Save

Privacy Impact Assessment Form

v 1.47.4

Status | Form Number | Form Date

	Question	Answer		
1	OPDIV:			
2	PIA Unique Identifier:			
2a	Name:	NIH Workplace Civility and Equity Survey		
3	The subject of this PIA is which of the following?	○ General Support System (GSS) ○ Major Application ○ Minor Application (stand-alone) ○ Minor Application (child) ◉ Electronic Information Collection ○ Unknown		
3a	Identify the Enterprise Performance Lifecycle Phase of the system.	Development		
3b	Is this a FISMA-Reportable system?	○ Yes ◉ No		
4	Does the system include a Website or online application available to and for the use of the general public?	○ Yes ◉ No	◉ Accept ○ Reject	
5	Identify the operator.	○ Agency ◉ Contractor		
6	Point of Contact (POC):	POC Title: Chief, Strategic Workforce Analytics and Engagement Branch POC Name: Jonathan Lappin POC Organization: NIH/OD/OM/OHR/Workforce Support and Development Division POC Email: lappinjo@od.hih.gov POC Phone: 301-435-7562	◉ Accept ○ Reject	
7	Is this a new or existing system?	◉ New ○ Existing		
8	Does the system have Security Authorization (SA)?	◉ Yes ○ No	◉ Accept ○ Reject	

Save

8a	Date of Security Authorization	01/03/2022	
11	Describe the purpose of the system.	The system will use the Qualtrics SaaS platform to collect data via a web survey from all NIH employees, contractors, trainees and special volunteers about their experiences of harassment and discrimination at NIH. The system will track response and will provide a response dashboard that will be accessible by authorized users at NIH. The response dashboard will indicate the response rates to the survey by Institute and Center (IC). Qualtrics has FedRAMP certification at a moderate impact level that expires 4/1/2023	(•) Accept ( ) Reject
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 system will maintain respondent name, NIH email address, organizational code, NIH Enterprise Directory (NED) ID, and IC in addition to their survey responses. To support authentication, the systems assigns and stores personal	(•) Accept ( ) Reject
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	Respondent name, NIH email address, organizational code, NED ID, and IC will be maintained in the system in order to track response to the survey by IC. Demographic information	(•) Accept ( ) Reject
14	Does the system collect, maintain, use or share **PII**?	(•) Yes ( ) No	(•) Accept ( ) Reject
15	Indicate the type of PII that the system will collect or maintain.	[ ] Social Security Number [ ] Date of Birth [x] Name [ ] Photographic Identifiers [ ] Driver's License Number [ ] Biometric Identifiers [ ] Mother's Maiden Name [ ] Vehicle Identifiers [x] E-Mail Address [ ] Mailing Address [ ] Phone Numbers [ ] Medical Records Number [ ] Medical Notes [ ] Financial Account Info [ ] Certificates [ ] Legal Documents [ ] Education Records [ ] Device Identifiers [ ] Military Status [ ] Employment Status [ ] Foreign Activities [ ] Passport Number [ ] Taxpayer ID Institute or Center (IC) Role at NIH (employee, contractor, trainee, volunteer) Organizational code, PINs, Usernames, Passwords NED ID Race, Age, Length of Employment	(•) Accept ( ) Reject
16	Indicate the categories of individuals about whom PII is collected, maintained or shared.	[x] Employees [ ] Public Citizens [ ] Business Partners/Contacts (Federal, state, local agencies) [x] Vendors/Suppliers/Contractors [ ] Patients Other: trainees and special volunteers	(•) Accept ( ) Reject

Save

17	How many individuals' PII is in the system?	10,000-49,999	(•) Accept ( ) Reject
18	For what primary purpose is the PII used?	Name, email address, IC and PIN are used to track survey completion. Role at NIH is used to provide the proper survey pathway for the respondent.	(•) Accept ( ) Reject
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	IC and role at NIH will be used in aggregate during analyses.	(•) Accept ( ) Reject
20	Describe the function of the SSN.	not applicable	(•) Accept ( ) Reject
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.	As covered under NIH SORN 09-25-0156, authority for this system comes from the authorities regarding the establishment of the National Institutes of Health, its general authority to conduct and fund research and to provide training assistance, and its general authority to maintain records in connection with these and its other functions (42 U.S.C. 203, 241, 289l-1 and 44 U.S.C. 3101), and Section 301 and 493 of the Public Health Service Act.	(•) Accept ( ) Reject
22	Are records on the system retrieved by one or more PII data elements?	(•) Yes ( ) No	(•) Accept ( ) Reject
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: SORN 09-25-0156, Records of Participants in Programs and Responses in Surveys Used to Evaluate Programs of the Public Health Service Published: Published: ☐ In Progress	

