1. OPDIV	National Institutes of Health
2. PIA Unique Identifier	P-1110930-742633
2a. Name	CRSS: OCRTME Training Program
3. The subject of this PIA is which of the following?	Major Application
3a. Identify the Enterprise Performance Lifecycle Phase of the system.	Operational
3b. Is this a FISMA-Reportable system?	Yes
4. Does the system include a Website or online application available to and for the use of the general public?	Yes
Accept / Reject Status	
Question 4 Comment	
5. Identify the operator.	Agency
6. Point of Contact (POC)	
POC Title	System Owner
POC Name	Simmons, Jennifer
POC Organization	NIH/CC/OCRTME
POC Email	simmonsjn@mail.nih.gov
POC Phone	301.402.0914
Accept / Reject Status	
Question 6 Comment	
7. Is this a new or	New

existing system?	
8. Does the system have Security Authorization (SA)?	Yes
Accept / Reject Status	
Question 8 Comment	
8a. Date of Security Authorization	12/31/2017
9. Indicate the following reason(s) for updating this PIA. Choose from the following options.	
Other	
Accept / Reject Status	
Question 9 Comment	
10. Describe in further detail any changes to the system that have occurred since the last PIA.	The system's management changed substantially in 2018. The CC was using two different vendors for two clusters of websites that OCRTME was operating, Digital Infuzion and D'Vinci Interactive. The D'Vinci Interactive contract is no longer with NIH CC, but rather NIH OD (as of December 2018).
Accept / Reject Status	
Question 10 Comment	
11. Describe the purpose of the system.	This collection of administrative systems, known as Clinical Research Student records system (CRS), tracks applications from healthcare researchers, providers and administrators in training at the National Institutes of health (NIH) Clinical Center (CC) Office of Clinical Research Training and Medical Education's (OCRTME)

	undergraduate and graduate medical education programs. A third-party web application provider, under the direction of the Executive Director for Graduate Medical Education, provides online course registration functionality for NIH training programs and conduct Alumni tracking surveys for graduates of the NIH training programs, all sites hosted at NIH. The programs administered are as follows: Medical Research Scholars Program Graduate Medical Education Clinical Electives Program Doctor of Philosophy (Ph.D.) Summer Course Resident Electives Program Clinical Research Training Program (CRTP)/Alumni Survey
Accept / Reject Status	
Question 11 Comment	
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.)	The personally identifiable information (PII) collected includes name, personal mailing address, personal phone number, personal email address, educational records, and employment status. The information is not disseminated, and is used to process applicants for training programs sponsored by various Institutes and Centers (ICs) within the NIH. The information is submitted voluntarily by medical/dental students or physicians and is collected to determine the suitability of applicants for NIH clinical research training programs. Those solicited may be members of the general public. The system uses specific login information 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 (IMS), which combines the identity and authentication tools and capabilities used throughout the NIH enterprise. IMS maintains its own unique privacy impact assessment (PIA). The purpose of the IMS is to authenticate and authorize all users and computers in a Windows domain network; assigning and enforcing

	information security policies for all computers and installing or updating software. The IMS collects unique user names and passwords (user credentials) and stores them in an encrypted format. The IMS is an essential service which facilitates and governs network access to various resources.
Accept / Reject Status	
Question 12 Comment	
13. Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	This collection of administrative systems, known as Clinical Research Student records system (CRS), tracks applications from healthcare researchers, providers and administrators in training at the National Institutes of health (NIH) Clinical Center (CC) Office of Clinical Research Training and Medical Education's (OCRTME) undergraduate and graduate medical education programs. A third-party web application provider, under the direction of the Executive Director for Graduate Medical Education, provides online course registration functionality for NIH training programs and conduct Alumni tracking surveys for graduates of the NIH training programs, all sites hosted at NIH. The programs administered are as follows: Medical Research Scholars Program Graduate Medical Education Clinical Electives Program Doctor of Philosophy (Ph.D.) Summer Course Resident Electives Program Clinical Research Training Program (CRTP)/Alumni Survey The personally identifiable information (PII) collected includes name, personal mailing address, personal phone number, personal email address, educational records, and employment status. The information is not disseminated, and is used to process applicants for training programs sponsored by various Institutes and Centers (ICs) within the NIH. The information is submitted voluntarily by medical/dental students or physicians and is collected to determine the suitability of applicants for NIH clinical research training programs. Those solicited may be members of the

	general public. The system uses specific login information 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 (IMS), which combines the identity and authentication tools and capabilities used throughout the NIH enterprise. IMS maintains its own unique privacy impact assessment (PIA). The purpose of the IMS is to authenticate and authorize all users and computers in a Windows domain network; assigning and enforcing information security policies for all computers and installing or updating software. The IMS collects unique user names and passwords (user credentials) and stores them in an encrypted format. The IMS is an essential service which facilitates and governs network access to various resources.
Accept / Reject Status	
Question 13 Comment	
14. Does the system collect, maintain, use or share PII?	Yes
Accept / Reject Status	
Question 14 Comment	
15. Indicate the type of PII that the system will collect or maintain.	Name, E-Mail Address, Phone Numbers, Education Records, Mailing Address, Employment Status
Accept / Reject Status	
Question 15 Comment	

16. Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees, Public Citizens
Accept / Reject Status	
Question 16 Comment	
17. How many individuals' PII is in the system?	10,000-49,999
Accept / Reject Status	
Question 17 Comment	
18. For what primary purpose is the PII used?	For clinical research training programs and to evaluate the effectiveness / outcome of NIH clinical research training programs.
Accept / Reject Status	
Question 18 Comment	
19. Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	The information collected is used to validate the compliance of graduate medical education training programs sponsored by the Clinical Center with the requirements of external accrediting organizations, specifically the Accreditation Council for Graduate Medical Education located in Chicago, IL.
Accept / Reject Status	
Question 19 Comment	
20. Describe the function of the SSN.	SSN is not collected. It is acknowledged that SSN may appear on transcripts. This collection would be unsolicited and incidental. The SSN is never used and

	could be removed.
Accept / Reject Status	
Question 20 Comment	
20a. Cite the legal authority to use the SSN.	SSN is not collected.
21. Identify legal authorities governing information use and disclosure specific to the system and program.	42 USC 241, 263, 282
22. Are records on the system retrieved by one or more PII data elements?	Yes
Accept / Reject Status	
Question 22 Comment	
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:	09-25-0014, Clinical Research: Student Records, HHS/NIH/OD/OIR/OE
Published:	
Published:	
In Progress	No
23. Identify the sources of PII in the system.	In-Person, Hard Copy: Mail/Fax, Email, Online
Accept / Reject Status	

Question 23 Comment	
23a. Identify the OMB information collection approval number and expiration date.	OMB Number: 0925-0698 (Application Process for Clinical Research Training and Medical Education at the Clinical Center and its impact on Course and Training Program Enrollment and Effectiveness) The expiration date is 07/31/2020 and will be renewed.
24. Is the PII shared with other organizations?	Yes
Accept / Reject Status	
Question 24 Comment	
24a. Identify with whom the PII is shared or disclosed and for what purpose.	
Within HHS	Yes
	Applicant names within the system may be shared with other NIH institutes.
Other Federal Agency/Agencies	No
State or Local Agency/Agencies	No
Private Sector	No
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)).	There are no MOUs or ISAs for this system.

24c. Describe the procedures for accounting for disclosures.	
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.	Individuals self-select for application and make the affirmative action to visit the NIH website(s) in question. Applicants are notified at the website where data is collected that submission of information is voluntary but necessary for program application and consideration.
Accept / Reject Status	
Question 25 Comment	
26. Is the submission of PII by individuals voluntary or mandatory?	Voluntary
Accept / Reject Status	
Question 26 Comment	
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.	Individuals may opt out by not applying to the program.
Accept / Reject Status	
Question 27 Comment	
28. Describe the process to notify and obtain consent from	The information received from respondents is only used for the two purposes documented, evaluation for the purpose of selecting qualified participants and

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.	validation of compliance with the requirements of external accrediting organizations. No changes to the OCRTME program are likely to occur. If a change were to occur, applicant data would then be used to notify and obtain consent from applicants for any new use.
Accept / Reject Status	
Question 28 Comment	
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.	A Privacy Rights Complaint Form is available to individuals when they believe that their PII has been inappropriately used or disclosed. The Clinical Center's Privacy Office will review the complaint and respond to the concern within 30 business days. Complaints could also be submitted to the System Manager, who would investigate and share findings with CC Information Systems Security Officer (ISSO) and CC Privacy Officer.
Accept / Reject Status	
Question 29 Comment	
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.	OCRTME follows an auditing and accountability Standard Operating Procedure. The system owner regularly reviews and analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions (such as reporting security violations).

Accept / Reject Status	
Question 30 Comment	
31. Identify who will have access to the PII in the system and the reason why they require access.	
Users	Yes
	Users need access to screen program applicants.
Administrators	Yes
	Administrators do not have access to the applicant data but may have unforseen, incidental access in the performance of administrative functions.
Developers	No
Contractors	No
Others	No
32. Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Access to PII is assigned based upon job roles/responsibilities. A NIH Active Directory (AD) account login is required to gain access to the stored PII data. The access rights of the logged on user's AD account determines file system permissions and whether PII may be accessed. NIH Active Directory maintains its own unique PIA, including all legal authorities documented.
Accept / Reject Status	
Question 32 Comment	
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.	Appropriate access is granted to the system based on predefined roles and job descriptions, and administrative access is limited to authorized employees based on current roles. Dual factor authentication with NIH Personal Identity Verification (PIV) card and NIH Active Directory will occur at time of login to the NIH Network and 3M System. System owners are responsible for creating the proper security

