Privacy Impact Assessment (PIA): OS - OS ISM - QTR2 - 2025 - OS2838545

Created Date: 6/4/2025 1:08 PM Last Updated: 6/24/2025 2:35 PM

Copy PIA (Privacy Impact Assessment)

Do you want to copy this PIA ?

Please select the user, who would be submitting the copied PIA.

Instructions

Review the following steps to complete this questionnaire:

1) Answer questions. Select the appropriate answer to each question. Question specific help text may be available via the icon. If your answer dictates an explanation, a required text box will become available for you to add further information.

2) Add Comments. You may add question specific comments or attach supporting evidence for your answers by clicking on the icon next to each question. Once you have saved the comment, the icon will change to the icon to show that a comment has been added.

3) Change the Status. You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.

4) Save/Exit the Questionnaire. You may use any of the four buttons at the top and bottom of the screen to save or exit the questionnaire. The button allows you to complete the questionnaire. The button allows you to save your work and close the questionnaire. The button allows you to save your work and remain in the questionnaire. The button closes the questionnaire without saving your work.

Acronyms
ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

General Information

PIA Name:	OS - OS ISM - QTR2 - 2025 - OS2838545	**PIA ID:**	3267961
Name of Component:	OS - OS - OS - Interactive Service Management	**Name of ATO Boundary:**	Interactive Service Management
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	26
Submission Status:	Submitted	**Submit Date:**	6/3/2025
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	OS
Security Categorization:		**OpDiv PIA ID:**	OS2838545
Legacy PIA ID:		**Make PIA available to Public?:**	No

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
2:	Is this a FISMA-Reportable system?	Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
4:	ATO Date or Planned ATO Date.	12/8/2023
5:	Is the system or electronic information collection, agency or contractor operated?	Agency

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	New Interagency Uses
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	OS ISM (ServiceNow) is about to integrate the Nuvolo Plugin which is s an Integrated Workplace Management calendar into the the system, by creating a public calendar report in OS ISM that displays the schedule for the day. These public reports can be accessed via URL, allowing them to be displayed on a kiosk screen . To enable this functionality, the following underlying data from the relevant tables and fields would need to be made accessible through the URL. Details of meeting reservations made, with location code, subject of the meeting, time, assigned space, Operating Division (OpDiv), Staff Division (StaffDiv) seat status, ,etc.
PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Agency

PTA - 4:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions.	The purpose of Office of the Secretary Interactive Service Management (OS ISM) is to advertise and automate the services that organizations within HHS provide to others. Primarily, the system is meant to advertise and automate the Information Technology (IT) services provided by Office of the Chief Information Officer (OCIO), but the system is flexible enough to support management of non-IT services such as Office of Human Resources (OHR) Policy Groups, Change Management Processes, Business Offices, Portfolio Management Offices, Help Desk and Human Resources. As of October 2021, the Safe Workplace module has been added to the OS ISM platform to track the reporting of federal employee vaccine status per the President's executive order. Federal employees will login into OS ISM via AMS to report their vaccine status. Supervisors will have the ability to review the status reported along with an attachment of the employee's vaccine record. The OASH organization added a database connection to store their Commission Corp data for employee processing.
PTA - 5:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored.	The OS ISM system will create tickets recording incidents reported by the users of the services offered by the Office of the Chief Information Officer (OCIO and incidents reported by HR specialists regarding HR processes and employee activities. These tickets will contain the requestor name, Phone number, location and description of issue. The aforementioned information is not shared outside the normal workflow and the information will remain in the system until the issue is resolved. Also, user information will be imported from AMS, OHR's Enterprise Human Capital Management (EHCM) system (which have their own Privacy Impact Assessment(PIA)s) and the OCIO-Operations' Active Directories to provide single sign on services and billing code information to bill OCIO Operations customers for products or services purchased. OS ISM will also store asset and configuration information pertaining to systems as long as the systems are connected via EANow and each OCIO-Operations customer purchased assets. Also, the OASH Commissioned Corps HR and Payroll data which includes PII and Protected Health Information (PHI) and the Federal Employee vaccination records. These interfaces except the Federal Employees vaccination Records are documented with Memorandum of Understanding (MOU)s for each interconnection into OS ISM. The data for the VAX system is populated by the employee, and eventually contractors working with the department. Employees are uploading the picture of their vaccination record, which will be stored in a secured CMDB. The data coming from AMS, OHR and OCIO-Operations includes: Employee name, Office telephone number, Work Street Address and Building name Supervisor Information (name,