Save

23	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains ☐ In-Person ☐ Hard Copy: Mail/Fax ☐ Email ☒ Online ☐ Other Government Sources ☒ Within the OPDIV ☐ Other HHS OPDIV ☐ State/Local/Tribal ☐ Foreign ☐ Other Federal Entities ☐ Other Non-Government Sources ☐ Members of the Public ☐ Commercial Data Broker ☐ Public Media/Internet ☒ Private Sector ☐ Other	◉ Accept ○ Reject
23a	Identify the OMB information collection approval number and expiration date.	OMB review underway	
24	Is the PII shared with other organizations?	○ Yes ◉ No	◉ Accept ○ Reject
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.	Information about the survey, including the privacy and use of data, is provided to respondents via email when invited to take the survey.	◉ Accept ○ Reject
26	Is the submission of PII by individuals voluntary or mandatory?	◉ Voluntary ○ Mandatory	◉ Accept ○ Reject
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.	Respondents choose whether to complete the web survey. Participation is completely voluntary.	◉ Accept ○ Reject
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.	Completion and return of the survey is considered to be consent to participate. No changes in disclosure or data use will be permitted without explicit consent from each survey respondent.	◉ Accept ○ Reject
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.	Respondents are provided with an email address they can contact with any concerns or questions.	◉ Accept ○ Reject
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.	System functionality, security, and accuracy are tested during system development and subsequently tested at regular intervals throughout the survey period.	◉ Accept ○ Reject

Save

31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users	Westat staff will manage sending of email invitations, review status of survey completions, and respond to emails to the Help Desk.	◉ Accept ○ Reject
		☒ Administrators	Westat IT professionals will manage the system and provide support.	
		☒ Developers	Westat IT professionals will trouble-shoot system problems.	
		☒ Contractors	The project is conducted directly by Westat on behalf of NIH.	
		☐ Others		
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Individuals are granted rights to the information in the system by the project director, who determines need-to-know based on the kind of job the person is doing and the particular requirements of the tasks assigned to that person.		◉ Accept ○ Reject
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.	User roles are defined and individuals are assigned to one or more roles. These roles ensure that access privileges are narrowly defined, and that only those staff members that need certain types of access are granted that access. In addition to limiting functions, physical access controls limit access to the system.		◉ Accept ○ Reject
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 manage or operate NIH applications or systems must attend complete security awareness training every year. There are five categories of mandatory IT training (Information Security, Counterintelligence, Privacy Awareness, Records Management, and Emergency Preparedness). Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials.		◉ Accept ○ Reject
35	Describe training system users receive (above and beyond general security and privacy awareness training).	Role-based security and privacy training is assigned as required by agency policy and direction by the system owner. Key staff participate in a yearly Contingency Planning and Incident Response (CP/IR) training.		◉ Accept ○ Reject
36	Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?	◉ Yes ○ No		◉ Accept ○ Reject

Save

37	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.	Records are retained and disposed of under the authority of the NIH Records Control Schedule Item 06-202 (DAA-GRS-2017-0007-0002). Workforce and succession planning records. Records about workforce planning and analysis, including succession planning, developed in support of executive-level and other agency planning initiatives. Includes planning and analysis models, planning data, briefing materials, studies and surveys, and lists of functions and staff at key locations. Destroy 3 years after issuing each new plan, but longer retention is authorized if required for business use. The contract's schedule for data retention is as follows "The disposition to be made of the Privacy Act records upon completion of task order performance is to post the data in Lexical where it will be maintained for five years. The contractor will ask for, receive, and clean the data for the next administration."	(•) Accept ( ) Reject
38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Administrative Controls: Administrators control account request and approval; annual trainings for cybersecurity education and awareness, incident reporting (IR), and contingency planning (CP); and annual review of the IR and CP plans. Procedures for onboarding and terminating staff. Technical Controls: Access to the information is controlled by role-based authentication. All servers have been configured to remove all unused applications and system files and all local account access except when necessary to manage the system and maintain integrity of data. Physical Controls: The servers reside in the contractor Westat's data center located in Rockville Maryland where policies, systems and procedures are in place to restrict access to and safeguard the data centers such as the use of magnetic key cards by all staff to access buildings and diesel-powered backup generators support the continuous operation of the data centers in case of long-term utility power failures.	(•) Accept ( ) Reject

