OPM Privacy Threshold Analysis

OPIM will use this form to determine whether a new or updated Privacy Impact Assessment (PIA) is required and whether a new or updated System of Records Notice (SORN) is required under the Privacy Act of 1974. OPIM will also use it to document the continuous monitoring of privacy risk and mitigation for the project, program, or system.

Please complete the form and submit it to PIAMail@opm.gov. Upon receipt of this PTA, the Chief Privacy Officer, or designee, will adjudicate the PTA and return it to you. As appropriate, you will be provided with further guidance on completing a PIA and SORN.

Summary Information

Date of Completion:	02/16/2024		
Project or Program Name:	USA Performance (USAP)		
Office:	Human Resources Solutions		
Branch/Group:	HRS		
Type of Project or Program:	System	Project/ Program status:	Existing
Date first developed:	07/01/2014		
Pilot launch date:		Pilot end date:	
PTA last updated:	03/29/2023		
ATO Status (if applicable):	Complete	ATO expiration date (if applicable):	06/15/2024

Project, Program, or System Manager

Name:	Ryan Hendricks		
Office Acronym:	HRS	Title:	USAP Product Development
Phone:	(202) 422-3066	Email:	Ryan.Hendricks@opm.gov

Information System Security Officer (ISSO) (if applicable)

Name:	Thomas Fiifi Koomson		
Phone:	(313) 358-5860	Email:	Thomas.Koomson@opm.gov

Specific PTA Questions

1. Overview:
Please provide a detailed description of the project, program or system and its purpose in a way a non-technical person could understand. The description should include the purpose of the project, which individuals are involved or impacted, a general lifecycle of the data, where the data is stored, and any collection instruments (e.g., forms, mobile application) used to collect information, as well as any other information needed to describe the project. If this is an updated PTA due to changes in a project, please describe the specific changes and/or upgrades that are triggering the update. If this is a renewal PTA due to an impending expiration, please state whether there were any changes since the last PTA approval.
USA Performance is the U.S. Office of Personnel Management's software solution to assist Federal agencies in implementing their Senior Executive Service (SES) and Non-SES performance management programs and systems. It offers a core suite of functionalities that meet a variety of agency performance management processes while ensuring compliance with Federal regulations and consistency with OPM recommendations. The system enables agencies to automate their performance appraisal process throughout the performance rating cycle. Agencies can also develop performance plans, track and monitor employees' performance, provide feedback and ratings, and electronically sign off on performance plans as agency appraisal programs require. USA Performance (USAP) is a user-friendly, web-based application that includes customizable advanced features. The system is managed by the Performance Management Solutions section of the Office of Personnel Management's (OPM) Human Resources Solutions. The purpose of the system is to assist managers in federal government agencies with their performance management initiatives and

2. From whom does the Project or Program collect, maintain, use, or disseminate information? Please check all that apply.	☐ This project does not collect, maintain, use, or disseminate any personally identifiable information ☐ Members of the public ☑ OPM employees ☐ Contractors working on behalf of OPM ☑ Employees of other federal agencies

3. Please identify all information that is collected, generated, or retained (such as names, addresses, emails, etc.) *for each category of individual or population*.

☑ Name	☐ Driver's License/State ID Number
☐ Date of Birth	☐ Social Media Handle/ID
☐ Place of Birth	☐ Biometric Identifiers
☐ Age	☐ Retirement
☐ Citizenship	☐ CSA/ CSF Number
☑ SSN	☐ Unique Entity Identifier
☐ Home Address	☐ Nationality
☐ Alias	☐ Sexual Orientation
☐ Nicknames	☐ Race
☐ Personal Email Address	☐ Ethnicity
☐ Personal Cell Number	☐ Mother's Maiden Name
☐ Resume or Curriculum	☐ Protected Health Information
☐ Business Financial Information	☑ Other. Please list: Grade, Series Work Location, Work Email Address, Organization, Work Phone Number, Position Title And Supervisory Status
☐ Tax Identification Number	
☐ Passport Number	
☐ Bank Account	
☐ Credit Card	
☐ Other Financial Account Number	

3(a) Does this Project, Program, or System collect, maintain, use, or disseminate Social Security numbers (SSN) or other types of stand-alone sensitive information?	○ No. ◉ Yes.
3(b) Please provide the specific legal basis for collecting the SSN:	Pursuant to 5 U.S.C. § 1103(c), OPM must design a set of systems, including
3(c) If the SSN is needed to carry out the functions and/or fulfill requirements of the Project, System, or Program, please explain why it is necessary and how it will be used.	
Social security numbers (SSN) are collected from the agency upon initial user account creation and/or load. An agency admin does have the ability to manually enter the user's SSN within USAP. The SSNs are unique and never displayed within the system unmasked. The SSN is required by OPM's eOPF system when transmitting the employee's performance evaluation from USAP to eOPF.	
3(d) If the Project, Program, or System requires the use of SSN, what actions are being taken to abide by Public Law No. 115-59, "Social Security Number Fraud Prevention Act of 2017," 42 U.S.C. § 405, which requires the use of privacy-enhancing SSN alternatives when there are technological, legal, or regulatory limitations to eliminating the SSN? Note: even if you are properly authorized to collect SSNs, you are required to use an alternate unique identifier. If there are technological, legal, or regulatory limitations to eliminating the SSN, privacy-enhancing alternatives should be taken, such as masking, truncating, or encrypting the SSN, or blocking the display of SSNs in hard copy or digital formats.	
Currently the SSNs are unique and never displayed within the system unmasked.	

