PTA / PIA: OS - COPSC - QTR1 - 2026 - OS3303768

Created Date: 4/15/2026 1:03 PM Last Updated: 4/21/2026 1:03 PM

General Information

PTA / PIA Name:	OS - COPSC - QTR1 - 2026 - OS3303768	**PTA / PIA ID:**	4414151
Component Name:	OS - Commissioned Officers Personnel System Cloud	**ATO Boundary Name:**	Commissioned Officers Personnel System Cloud
Overall Status:	Complete	**# of Days - Open:**	75
Submitter:		**Submit Date:**	4/13/2026
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OpDiv:**	OS
Security Categorization:	Moderate		
Make PIA available to Public?:	No	**PIA Required:**	Yes

General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
General 02:	Is this a FISMA-Reportable system?	Yes
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
General 04:	ATO Date or Planned ATO Date.	6/7/2027
General 05:	Is the system or electronic information collection, agency or contractor operated?	Contractor
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Pratishtha Bhatt
PTA 01A:	POC Title and Organization	ISSO, OS/OASH
PTA 01B:	POC Email Address	pratishtha.bhatt@hhs.gov
PTA 01C:	POC Phone Number	(240) 276-8179
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Agency

PTA 04:	Please give a brief overview of the purpose of the system by describing what the functions of the system are and how the system carries out those functions in support of HHS.	The COPSC system is an HHS Major Application categorized with a Federal Information Processing Standards (FIPS) 199 Security Categorization of Moderate (M-M-M). COPSC is Publicly accessible, and an HHS Privacy sensitive system hosted in the Amazon Web Services (AWS) GovCloud IaaS Federal Risk and Authorization Management Program (FedRAMP) Cloud Service Provider (CSP) High environment (Package ID # F1603047866). COPSC's mission is to provide a platform for conducting and supplementing CC (Commissioned Corps) human resources (HR) and payroll reporting functions. COPS-C sends and receives data from the Commissioned Corps Payroll Cloud (CCP-C). It provides the data necessary to identify officers in the Commissioned Corps Business Process Management Cloud (CCBPM-C) system. In addition, COPSC initiates payroll data transmission by manual Secure File Transfer Protocol (SFTP/SSH) to other external systems. The COPSC system is comprised of the following four components: 1) Commissioned Corps Information Management System (CCMIS) website – a public site, https://dcp.psc.gov/ccmis, containing information for Public Health Service (PHS) officers, liaisons, and administrators. 2) PAC (Professional Advisory Committees) web content management site – https://dcp.psc.gov/osg/, which is available to the selected PAC committee members on the network for managing content. 3) COPSC Database -- an oracle database that contains HR data and payroll data received for active-duty officers from the CCP-C (Commissioned Corps Payroll cloud) system used for reporting purposes only. 4) United States Public Health Service (USPHS) website -- a public facing website, https://www.usphs.gov/, containing information for individuals interested in serving in the CC. Additionally, the COPSC system supports CCMIS Secure area applications that can be reached after multi-factor authentication.
PTA 05:	List and/or describe all the types of information that are collected, maintained, and/or shared by the system regardless of whether that information is PII and how long that information is stored.	Only the COPSC oracle database audit records over a year are being purged, any record under a year is maintained on the system. The COPSC application data maintains records permanently and has records back to 1998. COPSC system contains Personally Identifiable Information (PII) because some of its six-child subsystem listed below, each having their own Privacy Impact Assessments (PIAs), contains PII such as: Social Security Number (SS#), Officer's demographic, assignment, award,

administrative action, payroll, and promotion data stored and maintained in the systems listed below:

1) COPSC-Public Health Service Human Resources Applications

2) COPS10GDBPHSPAYROLL
3) COPS10GDB-PHSPUBLICINFOCCMIS

4) COPS10GDB-THICKCLIENT

5) COPS10GDBCOER

6) COPS10GDB-READINESS

COPSC non-PII data can be found in each of its subsystems described below.