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

	Reviewer Questions	Answer	
1	Are the questions on the PIA answered correctly, accurately, and completely?	( ) Yes ( ) No	(•) Accept ( ) Reject
Reviewer Notes			
2	Does the PIA appropriately communicate the purpose of PII in the system and is the purpose justified by appropriate legal authorities?	( ) Yes ( ) No	(•) Accept ( ) Reject
Reviewer Notes			

Save

	Reviewer Questions	Answer	
3	Do system owners demonstrate appropriate understanding of the impact of the PII in the system and provide sufficient oversight to employees and contractors?	◯ Yes ◯ No	◉ Accept ◯ Reject
Reviewer Notes			
4	Does the PIA appropriately describe the PII quality and integrity of the data?	◯ Yes ◯ No	◉ Accept ◯ Reject
Reviewer Notes			
5	Is this a candidate for PII minimization?	◯ Yes ◯ No	◉ Accept ◯ Reject
Reviewer Notes			
6	Does the PIA accurately identify data retention procedures and records retention schedules?	◯ Yes ◯ No	◉ Accept ◯ Reject
Reviewer Notes			
7	Are the individuals whose PII is in the system provided appropriate participation?	◯ Yes ◯ No	◉ Accept ◯ Reject
Reviewer Notes			
8	Does the PIA raise any concerns about the security of the PII?	◯ Yes ◯ No	◉ Accept ◯ Reject
Reviewer Notes			
9	Is applicability of the Privacy Act captured correctly and is a SORN published or does it need to be?	◯ Yes ◯ No	◉ Accept ◯ Reject
Reviewer Notes			
10	Is the PII appropriately limited for use internally and with third parties?	◯ Yes ◯ No	◉ Accept ◯ Reject
Reviewer Notes			
11	Does the PIA demonstrate compliance with all Web privacy requirements?	◯ Yes ◯ No	◉ Accept ◯ Reject
Reviewer Notes			
12	Were any changes made to the system because of the completion of this PIA?	◯ Yes ◯ No	◉ Accept ◯ Reject
Reviewer Notes			

Save

General Comments	

OPDIV Senior Official for Privacy Signature	Celeste E. Dade-vinson -S Digitally signed by Celeste E. Dade-vinson -S Date: 2022.05.18 14:16:24 -04'00'	HHS Senior Agency Official for Privacy	

Third-Party Website Assessment PIA Form

v 1.47.4

Status | Form Number: Read Only | Form Date: Read Only

	Question	Answer	
1	OPDIV:	Read Only - OPDIV	
2	TPWA Unique Identifier (UID):	Read Only - TPWA UID	
3	TPWA Name:	Read Only - TPWA Name	
4	Is this a new TPWA?	○ Yes ○ No	
4a	Please provide the reason for revision		
5	Will the use of a third-party Website or application create a new or modify an existing HHS/OPDIV System of Records Notice (SORN) under the Privacy Act?	○ Yes ○ No	◉ Accept ○ Reject
5a	Indicate the SORN number (or identify plans to put one in place.)	SORN Number: If not published:	
6	Will the use of a third-party Website or application create an information collection subject to OMB clearance under the Paperwork Reduction Act (PRA)?	○ Yes ○ No	◉ Accept ○ Reject
6a	Indicate the OMB approval number and approval number expiration date (or describe the plans to obtain OMB clearance.)	OMB Approval Number Expiration Date Explanation	
7	Does the third-party Website or application contain Federal Records?	○ Yes ○ No	◉ Accept ○ Reject