		email, phone number, mailing address), employee home address, and telephone number, Social Security Number (SSN), Employee Identification (ID), and birth date and employee work status. Billing code Assets assigned System information including the internet Protocol (IP) Addresses Device identifier: depending on the customer receiving ISM services, this could refer to the asset tag number which is affixed to a laptop or printer. This can also refer to the media access control (MAC) address, a unique identifier assigned to an HHS network device. HHS user credentials will be pushed into OS ISM via AMS Single Sign On. AMS is the system of record for user login credentials via their identity and authentication management program The system will also through the Nuvolo Plugin calendar create a public calendar report in OS ISM that displays a table with non-PII details of meeting reservations made, with location code, time, assigned space, Operating Division (OpDiv), Staff Division (StaffDiv) seat status, These public reports can be accessed via URL, allowing them to be displayed on a kiosk screen on the ISM system
PTA - 5A:	Are user credentials used to access the system?	Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system. The system providing credentials is
PTA - 5B:	Please identify the type of user credentials used to access the system.	
PTA - 6:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual.	OS ISM is a configuration of ServiceNow that implements the specific service request fulfillment processes, incident handling procedures, project and portfolio processes defined by OCIO, the HR Service delivery processes defined by the OHR group, the Nuvolo Move Management application for OASH to manage the movement of their officers and employees, the Audit management application for Assistant Secretary for Legislation (ASL) to manage the Government Accountability Office (GAO) audit program, and the Safe Workplace module to track and monitor vaccine status of the federal workforce. ServiceNow is the product name of many modules purchased from the vendor. The finished configured platform is named OS ISM. HHS does not use product names for its systems. The system also implements interfaces to other service management systems to provide a seamless experience for the organizations OCIO supports. Credentials to support authentication of system administrators are not stored in OS ISM. However, all ServiceNow administrators must be registered with ServiceNow to initiate any operations and maintenance activities managed by the ServiceNow vendor. Otherwise, OS ISM depends on the Access Management System (AMS) as the primary mechanism for authenticating users. AMS stores all user credentials. The OS ISM system will create tickets recording incidents reported by the users of the system and a

		service catalog of products and services offered by OCIO and non-OCIO organizations. User credential information will be imported from AMS for single sign-on services and Active Directories information from ODCIO for billing code information to bill customers for products or services purchased. OS ISM will also store asset and configuration information pertaining to systems and each ODCIO customer purchased assets. These interfaces are documented with a MOU with each AMS, ODCIO, Business Intelligence Information System (BIIS) and OASH. The data coming from AMS, ODCIO, BIIS, and OASH includes: OHR PII data comes from BIIS Cloud for the use of processing employee HR transactions and on-boarding. Other data includes Employee name Office telephone number Work Street Address and Building name Supervisor Information (name, email, phone number, mailing address) Billing code Assets assigned System information including IP Addresses Device identifier: depending on the customer receiving ISM services, this could refer to the asset tag number which is affixed to a laptop or printer. This can also refer to the media access control (MAC) address, a unique identifier assigned to an HHS network device. HHS user credentials will be pushed into OS ISM via AMS Single Sign On. AMS is the system of record for user login credentials via their identity and authentication management program. The system also, maintains records of room reservation with location code, time , title, StaffDiv/OpDiv specified, through its Nuvolo application.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	Yes
PTA - 8:	Does the system include a website or online application?	No
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	
PTA - 9:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	
PTA - 10:	Does the website have a posted privacy notice?	
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	
PTA - 12:	Does the website use web measurement and customization technology?	
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	
PTA - 13A:	Does the website collect PII from children under the age thirteen?	

