Privacy Impact Assessment (PIA): OS - CCP-C - QTR1 - 2025 - OS2313576

Created Date: 2/20/2025 4:02 PM Last Updated: 3/11/2025 9:29 AM

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 - CCP-C - QTR1 - 2025 - OS2313576	**PIA ID:**	2791482
Name of Component:	OS - OS - Commissioned Corps Payroll - Cloud	**Name of ATO Boundary:**	Commissioned Corps Payroll - Cloud
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	48
Submission Status:	Submitted	**Submit Date:**	2/27/2025
Next Assessment Date:	N/A	**Expiration Date:**	3/10/2028
Office:		**OPDIV:**	OS
Security Categorization:	Moderate	**OpDiv PIA ID:**	OS2313576
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.	
5:	Is the system or electronic information collection, agency or contractor operated?	Contractor

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	N/A
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 Commissioned Corps Payroll Cloud (CCPC) is a secure, web-based system, available only to the Human Resource and Payroll Technicians at the Commissioned Corp (CC) Headquarters (HQ), providing payroll and personnel services for more than 6,500 Commissioned Corps Active Duty Officers. CCP-C provides an integrated solution for the Commissioned Corps personnel and payroll requirements: the collection of Active-Duty Officer's (ADO) educational qualification, license information, duty station location, agency and position identification, dependent details, state tax and federal tax details, determination of pay categories, gross to net calculations, and interface with all the various internal and external systems required to ensure the accurate disbursement of funds. The CCP-C system has payroll data for all ADOs that are generated based on the data contained in the system, including personally identifiable information (PII). The initial records source is the application form (Public Health Service (PHS)-50) completed by the applicant when applying to the Commission Corp. The CCP-C system calculates the Commissioned Corps Payroll on a monthly basis. Those calculations are used for post-payroll processing. Payroll files are moved to the Commissioned Officer Personnel System (Oracle) 10G Data Base (COPS10GDB) system (a separate HHS system with its own privacy impact assessment (PIA)) for final payroll processing. (note: It is now Oracle 11G version of the database) The COPS10GDB system then receives files from CCP-C and transmits the files to both the Treasury for Electronic Funds Transfer (EFT) payments, and to the Thrift Savings Plan (TSP).
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.	CCP-C will collect, maintain, store, and/or share the following information: 1) Health and Human Services (HHS) staff who are Human Resource (HR) Specialists and Payroll Technicians, direct contractors, and contractors have minimal PII stored on the system (Social Security Numbers (SSNs), emails, phone numbers, and names). The names, email addresses and passwords are used as login credentials to access the system. 2) The CCP-C system provides payroll and personnel services for more than 6,500 Commissioned Corps ADOs, and the process involves the collection of source documents, determination of pay categories, gross to net calculations, and interfacing with other HHS systems required to ensure the accurate disbursement of funds. Information collected for this group includes names, addresses (email and mailing), SSN, personnel orders, phone numbers, military service dates, education records, dates of birth, employment status, marital status, and financial information (paycheck amounts). These data elements form the data attributes of the ADO, either to uniquely identify the officer, or to determine the payroll benefits (example: Basic Allowance for Housing amount is based on the officer's residence address). The SERNO (unique serial number), SSN, date of birth, gender, determine a unique record. The category, grade,

		license, education, and position details, determine the bonus/special pay the officer is entitled to, and the base salary for that grade and position. The service dates, education, and category determine the retirement eligibility. The personnel orders represent the nature of HR actions that took place and determine the Operating Division (OPDIV) that is paying for the officer. The CCP-C system has payroll data for all ADOs that are generated based on the data contained in the system, including personally identifiable information (PII). The records source is the application form (Public Health Service (PHS)-50) completed by the applicant when applying to the Commission Corp. The CCP-C system shares the Personnel and Payroll data with COPS10GDB. Information shared includes names, addresses (email and mailing), SSNs, personnel orders, phone numbers, military service dates, education records, dates of birth, employment status, marital status, and financial information (paycheck amounts) for Commissioned Corps Officers, including SERNOs, category, grades, licenses, and position details. COPS10GDB receives the payroll details, and also transmits them to Treasury, Social Security Administration, Accounting for Pay System, and TSP. New account creation is a function the Contractor is responsible for. The Data Systems Integration (DSI) will securely email the account forms to the Contractor who will create the accounts and securely email back the credentials to DSI. DSI will then contact the technician and provide the new credentials. All information is stored in the system foe indefinite period of time and is not deleted from database. All information/data is safeguarded.
PTA - 5A:	Are user credentials used to access the system?	Yes
PTA - 5B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card Non-HHS User Credentials Username Password