4. How does the Project, Program, or System retrieve information?	☑ By a unique identifier. Please list all unique identifiers used: f yes, please list all personal identifiers used: The system uses the full name and the social security number as the primary identifier. ☐ By a non-unique identifier or other means. Please describe:
5. What is the records retention schedule(s) for the information collected for each category type (include the records schedule number)? If no schedule has been approved, please provide proposed schedule, or plans to determine it. Note: If no records schedule is in place or are unsure of the applicable records schedule, please reach out to the OPM Records Officer.	The performance records contained in USAP are covered by the OPM/GOVT-2 Employee Performance File SORN.
5(a) How does the Project, Program, or System ensure that records are disposed of or deleted in accordance with the retention schedule (e.g., technical/automatic purge, manual audit)?	USA Performance has worked with eOPF and USA Staffing to now include a retention flag in the system. The retention flag keys off the performance appraisal rating period and electronically disposes of
6. Does this Project, Program, or System connect, receive, or share PII with any other Office, projects, programs, or systems?	○ No. ◉ Yes. If yes, please list: For participating agencies, USAP transmits the SSN as part of the employee's performance evaluation transfer to OPM's eOPF.
7. Does this Project, Program, or System connect, receive, or share PII with any external (non-OPM) government or non-government partners or systems?	○ No. ◉ Yes. If yes, please list: Council of the Inspectors General on Integrity and Efficiency (CIGIE) ,Court Services and Offender Supervision Agency (CSOSA),Defense Nuclear Facilities Safety Board (DNFSB) Executive Office of the President, Office of Management and Budget (OMB), Executive Office of the President, Office of National Drug Control Policy (ONDCP), Executive Office of the President, Office of Science and Technology (OSTP), Executive Office of the President, US Trade Representative (USTR)

8. Is this sharing pursuant to new or existing information sharing agreement (MOU, MOA, etc.)? If applicable, please provide agreement as an attachment.	Existing Please describe applicable information sharing governance in place: EHRIDW – MOU (Enterprise Human Resources Integrations Data Warehouse) eOPF – MOU (Electronic Official Personnel Folder) DHS, Office of the Chief Human Capital Officer (OCHCO), Human Capital Business Solutions (HCBS) Enterprise Information Environment (EIE). HHS Enterprise Human Capital Management (EHCM) -MOU United States Secret Service (USSS) Application Provisioning System (APS) – MOU National Science Foundation (NFS) NSF Network General Support System (GSS) – MOU U.S. Environmental Protection Agency (EPA) Office of Administration Services Information System (OASIS) - MOU
9. Does the Project, Program, or System have a mechanism to track external disclosures of an individual's PII?	○ No. What steps will be taken to develop and maintain the accounting: ● Yes. In what format is the accounting maintained: The USAP web application documents an accounting of PII disclosures within the system's audit logs. The recorded information is sufficient to establish what events occurred, the sources of the events, and the outcomes. Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system where the event occurred; (iii) type of event; (iv) subject identity; and (v) the outcome (success or failure) of the event.
10. Does this Project, Program, or System use or collect data involving or from any of the following technologies:	☐ Social Media ☐ Advanced analytics ☐ Live PII data for testing ☑ No
11. Does the planned effort include any interaction or intervention with human subjects via pilot studies, exercises, focus groups, surveys, equipment or technology, observation of public behavior, review of data sets, etc. for research purposes?	● No. ○ Yes.
12. Does the Project, Program, or System provide role-based or additional privacy training for personnel who have access, in addition to annual privacy training required of all OPM personnel?	● No. ○ Yes. If yes, please list: All OPM employees receive annual Security and Privacy Awareness Training which covers of handling PII-related information. There are no specific role-based training currently required to use the system.