PTA - 13B:	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?	
PTA - 14:	Does the system have a mobile application?	Yes
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	Third-party
PTA - 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	The mobile application is for Deskside Agents and Asset Managers to be able to view and work Service Requests without having to return constantly to their desk to use the Desktop interface ServiceNow provides through browsers. The Mobile application additionally provides a scanner functionality that works with the barcodes Asset Management uses on HHS property so that they can more easily track and maintain inventory. There is also the Nuvolo mobile application, which is used to streamline room reservation management by allowing users to book spaces via their mobile devices and to provide real-time visibility of conference room schedules through in-room kiosks module. All current reservation users in the OS ISM (ServiceNow) system can download and access Nuvolo mobile application.
PTA - 16:	Does the mobile application/ have a privacy notice?	Yes
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	No
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
PTA - 18:	Does the mobile application use measurement and customization technology?	No
PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	No
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	
PTA - 19B:	Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	Yes
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Social Security Number Name Email Address Phone numbers Medical records (PHI) Date of Birth Mailing Address Medical Records Number Devices Identifiers Employment Status Other - Free text Field - Office Address; Employee ID; IP Address; Immunization Records; Vaccination Record Card; Medical and Religious Exceptions. Location code, assigned space, Operating Division (O
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	Above 2000

PIA - 4:	For what primary purpose is the PII used?	The Personal Identifiable Information (PII) is used in authentication management of user login to the Office of the Secretary Interactive Service Management (OS ISM). And the PII data also assists the Office of the Deputy Chief Information Officer-Operations (ODCIO-Ops) in recognizing its customers, how to bill its customers, where to find customers within HHS, identify equipment assigned to customers and its condition and how DCIO-OPs operates as a supplier of services and products. Also, PII is used by Office of Human Resources (OHR) through modules named HR Exchange, HireNow, DetailNow, and PerformanceNow to assist the organization in supporting the employees and managers of the Department of Health and Human Resources (HHS) in their human resource activities. Some of the services provided include: new hire, a consolidated help desk, on-boarding new employees, allowing current employees access to their HHS employee records, and to allow employees the flexibility to make changes to their personal records. Vaccination data is shared with HHS supervisors to validate employee vaccine status. Vaccination statuses are also reported to the Office of Management and Budget (OMB). Images of the vaccination records are used to track whether employees have been fully or partially vaccinated per the Presidents executive order to control the spread of COVID-19. Office of the Assistant Secretary for Health(OASH) PII data is used by OASH to support the officers and employees HR, payroll, and facility/office space needs. The system will also through the Nuvolo Plugin calendar create a public calendar report in OS ISM that displays a table with non-PII details of meeting reservations made. These public reports can be accessed via URL, allowing them to be displayed on a kiosk screen on the ISM system.

PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	OS ISM can also create reports surrounding hardware and software performance metrics within the application. OCIO management can also generate reports reflecting current performance statistics and trends. As part of the change management process, testing is performed in-house and on a limited basis with no PII data initially except at the last stage of testing to ensure the exact required data is pulled by the connecting system and are immediately deleted after testing. Such data are fully encrypted during testing and access is limited to the OHR ServiceNow Manager. So technically, there is no real secondary use of the PII except as a managerial tool to display information in a user friendly format. Office of the Chief Information Officer (OCIO) /Office of the Chief Product Officer (OCPO) has a reporting branch that is established to design reports at customers' request
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	The Social Security Number (SSN) and Commission Corp Serial Numbers are used by the OHR and OASH respectively in supporting the employees and managers of the Department of Health and Human Resources (HHS) in their human resource activities such as, a consolidated help desk, on-boarding new employees, allowing current employees access to their HHS employee records.
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	This information is provided pursuant to 5 United States Code (U.S.C.) 552a (Privacy Act of 1974) for individuals supplying information for inclusion in a system of records. Executive Order (E.O.) 9397 and 31 U.S.C. 7701(c) (2) authorize the collection of the SSN. The former is the Executive Order noting that the SSN is to be used for various official government purposes, including as the Taxpayer Identification Number (TIN), and the latter states "The head of each Federal agency shall require each person doing business with that agency to furnish to that agency such person’s taxpayer identifying number."
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	The implementation of this system, including activities such as the collection of PII necessary for operating it, are authorized by 5 U.S.C. 301. 42 U.S.C § 3502 creates the Office of the Assistant Secretary for Administration (ASA) at HHS, and among the duties delegated to the ASA are oversight of these services, which are necessary to developing and maintaining a workforce. 31 U.S.C. 66a; 5 U.S.C. 5501 et seq., 5525 et seq., 5701 et seq., and 6301 et seq.; Executive Order 9397; Pub. L. 100–202, Pub. L. 100–440, and Pub. L. 101–509
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	Name, Social Security Number (SSN), Employee ID, OASH Serial Number, Vaccination Records, HHSID

