1. OPDIV	National Institutes of Health
2. PIA Unique Identifier	
2a. Name	NEI Electronic Individual Development Plan
3. The subject of this PIA is which of the following?	Tier 4
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	
Question 4 Comment	
5. Identify the operator.	Agency
6. Point of Contact (POC)	
POC Title	Training Director
POC Name	Cesar Perez-Gonzalez
POC Organization	National Eye Institute, NIH
POC Email	cesarp@nei.nih.gov
POC Phone	301-827-7755
Accept / Reject Status	
Question 6 Comment	
7. Is this a new or existing system?	New
8. Does the system have Security Authorization (SA)?	Yes
Accept / Reject Status	

Question 8 Comment	
8a. Date of Security Authorization	Jan 29, 2020
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.	
Accept / Reject Status	
Question 10 Comment	
11. Describe the purpose of the system.	The electronic Individual Development Plan (eIDP) system is used by the National Eye Institute's (NEI) intramural training program to help fellows and trainees identify their career goals and professional development needs.
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 majority of the Personally Identifiable Information (PII) information comes from NIH Enterprise Directory (NED), the NIH Fellowship Payment System (FPS), and NIH nVision. Personally Identifiable Information (PII) includes name, email, phone number, race, and gender and ethnicity (optional). eIDP 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), formerly known as the Active Directory (AD), which combines the identity and authentication tools and capabilities used throughout the NIH enterprise. The IMS has its own approved PIA on record, including all legal authorities documented.
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.	The electronic Individual Development Plan (eIDP) system is used by the National Eye Institute's (NEI) intramural training program to help fellows and trainees identify their career goals and professional development needs. The majority of the Personally Identifiable Information (PII) information comes from NIH Enterprise Directory (NED), the NIH Fellowship Payment System (FPS), and NIH nVision. Personally Identifiable Information (PII) includes name, email, phone number, race, and gender and ethnicity (optional). eIDP 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), formerly known as the Active Directory (AD), which combines the identity and authentication tools and capabilities used throughout the NIH enterprise. The IMS has its own approved PIA on record, including all legal authorities documented.
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	Name, E-Mail Address, Phone Numbers, Gender, Race and ethnicity

or maintain.	
Accept / Reject Status	
Question 15 Comment	
16. Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees
Accept / Reject Status	
Question 16 Comment	
17. How many individuals' PII is in the system?	100-200
Accept / Reject Status	
Question 17 Comment	
18. For what primary purpose is the PII used?	The PII information used by the eIDP system identifies NEI Trainees and Fellows that need to create an Individual Development Plan (IDP). The PII data is used to identify the NEI staff. The gender and race of the staff is used for aggregate data reporting.
Accept / Reject Status	
Question 18 Comment	
19. Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	N/A
Accept / Reject Status	
Question 19 Comment	

20. Describe the function of the SSN.	N/A
Accept / Reject Status	
Question 20 Comment	
20a. Cite the legal authority to use the SSN.	N/A
21. Identify legal authorities governing information use and disclosure specific to the system and program.	42 U.S.C. 241(d), 281
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:	09-25-0216 NIH Electronic Directory (NED)
Published:	
Published:	
In Progress	
23. Identify the sources of PII in the system.	Online, Within the OPDIV
Accept / Reject Status	
Question 23 Comment	
23a. Identify the OMB information collection approval number and expiration date.	An OMB collection approval number is not needed as the eIDP Website/Database only uses the PII of federal employees for internal use only.