13. Is there a FIPS 199 determination?	◯ No. ◉ Yes. Please indicate the determinations for each of the following: **Confidentiality:** ◯ Low ◉ Moderate ◯ High ◯ Undefined **Integrity:** ◯ Low ◉ Moderate ◯ High ◯ Undefined **Availability:** ◯ Low ◉ Moderate ◯ High ◯ Undefined

Completed by the OPM Chief Privacy Officer or Designee

Privacy Office Reviewer:	Tommy Hudson
Date Review Completed:	03/22/2024
PTA Expiration Date:	03/21/2025

Designation

Privacy Sensitive System:	◉ Yes ◯ No
Category of System:	Choose an item If "other" is selected, please describe:
Privacy compliance and assurance (PCA):	
☐ Privacy compliance documentation in progress ☐ PTA sufficient at this time ☐ PIA required ☐ SORN required	☐ Privacy Act Statement Required ☐ PRA clearance required ☐ Records Schedule Required ☐ New information sharing arrangement required

PIA:	System covered by existing PIA USA Performance (USAP) May 13, 2020 - current PIA under review by Privacy Office. Expected completion date no later than end of third quarter FY 24
SORN:	System covered by existing SORN OPM/GOVT-2 Employee Performance File System Records

Privacy Office Comments:

Please describe rationale for privacy compliance determination above, and any further action(s) that must be taken by Office.

USAP collects, uses, disseminates, and maintains the personally identifiable and performance evaluation information about employees to include full name, social security number and other personally identifying information. The Privacy Impact Assessment was last reviewed and approved in May 2020,. The updated PIA is currently under review by the Privacy Office. Information content of the PIA has not changed therefore OPM GOVT-2 SORN still provides adequate coverage for the system of record.

Privacy Controls

Privacy controls are the administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling of PII. The privacy control families can be implemented at the organization, office, program, or information system level, under the leadership of the Senior Agency Official for Privacy (SAOP) or Chief Privacy Officer (CPO) and in coordination with the Chief Information Security Officer (CISO), Chief Information Officer (CIO), program officials, and legal counsel. NIST SP800-53 Rev.5 provides a summary of the privacy controls. Indicate, in the context of this PTA, whether the control is met (Y), not met (N), or Not Applicable (N/A).

Control Number	Privacy Controls (NIST SP800-53 Rev.5)	Control Status
PT	Authority and Purpose	Yes
PT-2	Authority to Process Personally Identifiable Information	Yes
PT-3	Personally Identifiable Information Processing	Yes
PM-3	Information Security and Privacy Resources	Yes
PM-18	Privacy Program Plan	Yes
PM-19	Privacy Program Leadership Role	Yes
TR-3	Dissemination of Privacy Program Information	Yes
RA-3	Risk Assessment	Yes
RA-8	Privacy Impact Assessment	Yes
SA-1	Policies and Procedures	Yes
SA-4	Acquisition Process	Yes
SA-9	External System Services	Yes
CA-2	Control Assessments	Yes
AT-1	Policies and Procedures	Yes
AT-2	Literacy Training and Awareness	Yes
AT-3	Role-based Training	Yes

Control Number	Privacy Controls (NIST SP800-53 Rev.5)	Control Status
AT-3(5)	Role-based Training / Processing Personally Identifiable Information	Yes
PL-4	Rules of Behavior	Yes
PM-27	Privacy Reporting	Yes
AR-7	Privacy-Enhanced System Design and Development	Yes
PM-20	Dissemination of Privacy Program Information	Yes
PM-21	Accounting of Disclosures	Yes
PM-22	Personally Identifiable Information Quality Management	Yes
PM-24	Data Integrity Board	Yes
SI-1	Policies and Procedures	Yes
SA-8(33)	Security and Privacy Engineering Principles / Minimization	Yes
SI-12(1)	Information Management and Retention / Limit PII Elements	Yes
MP-6	Media Sanitization	Yes
SI-12	Information Management and Retention	Yes
SI-12(3)	Information Management and Retention / Information Disposal	Yes
SI-12(2)	Information Management and Retention / Minimize PII in Testing, Training and Research	Yes
PT-4	Consent	Yes
AC-1	Policies and Procedures	Yes
AC-3(14)	Access Enforcement / Individual Access	Yes
SI-18	Personally Identifiable Information Quality Operations	Yes

Control Number	Privacy Controls (NIST SP800-53 Rev.5)	Control Status
SI-18(4)	Personally Identifiable Information Quality Operations / Individual Requests	Yes
SI-18(5)	Personally Identifiable Information Quality Operations / Notice of Correction or Deletion	Yes
PM-25	Minimization of PII used in Testing, Training, and Research	Yes
PM-26	Complaint Management	Yes
PM-5(1)	System Inventory / Inventory of Personally Identifiable Information	Yes
IR-8	Incident Response Plan	Yes
IR-8(1)	Incident Response Plan / Breaches	Yes
PT-5	Privacy Notice	Yes
PT-5(1)	Privacy Notice / Just-In-Time Notice	Yes
PT-5(2)	Privacy Notice / Privacy Act Statements	Yes
PT-6	System of Records Notice	Yes
AC-21	Information Sharing	Yes
AU-2	Event Logging	Yes