PIA - 8B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	OPM/GOVT-1 General Personnel Records, December 11, 2012, 77 FR 79694; modified November 30, 2015, 80 FR 74815 09-40-0001 Public Health Service (PHS) Commissioned Corps General Personnel Records, 63 FR 68596 - PDF (12/11/98), 83 FR 6591 (2/14/18) 09-90-1901 HHS Correspondence, Customer Service, and Contact List Records, 84 FR 28823 (6/20/19) 09-90-0777 Facility and Resource Access Control Records, 75 FR 47812 (8/9/10), 83 FR 6591 (2/14/18) OPM/GOVT-10, Employee Medical File System of Records: 75 Fed. Reg. 35099 (June 21, 2010) amended 80 Fed. Reg. 74815 (Nov. 30, 2015).
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Email Other Government Sources Within the OPDIV Other HHS OPDIV
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 10A:	Provide the information collection approval number.	
PIA - 10B:	Identify the OMB information collection approval number expiration date.	
PIA - 10C:	Explain why an OMB information collection approval number is not required.	There is no applicable Office of Management and Budget (OMB) information collection approval number for this item. The Paperwork Reduction Act (PRA) only requires OMB number for a system that generates or collects information from the public, whereas, the system only stores Federal employees PII.
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	Yes
PIA - 11A:	Identify with whom the PII is shared or disclosed.	Other Federal Agency/Agencies Private Sector Within HHS

PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	PII is shared by the Office of Human Resources (OHR) to assist employees and managers of the Department of Health and Human (HHS) in their human resource activities. The same explanation applies to the OASH organization who are assisting their officers and commanders working within the Department. Vaccination data is shared with HHS supervisors to validate employee vaccine status. Vaccination statuses are also reported to the OMB. PII is shared with Premier Logitech, a non-governmental, private company for the purpose of order fulfillment and shipping or inventory control.

PIA - 11C:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	There are Interconnection Security Agreement (ISA)s with the: US Office of Personnel Management (OPM); The Defense Finance Accounting Services (DFAS)-Remedy system; Premier Logitech-Mantis Warehouse Management System (WMS); Administration of Children and Families (ACF)-Upstream; and Memorandum of Understanding(MOU)s with the: OHR for the Enterprise Human Capital Management (EHCM); Business Intelligence Information System (BIIS); PSC Locator (Background Investigation Tracking System (BITS) Module; AMS for the AMS Federated single sign-on and the Smart Card Management System (SCMS) systems; and OASH for the OASHNow system, for all these interconnections in addition to filing out a user request form. Each ISA and MOU contain statements that limit sharing and disclosure of information other than as permitted or required by the Agreement or as required by law. Each party to the agreement accept to report to the other party any use or disclosure of the information not provided for by the ISA/MOU of which it becomes aware. Both parties agree to maintain the level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of the information contained in the systems. In the case of the Vax System, there are no requirements for a signed agreements on information sharing with the OMB. Vaccination statuses are reported to the OMB based on a presidential executive order