	groups within their systems with the applicable permissions for group members to enforce least privilege.
Accept / Reject Status	
Question 33 Comment	
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.	All NIH employees and direct contractors must take the NIH Information Security Awareness Course and NIH Privacy Awareness Course prior to being granted access to NIH information resources. In addition, the Information Security and Privacy Awareness Refresher must be taken annually. Administrators and Privileged Users/Developers require additional security and privacy training specific to their roles and responsibilities. Determinations are made based on Role based access controls and least privilege.
Accept / Reject Status	
Question 34 Comment	
35. Describe training system users receive (above and beyond general security and privacy awareness training).	Application specific one-on-one peer training is provided as needed.
Accept / Reject Status	
Question 35 Comment	
36. Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring	Yes

adherence to privacy provisions and practices?	
Accept / Reject Status	
Question 36 Comment	
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 Intramural Records Retention Schedule. Medical Staff Credentialing Records, DAA-0443-2012-0007-0011, are temporary records that can be destroyed 30 years after cutoff, which is one year after the medical staff member leaves patient care. Records are maintained within this system for a time of no less than six years after a password is altered or an user account is terminated in accordance with National Archives and Records Administration (NARA) record retention schedule: 3.2.031, System access records; Systems requiring special accountability for access; DAA-GRS-2013-0006-0004
Accept / Reject Status	
Question 37 Comment	
38. Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Physical Controls: The information technology (IT) hardware used to host protected information is located 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 facilities security for security and environmental hazards. Technical Controls: 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. 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.
Accept / Reject Status	
Question 38 Comment	
39. Identify the publicly-available URL.	https://ocrtmeapps.cc.nih.gov/mrsp https://ocrtmeapps.cc.nih.gov/gme https://ocrtmeapps.cc.nih.gov/phdsummercourse/ https://ocrtmeapps.cc.nih.gov/rep/ https://ocrtmeapps.cc.nih.gov/survey
Accept / Reject Status	
Question 39 Comment	
40. Does the website have a posted privacy notice?	Yes
Accept / Reject Status	
Question 40 Comment	
40a. Is the privacy policy available in a machine-readable format?	No

41. Does the website use web measurement and customization technology?	No
Accept / Reject Status	
Question 41 Comment	
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).	
Web Beacons	No
Collects PII?	No
Web Bugs	No
Collects PII?	No
Session Cookies	Yes
Collects PII?	No
Persistent Cookies	No
Collects PII?	No
Other ...	
Collects PII?	Undefined
42. Does the website have any information or pages directed at children under the age of thirteen?	No
Accept / Reject Status	
Question 42 Comment	
42a. Is there a unique privacy policy for the website, and does the	Undefined

unique privacy policy address the process for obtaining parental consent if any information is collected?	
43. Does the website contain links to non-federal government websites external to HHS?	No
Accept / Reject Status	
Question 43 Comment	
43a. Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	Undefined
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.	
1. Are the questions on the PIA answered correctly, accurately, and completely?	
Reviewer Notes	
Accept / Reject Status	
Question 1 Comment	
2. Does the PIA	

appropriately communicate the purpose of PII in the system and is the purpose justified by appropriate legal authorities?	
Reviewer Notes	
Accept / Reject Status	
Question 2 Comment	
3. Do system owners demonstrate appropriate understanding of the impact of the PII in the system and provide sufficient oversight to employees and contractors?	
Reviewer Notes	
Accept / Reject Status	
Question 3 Comment	
4. Does the PIA appropriately describe the PII quality and integrity of the data?	
Reviewer Notes	
Accept / Reject Status	
Question 4 Comment	
5. Is this a candidate for PII minimization?	
Reviewer Notes	

Accept / Reject Status	
Question 5 Comment	
6. Does the PIA accurately identify data retention procedures and records retention schedules?	
Reviewer Notes	
Accept / Reject Status	
Question 6 Comment	
7. Are the individuals whose PII is in the system provided appropriate participation?	
Reviewer Notes	
Accept / Reject Status	
Question 7 Comment	
8. Does the PIA raise any concerns about the security of the PII?	
Reviewer Notes	
Accept / Reject Status	
Accept / Reject Status	
Question 8 Comment	
9. Is applicability of the Privacy Act captured correctly and is a	

SORN published or does it need to be?	
Reviewer Notes	
Accept / Reject Status	
Accept / Reject Status	
Question 9 Comment	
10. Is the PII appropriately limited for use internally and with third parties?	
Reviewer Notes	
Accept / Reject Status	
Question 10 Comment	
11. Does the PIA demonstrate compliance with all Web privacy requirements?	
Reviewer Notes	
Accept / Reject Status	
Question 11 Comment	
12. Were any changes made to the system because of the completion of this PIA?	
Reviewer Notes	
Accept / Reject Status	
Question 12 Comment	

General Comments	
Status and Approvals	
IC Status	IC Approved
OSOP Status	Undefined
OPDIV Senior Official for Privacy Signature	
HHS Senior Agency Official for Privacy	