In addition, the IT contractors are required to adhere to the security guidelines contained in the DHHS Automated Information Systems Security Program (AISSP) Handbook. Software development is performed on servers maintained by the contractor. Staging is on a shared NIH server residing inside the NIH firewall. Development will occur on specific servers maintained by the NIH Office of Information Technology. All contract employees are subject to a National Agency Check and Inquiry Investigation plus a Credit Check (NACIC).

APPROVAL/DEMOTION

1	System Information
System Name:	NIH OD Research and Training Opportunities System (RTO)

2	PIA Reviewer Approval/Promotion or Demotion
Promotion/Demotion:	Promote
Comments:	Antoine D. Jones
Approval/Demotion Point of Contact:	Steve Alves
Date:	Aug 24, 2012

3	Senior Official for Privacy Approval/Promotion or Demotion
Promotion/Demotion:	Promote
Comments:	

4	OPDIV Senior Official for Privacy or Designee Approval

Please print the PIA and obtain the endorsement of the reviewing official below. Once the signature has been collected, retain a hard copy for the OPDIV's records. Submitting the PIA will indicate the reviewing official has endorsed it

This PIA has been reviewed and endorsed by the OPDIV Senior Official for Privacy or Designee (Name and Date):

Name: _____ **Date:** _____

Name:	Karen Plá
Date:	Sep 27, 2011

5	Department Approval to Publish to the Web
Approved for web publishing	Yes
Date Published:	Sep 1, 2009
Publicly posted PIA URL or no PIA URL explanation:	http://www.hhs.gov/pia/nih.html

PIA % COMPLETE

1	PIA Completion
PIA Percentage Complete:	100.00
PIA Missing Fields:	