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.	CCP-C is a web-based system that provides payroll and personnel services for the 6,500+ Commissioned Corps Active-Duty Officer population. Information collected includes names, addresses, SSNs, license details, addresses, phone numbers, military service dates, marital status, education details, military status, dates of birth, license details, and financial information (paycheck amounts) for Commissioned Corps Officers. The data along with the personnel orders and pay information generated in the system is maintained and shared with COPS10GDB. COPS10GDB shares this information with The Treasury, TSP, Social Security Administration, HHS General Ledgers (via Accounting For Pay System (AFPS), and Defense Manpower Data Center (DMDC)
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?	Yes
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	Yes
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.	PHS Officers log in to the CCMIS (Commissioned Corps management Information System) dashboard (COPS-C) system, on the homepage there are links to take officers to different areas including the payroll system (CCP-C). All USPHS Officers within the Commission Corp have access to the payroll site to view their personal payroll information, download pay stubs, see retirement information, etc. The URL for the payroll site is not public and cannot be accessed without logging into the COPS-C system to access the payroll site.
PTA - 10:	Does the website have a posted privacy notice?	Yes
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	No
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?	No
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?	No
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?	No
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	
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.	
PTA - 16:	Does the mobile application/ have a privacy notice?	

PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	
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?	
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?	
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?	No
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 Education Records Military Status Date of Birth Mailing Address Financial Account Info Legal Documents Employment Status Other - Free text Field - SERNO (unique serial number)
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors Vendors/Suppliers/Third-Party Contractors (Contractors other than 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?	Personally Identifiable Information (PII) is primarily used for: 1) Commissioned Corps (CC) officers and others - providing full pay and personnel services. 2) Health and Human Services (HHS) Employees and Direct contractors - to run personnel and payroll transactions on the officers and for authentication purposes to perform job duties. 3) Vendors/Contractors - other contracted staff (non-direct contractors) who support the application and perform administrative duties. The primary use for the PII collected from contractors/vendors, and HHS Employees is only for user access to the system. The primary use for the PII collected on the Commissioned Officers is for running Human Resources (HR) and Payroll operations and providing a monthly payroll.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	There are no secondary uses of Personally Identifiable Information (PII) within Commissioned Corps Payroll - Cloud (CCP-C) system.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	The SSN determines a unique record in database along with other fields like SERNO (unique serial number), date of birth and sex.
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	The Public Health Service Act (42 United States Code (U.S.C.) 202-217, 218a, 224, 228, 233, and other pertinent sections); The Social Security Act (42 U.S.C. 410(m) et seq.); portions of Title 10, U.S.C., related to the uniformed services; portions of the Title 37, U.S.C., related to pay and allowance for members of the uniformed services; portions of Title 38, U.S.C., related to benefits administered by the Department of Veterans Affairs; sections of 50 U.S.C. App., related to the selective service obligations and the Soldiers' and Sailors' Civil Relief Act; Executive Order (E.O.) 9397, 'Numbering System for Federal Accounts Relating to Individual Persons'; E.O. 10450, 'Security Requirements for Government Employment'; and E.O. 11140, which delegates the authority to administer the PHS Commissioned Corps from the President to the Secretary, HHS.

PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	The Public Health Service Act (42 United States Code (U.S.C.) 202-217, 218a, 224, 228, 233, and other pertinent sections); The Social Security Act (42 U.S.C. 410(m) et seq.); portions of Title 10, U.S.C., related to the uniformed services; portions of the Title 37, U.S.C., related to pay and allowance for members of the uniformed services; portions of Title 38, U.S.C., related to benefits administered by the Department of Veterans Affairs; sections of 50 U.S.C. App., related to the selective service obligations and the Soldiers' and Sailors' Civil Relief Act; Executive Order (E.O.) 9397, 'Numbering System for Federal Accounts Relating to Individual Persons'; E.O. 10450, 'Security Requirements for Government Employment'; and E.O. 11140, which delegates the authority to administer the PHS Commissioned Corps from the President to the Secretary, HHS.
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.	SSN, SERNO (unique serial number)
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.	09-90-1402 HHS Payroll Records 09-40-0001 Public Health Service (PHS) Commissioned Corps General Personnel Records
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Hard Copy Mail/Fax Email Government Sources Within the OPDIV Other HHS OPDIV Non-Government Sources Private Sector
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA - 10A:	Provide the information collection approval number.	Office of Management & Budget (OMB) No. 0937-0025 Expiration: 2/28/2027
PIA - 10B:	Identify the OMB information collection approval number expiration date.	2/28/2027
PIA - 10C:	Explain why an OMB information collection approval number is not required.	
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 Within HHS

PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	Personally Identifiable Information (PII) is primarily shared for: 1) Commissioned Corps (CC) officers and others - providing full pay and personnel services. 2) Health and Human Services (HHS) Employees and Direct contractors - to run personnel and payroll transactions on the officers and for authentication purposes to perform job duties. 3) Vendors/Contractors - other contracted staff (non-direct contractors) who support the application and perform administrative duties. The primary use for the PII collected from contractors/vendors, and HHS Employees is only for user access to the system. The primary use for the PII collected on the Commissioned Officers is for running Human Resources (HR) and Payroll operations and providing a monthly payroll.
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)).	MOU between CCP-C and XMS (NextGen External User Management System) for Personal Identity Verification (PIV) integration for sign in and Multi Factor Authentication (MFA) requirements Commissioned Officers Personnel System Cloud (COPSC) and CCP-C MOU for PII sharing.

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.	Data stored on Managed Disks are encrypted at rest using 256-bit AES (Advanced Encryption Standard) FIPS (Federal Information Processing Standard) 140-2 compliant Azure Storage Service Encryption, where the encryption keys are Microsoft-managed keys stored in Azure Gov. Data backups are double encrypted, first using 256-bit AES file level encryption, and then stored on 256-bit AES FIPS 140-2 compliant encrypted Azure Storage Service Encryption. Data stored in the Oracle database is secured using Oracle Database Security. User accounts are password protected and subject to Oracle role-based access and privileges. CCP-C uses an Oracle package to create masked tables in a secured schema within the production database instance. Database table columns that are not tagged as PII are joined with randomized data to produce a complete set of masked tables. Randomized data is generated using third party test data generation tools and custom Oracle SQL (Structured query language) scripts. The masked tables are not accessible to anyone or any application outside of the embedded service principal executing the Oracle package. These masked tables are then encrypted and exported for use within the test environment. Production data never leaves the production Oracle database instance. CCP-C uses data masking provided by tonic.ai to remove PII and create Test data. The data masking process we employ eliminates PII from non-production data. No safeguarded (Production) PII is used to derive non-production data. The process used to create non-production data involves data masking (see diagram) whereby PII is tagged and removed. Those data fields – where PII had existed – are replaced by randomized data that does not resemble production data. Production data never leaves the CCP-C production Oracle database instance. CCP-C uses an 3rd party package (tonic.ai) to create masked tables in a secured schema within the production database instance. Database table columns that are not tagged as PII are joined with randomized data to produce a complete set of masked tables. Randomized data is generated using third party test data generation tools. The masked tables are not accessible to anyone or any application outside of the embedded service principal executing the Oracle package. These masked tables are then encrypted and exported for use within non-production environments.
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.	When an Officer applies to the Corps, they are notified via the application materials how their data will be used. Officers consent to the Personally Identifiable Information (PII) use by sending the data into the Corps as part of their application process. Corps Officers also sign data collection forms. The perspective applicant to the Commissioned Corps is required to complete the PHS-50 form which explicitly addresses the Privacy Act regarding the PII that is requested and collected. The form requires a signature by the applicant agreeing to provide the requested information on PHS-50 form. Should the applicant be selected to become a Commissioned Corps Officer, the relevant officer's information (provided on the PHS-50 form) is then entered into the CCP system by the technicians. PHS-50 provides the following Privacy Act Notice: Privacy Act Notice This statement is provided pursuant to the Privacy Act of 1974 (5 U.S.C. 552a). Our authority to collect this information is 42 U.S.C. 202 et seq.; and Executive Order 9397, 'Numbering System for Federal Accounts Relating to Individuals Persons.' The information provided on this form will become part of record systems 09-40-0001, 'Public Health Service (PHS) Commissioned Corps General Personnel Records. This information is collected in order to assess the qualifications of each applicant and make a determination whether the applicant meets the requirements to receive a commission. The information is used to make determinations on candidates/applicants seeking appointment to the Corps to assess whether they are suitable for life in the uniformed services based upon a review of a variety of assessment factors including, but not limited to: employment history, character, suitability investigation clearance, and a candidate's prior history of service in one of the uniformed services. Their potential for leadership as a commissioned officer and their ability to deal effectively with people is evaluated. Copies of these systems of records may be obtained by contacting the Commissioned Corps Headquarters office. This information will be used only as necessary in personnel administration processes carried out in accordance with established regulations and published notices of systems of records. Personally Identifiable Information (PII) submission is required for seeking employment as an active duty Commissioned Corps officer. Individuals can opt-out of the collection or use of their PII, and they will not be considered for Public Health Service Active Duty appointment. Consent for the collection, use and appropriate sharing of employees' PII for payment purposes