24. Is the PII shared with other organizations?	No
Accept / Reject Status	
Question 24 Comment	
24a. Identify with whom the PII is shared or disclosed and for what purpose.	
Within HHS	N/A
Other Federal Agency/Agencies	N/A
State or Local Agency/Agencies	N/A
Private Sector	N/A
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)).	N/A
24c. Describe the procedures for accounting for disclosures.	N/A
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.	PII data is sourced from existing, assess and approved NIH systems (NED, FPS, NIH nVision). Trainees will enter additional PII information that is not found in any NIH systems (gender, race, and ethnicity, at their option). The Trainees will submit the completed IDP for approval. The individuals will review all data that the system stores prior to their approval of the final submitted IDP. Sources systems maintain their own HHS Approved Privacy Impact Assessments, including all legal authorities documented.
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.	It is optional for the Trainees to complete an IDP. However, this can potentially disqualify them from the fellowship program since it is a requirement of the program. Information that is pulled from source systems offer opt-out options during their PII submission processes. All source systems maintain their own HHS Approved PIAs, with legal authorities documented.
Accept / Reject Status	
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.	NEI Trainees will have the opportunity to view changes to their PII information during the IDP renewal process. They will go through a submission and approval process for IDP renewals. They will know when a change occurs during the renewal period. Information that is pulled from source systems obtain consent during their PII submission processes. All source systems maintain their own HHS Approved PIAs, with legal authorities documented.
Accept / Reject Status	
Question 28 Comment	
29. Describe the process in place to resolve an individual's concerns when	The eIDP System source of most of the PII data is from NIH systems. The additional PII information requested from the Trainee is optional. The Trainee does not have to enter the optional PII data.

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 can update their PII information by logging into NED and/or contacting their Administrative Officer to update incorrect PII data.
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.	The PIA review will be conducted each time major eIDP functionalities are released that utilizes addition data (NED, nVision) or new PII data beyond the data included in the previous PIA. Minimally, a PIA review will be conducted yearly.
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
	Trainees, mentors, administrative officers complete and view the eIDP as it goes through the system.
Administrators	Yes
	Responsible for access control.
Developers	Yes
	Testing and customer defect resolution.
Contractors	
Others	
32. Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	All requests for access to the eIDP system will be assigned an appropriate profile (role) and approved by the System Owner before being implemented by the technical support team.
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.	Role based access controls are used to limit users' access to PII based on their defined job function and system role.
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.	The NIH Security Awareness Training course is used to satisfy this requirement. According to NIH policy, all personnel who use NIH applications must attend security awareness training every year. There are four categories of mandatory IT training (Information Security, Counterintelligence, Privacy Awareness, and Records Management). Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials.
Accept / Reject Status	
Question 34 Comment	
35. Describe training system users receive (above and beyond general security and privacy awareness training).	None
Accept / Reject Status	
Question 35 Comment	
36. Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy	Yes

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 maintained within eIDP until superseded, 3 years old, or 1 year after separation, in accordance with the National Archives and Records Administration (NARA) approved disposition schedule: DAA-GRS-2016- 0014-0003.
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.	Administrative safeguards: NIH staff take mandatory security and privacy training and include system security and contingency plan. Access is via least privilege through role-based access, and policies for retention and destruction of PII are in place. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job. Files are backed up regularly and stored offsite. Contract clauses ensure adherence to privacy provisions and practices. Physical Safeguards: Physical access to the system is controlled by security guards, employee badging, proximity cards, card readers, and security cameras. Access to the server is controlled by card readers at the server room door. There is a battery backup for power until the backup generator starts. Fire protection including sprinklers, and flooding sensors at the floor level. Technical Controls: Technical Safeguards include restricting files using secure socket layer encryption, a two-factor authentication and role-based access controls.
Accept / Reject Status	
Question 38 Comment	
39. Identify the publicly-available URL.	N/A

Accept / Reject Status	
Question 39 Comment	
40. Does the website have a posted privacy notice?	N/A
Accept / Reject Status	
Question 40 Comment	
40a. Is the privacy policy available in a machine-readable format?	N/A
41. Does the website use web measurement and customization technology?	N/A
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	
Collects PII?	
Web Bugs	
Collects PII?	
Session Cookies	
Collects PII?	
Persistent Cookies	
Collects PII?	
Other ...	
Collects PII?	

42. Does the website have any information or pages directed at children under the age of thirteen?	N/A
Accept / Reject Status	
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?	N/A
43. Does the website contain links to non-federal government websites external to HHS?	N/A
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?	N/A
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	Undefined
OSOP Status	Undefined
OPDIV Senior Official for Privacy Signature	
HHS Senior Agency Official for Privacy	