PIA - 11D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	We have ISAs and MOUs for these interconnections in addition to filing out a user request form. In the user request form, the requestor is required to provide the name and address of recipient, Also the date, nature and purpose for which the requested information will be used. And, only a licensed OHR supervisor can access the data with an individual account. The Federal employee vaccine and reasonable accommodation statuses are tracked through the Safe Workplace module on the OS ISM platform. Federal employees will login into OS ISM via AMS to report their vaccine status. Supervisors will have the ability to review the status reported along with an attachment of the employee's vaccine record. The reports are sent to the OMB per the President's executive order
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 12A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	

PIA - 13:	Describe the method for notifying individuals that their information will be collected and how they can opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.	OS ISM does not collect personal information directly from users, except the new Vaccination Tracking (VAX) system Data collection is performed by the Identity and Access Management(IAM) system, ODCIO-Ops, OHR. and OASH. The VAX system data is entered by the employee by uploading their vaccine record per OCIO Leadership in reference to the President's Executive order. The first two organizations push the information into OS ISM for Single Sign On functionality and to support ODCIO-Ops business process. And OHR uses the functionality of the system to store personal information about individuals. For the VAX System: On September 9, 2021, President Biden issued Executive Order: Requiring Coronavirus Disease 2019 Vaccination for Federal Employees, which requires Federal employees to be fully vaccinated against COVID-19, by November 22, 2021, except in limited circumstances where an employee is legally entitled to an accommodation. 'The purpose of this Presidential mandate is simple - to protect your health and safety and that of your colleagues, and members of the public with whom you may interact' PII data is collected from IAM, ODCIO -Ops and OHR for Single Sign On functionality, ODCIO's Lightweight Directory Access Protocol(LDAP) to support their business process, and OHR's Human Resource functions respectively. To opt-out, individuals and OS ISM will need to follow the processes established by IAM and ODCIO,OHR, and OASH to exclude these personal information. Vaccine data is required by a Presidential executive order . To opt-out, an employee must be granted one of the limited legal exceptions, i.e., an accommodation for a medical reason or sincerely held religious belief, practice, or observance. Such employee has to work with the Reasonable Accommodation organization within the department.
PIA - 14:	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.	PII data is not collected by OS ISM, but through interfaces with IAM, ODCIO, OHR. and OASH OS ISM will channel notifications and the collection of consents through IAM, ODCIO, OHR, or OASH. For the VAX system, the ASA has been sending notifications across the department concerning the VAX system and its use of vaccine records. Employees are asked to email the VAX Question email box with concerns

PIA - 15:	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.	OS ISM has interfaces established with IAM, ODCIO, OHR , and OASH for the organizations to push data into the OS ISM system. To resolve issues of concerns, OS ISM will contact IAM, ODCIO, OHR. or OASH and follow their processes to have any concerns addressed. For the VAX system employees are to send an email to the HHS Vax Question email box or open ticket with OCIO to be delivered to the appropriate security team Also, all HHS employees are required annually to take Security Awareness Courses such as the Cybersecurity Awareness Training, and Records Management Training on how to appropriately address privacy concerns
PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not.	OS ISM will rely on the periodic reviews established by the owners of the PII data, IAM, ODCIO, OHR, and OASH via the MOUs established with the organizations, OS ISM will ensure the security controls needed to protect privacy will be equal to that of IAM, ODCIO, OHR, and OASH.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Contractors Others
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes

PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Users: Fulfillers (license holders) or ODCIO Service Desk Agents who will initiate tickets in incident management or for a request for service on behalf of the end user or process the request per the assigned workflow. And for OHR Users: managers in their Human resources functions and for employees to have access to their personal records with flexibility to make changes where permitted. VAX users: (Purchased Safe Work Place (SWP) User Licenses) federal employees to share their vaccine record as evidence of vaccination or to request reasonable accommodation Administrators : To maintain the interfaces that push the PII data into the system. Change passwords or modify fulfiller accounts. Others (Data Integrators): No customization during these phases of implementation. If any, it is required to bring in the IAM, ODCIO, OHR or OASH interfaces. OS Supervisors: Supervisors of the department to validate employee vaccine status for the department to report to the OMB . Contractors Direct contractors will support the ODCIO Service Desk
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	OS ISM is a role-based system with predefined workflows. Each fulfiller is assigned to a group. The group identifies the activities and data the fulfiller is allowed access to do the assigned task. The groups are defined by the client, like ODCIO, and the process they have in place to control least privilege. Access control lists (ACL) are used to control access within the applications. The information submitted for vaccination will be treated as confidential information and will only be shared with those who have a need to know such as, individuals ensuring compliance with the Executive Order, supervisors, and human resources personnel, as appropriate
PIA - 20:	Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.	OS ISM is a role-based system with predefined work-flows. Each fulfiller is assigned to a group. The group identifies the activities and data the fulfiller is allowed access to do the assigned task. The groups are defined by the client, like ODCIO, and the process they have in place to control least privilege. Access control lists (ACL) are used to control access within the applications

