PIA Assessment

1. OPDIV	NIH
2. PIA Unique Identifier	P-3996611-590386
2a. Name	NIEHS CareerTrac
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?	No
4. Does the system include a Website or online application available to and for the use of the general public?	No
Accept / Reject Status	Undefined
Question 4 Comment	
5. Identify the operator.	Agency
6. Point of Contact (POC)	
POC Title	Chief, Program Analysis Branch
POC Name	Christie H. Drew, Ph.D.
POC Organization	NIH/NIEHS/DERT/PAB
POC Email	drewc@niehs.nih.gov
POC Phone	984-287-3255
Accept / Reject Status	Undefined
Question 6 Comment	

7. Is this a new or existing system?	Existing
8. Does the system have Security Authorization (SA)?	Yes
Accept / Reject Status	Undefined
Question 8 Comment	
8a. Date of Security Authorization	08/28/2020
9. Indicate the following reason(s) for updating this PIA. Choose from the following options.	PIA Validation (PIA Refresh/Annual Review)
Other	
Accept / Reject Status	Undefined
Question 9 Comment	
10. Describe in further detail any changes to the system that have occurred since the last PIA.	Not Applicable.
Accept / Reject Status	Undefined
Question 10 Comment	
11. Describe the purpose of the system.	CareerTrac (CT) is a trainee tracking and evaluation system for several National Institutes of Health (NIH) Institutes. The goal of this system is to track long-term trainee outcomes for specific trainees supported by National Institute of Environment Health Sciences

	(NIEHS), National Cancer Institute (NCI), National Institute of General Medical Sciences (NIGMS), and Fogarty International Center (FIC). The system allows extramural and intramural Principal Investigators (PIs) to track trainee's accomplishments. Most extramural PIs are required to track outcomes for 10-15 years as a condition of their grant award. The agency will use this information to evaluate the long-term outcomes of training program investments, such as trainee productivity, career outcomes and successes and make recommendations for improvement. The information may be aggregated for reporting purposes to other organizations, such as the Department of Health and Human Services (DHHS), Congress and other organizations interested in training investments and outcomes. The source systems from which this data is initially obtained have Privacy Impact Assessments and all legal authorities are documented.
Accept / Reject Status	Undefined
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.)	(1) The system will collect, track, and report on information about NIH-supported trainees, such as trainee name, contact information, biographical information, training information, and subsequent career information. The system also supports tracking of trainees' accomplishments, such as fellowships, awards, employment, education, product of policy development, publications, funding received, presentations at conferences, and students mentored. (2) The agency will use this information to evaluate the long-term outcomes of training program investments and make recommendations for improvement. The information may be aggregated for reporting purposes to other organizations, such as DHHS, Congress and other organizations interested in training investments and outcomes. (3) The information contains personally identifiable information (PII). (4) Submission of personal information for trainees who are officially appointed to Institutional training grant programs supported by NIH and for trainees who are

	supported by grants that do not require formal appointments through X-Train. PII for Manager Users (Principal Investigators) - First and Last Name, e-mail, username, external user ID, role. PII for Mentors - First and Last Name, Commons ID, Country, Institution, Department, Degree, Role Start and End Year in system. PII for Trainees - First, Middle, and Last Name and Suffix; Email Addresses (primary and secondary if provided); login information (Commons ID, SRP ID); Country of Origin, Region; Address (City, State/Province, Country, Region, and Postal Code); Phone (primary and cell phone); funding (sources of Support, amount or periods of support); Education (Institution, Location of Institution, Degree or Nature of Training, Degree Date or Dates of Training/Attendance, Honors [to include title and number of honor or award, source and amount of funding associated with honor or award, country for source of support]); Training Experience (Career Skills, Career Level, NIH Field of Training, Research Area, Research Project Title); Work Information (Institution/Organization/Company, Location of Work and Region, Department, Title, Dates of Employment, Tenure Status, Fellowship Name, Fellowship Type); Program Information (Trainee Status, Start and End Year in system); Bibliography (article titles, journal name and volume, publication date month and year, page count, co-author names, PMID and PMCID, research country, training status when research conducted, mentor during research or publication)
Accept / Reject Status	Undefined
Question 12 Comment	
13. Provide an overview of the system and describe the information it will collect, maintain (store), or share, either	CareerTrac is a trainee tracking and evaluation system for several NIH Institutes. The goal of this system is to track long-term trainee outcomes for specific trainees supported by NIEHS, NCI, NIGMS, and FIC. The system allows extramural and intramural PIs to track trainee's accomplishments. Most extramural PIs are required to