1) COPS10GDB-Public Health Service Human Resources Applications: Commissioned Corps Pay and Personnel System (COPS10GDB) tracks non-payroll-related Corps Officers' Human Resource (HR) data pertaining to, and including, officer demographic, assignment, award, administrative action, assimilation, and promotion
data. It consists of two child subsystems -- thick client and thin client.

2) COPS10GDB-PHSPAYROLL: The Commissioned Corps Payroll (CCP) system generates the payroll on a monthly basis that is used for post-payroll processing. These Payroll Transaction files are moved to the Commissioned
Officer Personnel System (Oracle) 10G Data Base (COPS10GDB) system (a separate HHS system) for final payroll processing.

3) COPS10GDBPHSPUBLICINFO CCMIS: The purpose of this website is to provide the public with information
about the Commissioned Corps Management and display information related to and helpful for the Public Health Service (PHS) Commissioned Corps Officers. This Website does NOT collect data.

4) COPS10GDB-THICKCLIENT: The system supports the Human Resources (HR) office of the U.S. Public Health Service Commissioned Corps (USPHS CC). More specifically, the system provides New Applicant processing information, Oracle Password reset, and Manual Commissioned Officer Effectiveness Reporting (COER) profile Maintenance entries.

5)COPS10GDB-COER: COER is a web-based system that provides a platform for the supervisors and reviewing officials to provide annual officer performance evaluation for the 6,700+ Commissioned Corps (CC) Active-Duty population.

6) COPS10GDB-READINESS: The purpose of the Readiness (is also called REDDOG) application is for officers to self-service all personal and readiness data. The administrative REDDOG is for REDDOG

		administrative users to view officer's data and process their readiness. The following information is stored by the above-mentioned systems of COPSC: Username and Password (User Credentials) SSN, Name, E-Mail Address, Phone Numbers, Medical Notes Certificates, Education Records, Military Status, Date of Birth, Mailing Address, Medical Records Number, Device Identifiers, Employment Status, Marital Status, and User credentials are being stored on Commissioned Officers Personnel System 10GDB (COPS10GDB) Only direct (not indirect) contractors support this system, and their above information is also stored in this system. Direct Contractors means the non-Federal, HHS employees. They are contractors but work alongside the Federal Employees in a Federal Office location. They are not regular system users but can be considered as administrators (code developers and database developers), and their user credentials are collected to allow them access this system for the purpose of application development and testing only. The information collected from them allows them access to this system, only for those purposes, are Username, Password, Personal Identity Verification (PIV) card and/or email address, Mailing Address, Phone Number and Date of Birth.
PTA 05A:	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.
PTA 05C:	Please identify the system that maintains the user credentials or controls access to this system.	ACCESS MANAGEMENT SYSTEM (AMS/XMS)
PTA 06:	Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual.	COPSC system contains PII, because some of its six child subsystems listed below, each having their own Privacy Impact Assessments (PIAs), contains PII data: SS#, Officer's educational qualification, license information, duty station location, agency and position identification, dependent details, state tax and federal tax details, determination of pay categories, and gross to net calculations. 1) COPS10GDB-Public Health Service Human Resources Applications 2) COPS10GDBPHSPAYROLL 3) COPS10GDBPHSPUBLICINFO CCMIS 4) COPS10GDBTHICKCLIENT 5) COPS10GDB-COER 6) COPS10GDB-READINESS 1) COPS10GDBPublic Health Service Human Resources Applications - Commissioned Corps Pay and Personnel System (COPS10GDB) tracks nonpayroll- related Corps Officers' Human Resource (HR) data pertaining to, and including, officer demographic, assignment, award, administrative action, assimilation, and

promotion data. It consists of two child subsystems -- thick client and thin client.

2) COPS10GDBPHSPAYROLL – The Commissioned Corps Payroll (CCP) system generates the payroll on a monthly
basis that is used for post-payroll processing. These Payroll Transaction files are moved to the Commissioned Officer Personnel System (Oracle) 10G Data Base (COPS10GDB) system (a separate HHS system) for final payroll processing.