		is implicit in the employer/employee relationship. Procedures for receiving payment for work are also addressed as part of employee in-processing.
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.	Relevant major changes to this system are not expected, but if they were to occur and notification of individuals were necessary, several avenues of communication would be available. This includes providing notices on physical pay stubs and using e-mail listservs specific to the Public Health Services organization.
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.	Individuals that suspect their information has been misused can contact the Commissioned Corps' (CC) Help Desk via a dedicated email account, cchelpdesk@hhs.gov. Individuals must supply their name and the unique Serial number assigned to them. Every officer has a unique serial number assigned to him. This number will uniquely identify a specific CC officer. This individual escalates concerns to the Director, who contacts security staff for the Office of the Assistant Secretary of Health (OASH), under the OS. Security staff are well-versed in HHS incident handling procedures, which are HHSwide and consistent with federal requirements.
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.	On a monthly basis, the Financial Services Branch reconciles payroll against transactions and the System Federal team validates the payroll ensuring no inappropriate parties have received payment. In response to a request for correction, a technician can enter a Nature of Action (NOA) code that will permit an edit in the Commissioned Corps Payroll system. This can only be done if the data subject submits written documentation to the Commissioned Corps Personnel office. Staff will then validate the information and enter it into the System via an NOA Code update. The software then updates the Commissioned Corps Payroll system with the new data.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors Third-Party Contractor (Contractors other than HHS 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.	Personally Identifiable Information (PII) is primarily used for: 1. **Users:** Commissioned Corps (CC) officers need access to PII for full pay and personnel services. 2. **Administrators:** Health and Human Services (HHS) Employees and Direct contractors need access to PII to run personnel and payroll transactions on the officers and for authentication purposes to perform job duties. 3. **Developers and Contractors** and other contracted staff (non-direct contractors) need access to PII to support the application and perform administrative duties. The primary use for the PII collected from contractors/vendors, and HHS Employees is only for user access to the system. The primary use for the PII collected on the Commissioned Officers is for running Human Resources (HR) and Payroll operations and providing a monthly payroll.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Level of access is determined by the user role. User roles access the data through pre-defined transactions. Only Systems Administrators have direct database access. User accounts are locked after 60 days of inactivity and quarterly reviews of login activity are used to deactivate accounts. Accounts are also deactivated upon request from the account holder's supervisor or the Systems Administrator.
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.	Access levels are provided and restricted based on the user's role and responsibilities.
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.	The HHS Office of the Secretary complies with the Federal Information Security Management Act (FISMA) requirement that all agencies require all system users (employees and contractors) to be exposed to security awareness materials, at least annually and prior to the employee's use of, or access to, information systems. Current trainings includes: Information Systems Security Awareness Training Privacy Awareness Training

PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	A quarterly CCP-C training session is presented to system users as part of Quarterly Commissioned Corps All-Hands meeting. Topics include how to securely work with Commissioned Corps data elements for reporting purposes; Presentation on the various Role based access that is available for users and annual authorization validation before access is granted; discussion of newly implemented security features in the current release; Demonstration of available reporting features of the system that help diagnose system performance and help troubleshoot issues; Discussion of planned future enhancements of the system.
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).	Information is maintained in the system as long as it is needed for servicing pay, performing personnel actions or reporting to Government authorities. At activation or new hire, employees are assigned a reference number. This reference number is utilized as part of our online audit trail feature. Each data entry, transaction, event and every business rule is time-stamped (stored at a point in time). This architecture provides complete access to an historical audit trail, enables searching or reporting on transactions by employee, automates back-out of any HR/payroll action and enables tracking of input errors. Payroll and HR transactions and other calculations are recorded in perpetuity. When officers retire or separate from duty, the records are marked with the appropriate status and removed from active status. The data are never deleted nor overwritten. If the Government ceases to use the current contractor then the entire historical database is transferred to the Government, and following confirmation, the information will be deleted by magnetically and physically destroying the storage media. General Records Schedule (GRS) GRS 3.1 General Technology Management Records. 010, information technology development project records. Disposition Instruction: Temporary. Destroy 5 years after project is terminated, but longer retention is authorized if required for business use. Disposition Authority: DAA-GRS2013-00050006 GRS 3.1 General Technology Management Records. 011, system development records. Disposition Instruction: Temporary: Destroy 5 years after system is superseded by a new iteration, or is terminated defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required by business use. For payroll records, GRS 2.4 Employee Compensation and Benefits Records. DAAGRS- 2016-0015-0004 Agency Payroll for each pay period. Disposition instruction: Temporary: Destroy when 56 years old.

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.	Administrative: All requests for user accounts in the system must be justified by the user's supervisor and approved by the system owner. Officer data is submitted and monitored by the officer. Signed Rules of Behavior forms are collected from users on a regular basis. Technical: Accounts are individual, with usernames and complex passwords. Role based access to data. Servers protected by Microsoft's Azure Cloud security infrastructure. Physical: The physical server security is provided at Microsoft's Azure environment.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	3/3/2025
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:**	3/5/2025
		SOP Days Open:	6

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	3/6/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 3/6/2025 all comments have been address for PTA-5, this could be update via 508 process as it seems OS was not able the update the PTA. Submitting for approval and for updates to be made to the PTA via 508 process. 2/25/2025: Please see the following comments and update accordingly: **PTA-5:** need to replace word “gender” with “sex.” **PIA-10A and PIA-10B:** Per reginfo.com the expiration date for the OMB number is 2/28/2027.	**Agency Privacy Analyst Days Open:**	1

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	3/11/2025
		SAOP Days Open:	5

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 11C	Data Feed Service, piafrmos_Release	2/11/2025	Please define/spell out the acronyms AMS/XMS, PIV, and COPSC on first use within this response.	
PIA - 11D	Data Feed Service, piafrmos_Release	2/11/2025	Please define/spell out the acronyms AES FIPS, SQL, and PHS on first use within this response.	
PIA - 18	Data Feed Service, piafrmos_Release	2/11/2025	This response should detail the reason(s) why each of the groups of individuals identified in PIA-17 (Users, Administrators, Developers, and Contractors) requires access to the PII on the system.	
PIA - 6	Data Feed Service, piafrmos_Release	2/13/2025	Please replace the word Gender with Sex per new executive order.	
PIA - 10A	VILLAFUERTE, NESTOR	2/25/2025	Please update the OMB number	
PIA - 10A	BLAND, CRYSTAL	2/26/2025	Per reginfo.com, the expiration date is 2/28/2027, please update accordingly.	
PIA - 10B	BLAND, CRYSTAL	2/26/2025	Per reginfo.com, the expiration date is 2/28/2027, please update accordingly.	
PIA - 1	BLAND, CRYSTAL	2/26/2025	Update for PTA-5: replace the word "gender" with "sex."	

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:	3/11/2025 9:29 AM	**History Log:**	View History Log