PIA - 21:	Identify the general security and privacy awareness training provided to system users (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.	OS ISM will follow and participate in the Departments IT Security Awareness and Privacy Awareness programs. Along with the Cyber-security Awareness program based on their role in the organization they support. Training is provided via a Train the Trainer type approach. As new fulfillers come on-board, training will occur at the customer level based on the role they are assigned
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Training is also provided by ServiceNow in the applications purchased. Some OCIO personnel are given system administration training as a first step in understanding ServiceNow. Direct contractors who are to use the tool must already have ServiceNow training and pass the security requirements of HHS.
PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	OS ISM will inherit the processes and guidelines established by IAM, ODCIO, OHR, and OASH regarding retention and destruction of PII. OS ISM receives updates from IAM, ODCIO, OHR, and OASH on a daily schedule as IAM, ODCIO,OHR and OASH will remove account information. We are working with the Records Management Office to determine if a new Records Retention Schedule is required or if General Records Schedule (GRS) 2.7 or another existing schedule fits. We will maintain records indefinitely until the appropriate schedule has been determined. For the Vaccination records, GRS 2.7, item 063 Vaccination attestations and proof of vaccination records (Pending Approval) will be the records retention schedule for the program records in the system.
PIA - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	OS Interactive Systems Management (ISM) uses secured connections to safeguard sensitive data per HHS security guidelines. Administrative - There are established Memorandum of understanding(MOU)s and Interconnection Security Agreement(ISA)s for every system that interconnects with OS ISM. And every user with administrative role must have a fulfiller license. Technical - PII data at rest or in-transit are encrypted. All communications between ServiceNow in the cloud and the HHS use secured connections. Also, Role Based Access control model is in use to limit user access to sensitive data. And ,all users are logically identified and authenticated before they are granted access. Physical - Data warehouses housing OS ISM servers and workstations are environmentally protected and are strictly restricted to validated employees only.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	6/3/2025
Privacy Analyst Comments:	Vanessa, This PIA is ready for your review. All necessary questions have been answered. Thank you, Jon	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:		**SOP Review Date:**	6/4/2025
		SOP Days Open:	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	6/12/2025
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 6/12/2025 This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	8

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	6/24/2025
		SAOP Days Open:	12

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	Data Feed Service, piafrmos_Release	6/3/2025	In the free text field, please also include the following information related to the new plugin: "Location code, assigned space, Operating Division (OpDiv), Staff Division (StaffDiv)"	
PIA - 4	Data Feed Service, piafrmos_Release	6/3/2025	Please also append to the end of the current response, this paragraph related to the new plugin: "The system will also through the Nuvolo Plugin calendar create a public calendar report in OS ISM that displays a table with non-PII details of meeting reservations made. These public reports can be accessed via URL, allowing them to be displayed on a kiosk screen on the ISM system."	

Admin Section

Is OpDiv Privacy Analyst Approved ?:	1	**Is OpDiv Privacy Analyst Return ? :**	0
		Is SOP Return ?:	0
Is Agency Privacy Analyst Approve ?:	1	**Is Agency Privacy Analyst Return ?:**	0
Is SAOP Approved?:	1	**Is SAOP Return ?:**	0
Total Approved:	4	**Total Return:**	0
Total Approval Required:	4		

Miscellaneous Fields

Last Updated:	6/24/2025 2:35 PM	**History Log:**	View History Log