Save

8	Point of Contact (POC):	POC Title POC Name POC Organization POC Email POC Phone	(•) Accept ( ) Reject
9	Describe the specific purpose for the OPDIV use of the third-party Website or application:		(•) Accept ( ) Reject
10	Have the third-party privacy policies been reviewed to evaluate any risks and to determine whether the Website or application is appropriate for OPDIV use?	( ) Yes ( ) No	(•) Accept ( ) Reject
11	Describe alternative means by which the public can obtain comparable information or services if they choose not to use the third-party Website or application:		(•) Accept ( ) Reject
12	Does the third-party Website or application have appropriate branding to distinguish the OPDIV activities from those of nongovernmental actors?	( ) Yes ( ) No	(•) Accept ( ) Reject
13	How does the public navigate to the third party Website or application from the OPIDIV?		(•) Accept ( ) Reject
13a	Please describe how the public navigate to the third-party website or application:		
13b	If the public navigate to the third-party website or application via an external hyperlink, is there an alert to notify the public that they are being directed to a nongovernmental Website?	( ) Yes ( ) No	
14	Has the OPDIV Privacy Policy been updated to describe the use of a third-party Website or application?	( ) Yes ( ) No	(•) Accept ( ) Reject
14a	Provide a hyperlink to the OPDIV Privacy Policy:		
15	Is an OPDIV Privacy Notice posted on the third-party Website or application?	( ) Yes ( ) No	(•) Accept ( ) Reject
15a	Confirm that the Privacy Notice contains all of the following elements: (i) An explanation that the Website or application is not government-owned or government-operated; (ii) An indication of whether and how the OPDIV will maintain, use, or share PII that becomes available; (iii) An explanation that by using the third-party Website or application to communicate with the OPDIV, individuals may be providing nongovernmental third-parties with access to PII; (iv) A link to the official OPDIV Website; and (v) A link to the OPDIV Privacy Policy	( ) Yes ( ) No	
15b	Is the OPDIV's Privacy Notice prominently displayed at all locations on the third-party Website or application where the public might make PII available?	( ) Yes ( ) No	

Save

16	Is PII collected by the OPDIV from the third-party Website or application?	◯ Yes ◯ No	◉ Accept ◯ Reject
17	Will the third-party Website or application make PII available to the OPDIV?	◯ Yes ◯ No	◉ Accept ◯ Reject
18	Describe the PII that will be collected by the OPDIV from the third-party Website or application and/or the PII which the public could make available to the OPDIV through the use of the third-party Website or application and the intended or expected use of the PII:		◉ Accept ◯ Reject
19	Describe the type of PII from the third-party Website or application that will be shared, with whom the PII will be shared, and the purpose of the information sharing:		◉ Accept ◯ Reject
19a	If PII is shared, how are the risks of sharing PII mitigated?		
20	Will the PII from the third-party Website or application be maintained by the OPDIV?	◯ Yes ◯ No	◉ Accept ◯ Reject
20a	If PII will be maintained, indicate how long the PII will be maintained:		
21	Describe how PII that is used or maintained will be secured:		◉ Accept ◯ Reject
22	What other privacy risks exist and how will they be mitigated?		◉ Accept ◯ Reject

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

	Reviewer Questions	Answer	
1	Are the responses accurate and complete?	◯ Yes ◯ No	◉ Accept ◯ Reject
Reviewer Notes			
2	Is the TPWA compliant with all M-10-23 requirements, including appropriate branding and alerts?	◯ Yes ◯ No	◉ Accept ◯ Reject
Reviewer Notes			
3	Has the OPDIV posted an updated privacy notice on the TPWA and does it contain the five required elements?	◯ Yes ◯ No	◉ Accept ◯ Reject
Reviewer Notes			

Save

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.

4	Does the PIA clearly identify PII made available and/or collected by the TPWA?	◯ Yes ◯ No	◉ Accept ◯ Reject
Reviewer Notes			
5	Is the handling of PII appropriate?	◯ Yes ◯ No	◉ Accept ◯ Reject
Reviewer Notes			
General Comments			

OPDIV Senior Official for Privacy Signature		HHS Senior Agency Official for Privacy	