permanently or temporarily.	track outcomes for 10 - 15 years as a condition of their grant award. We will use the system to conduct assessments and evaluations on trainee productivity, career outcomes, and successes. CareerTrac is a collaborative database used by multiple NIH Institutes and Centers (ICs), including NIEHS, NCI, NIGMS, FIC. This PIA covers all ICs. As new partners join the system, we will update the PIA accordingly. PII for Manager Users (Principal Investigators) - First and Last Name, e-mail, username, external user ID, role. PII for Mentors - First and Last Name, Commons ID, Country, Institution, Department, Degree, Role Start and End Year in system. PII for Trainees - First, Middle, and Last Name and Suffix; Email Addresses (primary and secondary if provided); login information (Commons ID, SRP ID); Country of Origin, Region; Address (City, State/Province, Country, Region, and Postal Code); Phone (primary and cell phone); funding (sources of Support, amount or periods of support); Education (Institution, Location of Institution, Degree or Nature of Training, Degree Date or Dates of Training/Attendance, Honors [to include title and number of honor or award, source and amount of funding associated with honor or award, country for source of support]); Training Experience (Career Skills, Career Level, NIH Field of Training, Research Area, Research Project Title); Work Information (Institution/Organization/Company, Location of Work and Region, Department, Title, Dates of Employment, Tenure Status, Fellowship Name, Fellowship Type); Program Information (Trainee Status, Start and End Year in system); Bibliography (article titles, journal name and volume, publication date month and year, page count, co-author names, PMID and PMCID, research country, training status when research conducted, mentor during research or publication)
Accept / Reject Status	Undefined
Question 13 Comment	

14. Does the system collect, maintain, use or share PII?	Yes
Accept / Reject Status	Undefined
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
	Training grant information (project ID, start/end dates, principal investigator), US Citizen/Permanent resident status, gender, ethnicity, race (for US citizens/residents), country of origin (for non-US citizens), employment history, training career histo
	Training Tracking Information: login information (Commons ID, SRP ID); Country of Origin, Region; Address (City, State/Province, Country, Region, and Postal Code); Phone (primary and cell phone); funding (sources of Support, amount or periods of support); Training Experience (Career Skills, Career Level, NIH Field of Training, Research Area, Research Project Title)
	Resume Information: Education (Institution, Location of Institution, Degree or Nature of Training, Degree Date or Dates of Training/Attendance, Honors [to include title and number of honor or award, source and amount of funding associated with honor or award, country for source of support]); Work Information (Institution/Organization/Company, Location of Work and Region, Department, Title, Dates of Employment, Tenure Status, Fellowship Name, Fellowship Type); Program Information (Trainee Status, Start and End Year in system); Bibliography (article titles, journal name and volume, publication date month and year, page count, co-author names, PMID and PMCID, research country, training status when research conducted, mentor during research or publication)
Accept / Reject Status	Undefined
Question 15 Comment	

16. Indicate the categories of individuals about whom PII is collected, maintained or shared.	Public Citizens
Accept / Reject Status	Undefined
Question 16 Comment	
17. How many individuals' PII is in the system?	10,000-49,999
Accept / Reject Status	Undefined
Question 17 Comment	
18. For what primary purpose is the PII used?	PII is used for program evaluation.
Accept / Reject Status	Undefined
Question 18 Comment	
19. Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	The secondary uses of PII are research and program improvement.
Accept / Reject Status	Undefined
Question 19 Comment	
20. Describe the function of the SSN.	Not Applicable.
Accept / Reject Status	Undefined