3) COPS10GDB-PHSPUBLICINFO CCMIS - The purpose of this website is to provide the public with information about the Commissioned Corps Management and display information related to and helpful for the Public Health Service (PHS) Commissioned Corps Officers. This Website does not collect data.

4) COPS10GDB-THICKCLIENT - The system supports the Human Resources (HR) office of the U.S. Public Health Service Commissioned Corps (USPHS CC). More specifically, the system provides New Applicant processing information,
Oracle Password reset, and Manual Commissioned Officer Effectiveness Reporting (COER) profile Maintenance entries. 5) COPS10GDB-COER - COER is a web-based system that provides a platform for the supervisors and reviewing officials to provide annual officer performance evaluation for the 6,700+ Commissioned Corps (CC) Active-Duty population.

6) COPS10GDB-READINESS – The purpose of the Readiness (is also called REDDOG) application is for officers to self- service all personal and readiness data. The administrative REDDOG is for REDDOG administrative users to
view officer's data and process their readiness. The following information is stored by the abovementioned
systems of COPS10GDB: Username and Password (User Credentials) Social Security Number Name E-Mail Address Phone Numbers Medical Notes Certificates Education Records Military Status Date of Birth Mailing Address
Medical Records Number Device Identifiers Employment Status Marital Status Direct contractors are being used to work on this system, and their above information is also stored in this system. Direct Contractors means the non-Federal, HHS employees. They are contractors but work alongside the Federal Employees in a Federal Office location. They are not regular system users but can be considered as administrators (code developers and database developers), and their user credentials are collected to allow them access this system for the purpose of application development and testing only. The information collected from them in order to allow them access to this system, only for those purposes, are Username, Password, Personal Identity Verification (PIV) card and/or email address, Mailing Address,

		Phone Number and Date of Birth.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	Yes
PTA 08A:	Provide the URL(s).	https://www.usphs.gov/ https://dcp.psc.gov/ccmis/ https://dcp.psc.gov/OSG/
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	Yes
PTA 09:	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.	Interested parties in the US Public Health Service. Includes careers or applicant enrollment starting point. Public, Individual Personnel, Readiness, Recruitment, and Payroll Information, Electronic Document Upload (e-DOCU), Electronic personnel folder (eOPF). Users access the website using public URL followed by login using their user credentials/Personal Identity Verification (PIV) credentials.
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?	Yes
PTA 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	No
PTA 12:	Does the website use web measurement and customization technology?	No
PTA 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA 14:	Does the system have a mobile application?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

Privacy Impact Assessment

Privacy Impact Assessment

PIA 22:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Identifying Numbers Social Security Number Device Identifiers Biographical Information Name Date of Birth User Credentials Certificates (e.g., training certificates) Education Records Employment Status/History Contact Information Email Address (Personal) Mailing Address (Personal) Phone Numbers (Personal) Medical Information Medical Records Number Other Other
PIA 22A:	Identify the "other" type(s) of personally identifiable information (PII) not mentioned in the above list.	Medical Notes, marital, Status, demographic, assignment, award, administrative action.
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	500 – 4,999
PIA 25:	For what primary purpose is the PII used?	Commissioned Officers Personnel System Cloud (COPSC) is an umbrella system, representing six different systems, that provides an integrated solution for the Commissioned Corps. COPSC stores all of the human resource (HR) data used by the Corps to manage its officers, supports the daily HR related activity (HR use only), and is used as a data reporting tool that is available to Officers and to HR staff. Functions supported include Yearly Officer Evaluation entry by Officers and their supervisors, Officer Leave Tracking management, reports for HR staff that display Officer data, for Payroll Tracking purposes, and applications for entry into the Commissioned Corps.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	PII is not used for secondary purposes.