Question 20 Comment	
20a. Cite the legal authority to use the SSN.	Not Applicable.
21. Identify legal authorities governing information use and disclosure specific to the system and program.	5. U.S.C. 301; 42 U.S.C. secs. 217a, 241, 242, 248, 281, 282, 284, 284a, 285, 285b, 285c, 285d, 285e, 285f, 285g, 285h, 285i, 285j, 285k, 285l, 285m, 285n, 285o, 285p, 285q, 285r, 285s, 285t, 286, 287, 287b, 287c-21, 287d, 288, 35 U.S.C. 200-212, 48 CFR Subpart 15.3 and 37 CFR 401.1-16; and42 U.S.C. 217a, 241, 282(b)(6), 284a, and 288.
22. Are records on the system retrieved by one or more PII data elements?	Yes
Accept / Reject Status	Undefined
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:	09-25-0036 Extramural Awards and Chartered Advisory Committees (IMPAC 2), Contract Information (DCIS), and Cooperative Agreement Information
Published:	09-25-0225 NIH Electronic Research Administration (eRA)
Published:	
In Progress	Undefined
23. Identify the sources of PII in the system.	Within the OPDIV, Other (Non-Government Sources)
Accept / Reject Status	Undefined

Question 23 Comment	
23a. Identify the OMB information collection approval number and expiration date.	The Office of Management and Budget (OMB) approval number is 0925-0568, with an expiration date of 04/30/2021.
24. Is the PII shared with other organizations?	Yes
Accept / Reject Status	Undefined
Question 24 Comment	
24a. Identify with whom the PII is shared or disclosed and for what purpose.	
Within HHS	No
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)).	
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.	Trainees are notified at the time they are appointed to the program via X-Train of the PII collected about them, based on the conditions of their awards. For all other trainees entered into the system, CareerTrac will provide an electronic notification to trainees about the purpose of the PII collected, its use and how it will be shared.
Accept / Reject Status	Undefined
Question 25 Comment	
26. Is the submission of PII by individuals voluntary or mandatory?	Voluntary
Accept / Reject Status	Undefined
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.	Trainees have the option not to participate in the program.

Data is placed into CareerTrac by the principal investigators on a voluntary basis.   PIs using CareerTrac are required to report on trainee data.   The appointment process (now managed through X-Train/IMPAC II) includes a standard privacy statement informing trainees about the existence of the system and about the use of the information.   Trainees may ask PI's to review their records, and may refuse to provide information, but they may not opt out of the system, because their PIs are required to track them. A new trainee portal will provide trainees with an optional way to submit data. Expected release of trainee portal winter 2021. |
| Accept / Reject Status | Undefined |
| | |

Question 27 Comment	
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.	NIEHS does not anticipate major changes to the system that would affect disclosure and/or changes in data use. However, if a major change in disclosure were to occur, users and trainees would be notified via email form letter based on the email listed in CareerTrac.
<u>Accept / Reject Status</u>	Undefined
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.	The trainee will write to their PI who will in turn forward the request to CareerTrac staff. The trainee should reasonably identity the record and specify the information being contested, the corrective action sought, and the reasons for requesting the correction, along with supporting information to show how the record is inaccurate or incomplete. The right to contest records is limited to information which is incomplete or inaccurate.
<u>Accept / Reject Status</u>	Undefined
Question 29 Comment	
30. Describe the process in place for periodic reviews of PII contained in the system to ensure the	Principal Investigators (PIs) have access to the system and are responsible for updating the information submitted. PIs can easily export trainee data from the system to provide the right of review. NIH program officials periodically review reports for the programs to

data's integrity, availability, accuracy and relevancy. If no processes are in place, explain why not.	ensure data quality.
Accept / Reject Status	Undefined
Question 30 Comment	

31. Identify who will have access to the PII in the system and the reason why they require access.	
Users	Yes
	Data entry, review, report and update. (Note: Users only have access to PII for the trainees associated with their Institution - they may NOT view PII for trainees funded by other organizations.)
Administrators	Yes
	Manage user accounts, system level data, data analysis and integrity
Developers	Yes
	Application maintenance and enhancements
Contractors	Yes
	For directed evaluation purposes
Others	Yes
	Program Officers have access to PII so that they can evaluate the effectiveness of training programs.
32. Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Users are assigned access in the system based on their role in the organization & reporting process. These roles are strictly controlled and limit access with the application.
Accept / Reject Status	Undefined
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.	Users are assigned access in the system based on their role in the organization & reporting process. These roles are strictly controlled and limit access with the application.
Accept / Reject Status	Undefined
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.	NIEHS has annual and refresher training for security and privacy awareness via Collaborative Institutional Training Initiative (CITI). According to NIH policy, all personnel who use NIH applications must attend security awareness training every year. There are five categories of mandatory IT training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Preparedness).
Accept / Reject Status	Undefined
Question 34 Comment	
35. Describe training system users receive (above and beyond general security and privacy awareness training).	CareerTrac staff regularly provide information sessions and training for users at grantee meetings and through webinars. We maintain robust help files, FAQs and have provided extensive tool tips within the system itself.
Accept / Reject Status	Undefined
Question 35 Comment	

36. Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
<u>Accept / Reject Status</u>	Undefined
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.	The post-award tracking requirements of the T32 grant program requires that the awardee's career be tracked for at least 15 years after the grant. CareerTrac is used to collect and track data in association with those grantees. As such, the records generated by this system appear to fall within the NIH Records Schedule, 02-005, Official Case Files of Applications and Awards, Appeals, and Litigation Records for Grants, Cooperative Agreements, and Other Transaction Activities.

The disposition of such records is to cut off annually following completion of final award-related activity that represents closing of the case file (e.g., end of project period, completed final peer review, litigation or appeal proceedings concluded) and to destroy the records 30 year(s) after cutoff.   This record schedule is the most appropriate approved schedule available for use with this requirement; however, further refinement to the retention requirements of these records may change, based on further discussion regarding records management. |
<u>Accept / Reject Status</u>	Undefined
Question 37 Comment	
38. Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical	Infrastructure: this system is supported by the NIEHS General Support System (GSS), located in the NIEHS datacenter that is on a Federal government campus, protected by armed guards, and behind secured doors where all entry and exit is tracked, monitored, and restricted to authorized individuals only (monitoring is

controls.	24/7). Physical Controls: The information technology (IT) hardware used to host protected survey 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: The IT hardware and software used to host the protected survey information 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 training and awareness classes and refreshers. Personnel accessing these systems use privileged and separate accounts for administrative access to systems. Security and Privacy Controls - Applied and Audited: The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the United States Department of Commerce that provides guidance to help federal agencies manage their information security systems. NIST issues Special Publications (SP) to relay specific guidelines and/or standards. To help federal agencies meet requirements set by the Federal Information Security Management Act (FISMA), NIST SP 800-53 defines standards and guidelines for the protection of agency's and citizen's private data. It includes security and privacy controls to be implemented as part of an organization-wide process that manages information security and privacy risk. The NIST SP 800-53 security

	and privacy controls will be applied and audited.
Accept / Reject Status	Undefined
Question 38 Comment	
39. Identify the publicly-available URL.	https://careertrac.niehs.nih.gov/public/home
Accept / Reject Status	Undefined
Question 39 Comment	
40. Does the website have a posted privacy notice?	Yes
Accept / Reject Status	Undefined
Question 40 Comment	
40a. Is the privacy policy available in a machine-readable format?	Yes
41. Does the website use web measurement and customization technology?	Yes
Accept / Reject Status	Undefined
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	Yes
Collects PII?	No
Web Bugs	No
Collects PII?	No
Session Cookies	Yes
Collects PII?	No
Persistent Cookies	Yes
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	Undefined
Question 42 Comment	
42a. Is there a unique privacy policy for the website, and does the 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	Undefined

Question 43 Comment	
43a. Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	

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?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
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?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Question 2 Comment	
3. Do system owners demonstrate appropriate	Undefined

understanding of the impact of the PII in the system and provide sufficient oversight to employees and contractors?	
Reviewer Notes	
Accept / Reject Status	Undefined
Question 3 Comment	
4. Does the PIA appropriately describe the PII quality and integrity of the data?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Question 4 Comment	
5. Is this a candidate for PII minimization?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Question 5 Comment	
6. Does the PIA accurately identify data retention procedures and records retention schedules?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Question 6 Comment	

7. Are the individuals whose PII is in the system provided appropriate participation?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Question 7 Comment	
8. Does the PIA raise any concerns about the security of the PII?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Accept / Reject Status	Undefined
Question 8 Comment	
9. Is applicability of the Privacy Act captured correctly and is a SORN published or does it need to be?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Accept / Reject Status	Undefined
Question 9 Comment	
10. Is the PII appropriately limited for use internally and with third parties?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined

Question 10 Comment	
11. Does the PIA demonstrate compliance with all Web privacy requirements?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Question 11 Comment	
12. Were any changes made to the system because of the completion of this PIA?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
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	