PIA 27:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses include that in your response.	Function of the SSN is for payroll and tax information required to remit any applicable taxes to the state or Internal Revenue Service (IRS), including Federal Insurance Contributions Act (FICA) and to generate federal tax documents. Personally Identifiable Information (PII) is used within the system to identify veterans who are eligible to receive benefits from the Veterans Affair (VA) office. Previously, physical packages were sent for veterans of the Office of Assistant Secretary of Health (OASH) United States Public Health Service (USPHS) to the VA office. These packages used physical resources and could be subject to loss by the courier delivering the package. Medical records and PII are submitted to the VA office for benefit processing. The Social Security Number (SSN) is the identifier used to submit the package through an Application Programming Interface (API) that the Veterans Affair (VA) office provides to other federal agencies. The VA API is unique to each office, and the United States Public Health Service (USPHS) has its own unique API key to submit this information. Using the SSN as the identifier, the VA office will know to whom the documents belong to within their system. All information is encrypted using Transport Layer Security (TLS) encryption and a designated API key.
PIA 27A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses, you may respond N/A.	Usage of veteran SSNs for the Veteran Affairs (VA) office is required for the VA office. Additional information on necessity can be found here: https://www.oprm.va.gov/privacy/SSNReduction.aspx
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	Please see Executive Order 11140 at the following link: https://www.archives.gov/federalregister/codification/executive-order/11140.html. Executive Order 11140 (Jan 30, 1964), 'Delegating certain functions of the President relating to the Public Health Service,' permits the Secretary of Health and Human Services (HHS) broad powers to appoint commissioned officers of the Reserve Corps; to prescribe titles, Appropriate to the several grades, for commissioned officers of the public health service (PHS) other than medical officers; to make or terminate temporary promotions of commissioned officers of the Regular Corps and Reserve Corps; and the authority to prescribe regulations appropriate to the operation of the Corps. Note that the text of this Executive Order is also available in the Federal Register at 29 FR 1637 and in the Code of Federal Regulations at 3 CFR, 1964-1965.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA 29A:	Please specify which PII data elements are used to retrieve records.	SERNO (Service Number), SSN, Name
PIA 29B:	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.	09-40-0001 PHS CC General Personnel Records

PIA 30:	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 Government Sources Within the OPDIV Other HHS OPDIV
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA 31A:	Provide the information collection approval number(s) and expiration date(s).	OMB 3060-1241 expiration date: 7/31/2025
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	Yes
PIA 32A:	Identify with whom the PII is shared or disclosed.	Other Federal Agency/Agencies Within HHS
PIA 32B:	For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.	PII is shared within other federal agencies/systems listed below: 1. **Agency Portal System (APS)** - Accenture Federal Services (AFS)/Federal Retirement Thrift Investment Board (FRTIB). COPSC shares payroll contributions, loan payments, participant indicative data, adjustments to the agency. 2. **ASPR Ready System** - ADMINISTRATION OF STRATEGIC PREPAREDNESS AND RESPONSE (ASPR). ASPR Ready and COPSC exchanges rostering data for Personnel Accountability of PHS responders. 3. **BOPNet System** - Department of Justice (DOJ)/Bureau of Prisons (BOP). COPSC system provides staffing and payroll data of active-duty Commissioned Corps officers to BOPNet system. 4. **Business Intelligence Information System (BIIS) -** HHS OCIO OEAD. COPSC provides officer demographic and payroll data to BIIS. 5. **CCBPM-C** system - HHS/OS/OASH/CCHQ. COPSC provides officer data necessary to run Promotion, Retention, and Flag boards to CCBPM. Document Storage and Retrieval from CCBPM-C. 6. **CCP-C** system - HHS/OS/OASH/CCHQ. COPSC receives and sends HR data and payroll data for active-duty officers from the CCP-C system used for reporting purposes only. 7. **CDC Comm Corps Data Feed System** - HHS Centers for Disease Control and Prevention (CDC). COPSC provides personnel and pay data of active-duty CC

officers in a fixed format for the reporting period to support consolidated departmental reporting done by the civilian personnel systems.

8. **CFC Online Donation System (cfcgiving.opm.gov) -** Office of Personnel Management – Combined Federal Campaign (OPM-CFC). COPSC transmit payroll related data files for Combined Federal Campaign, Give Back Foundation and TASC systems and supply payroll information of Commissioned Corps Officers.
9. **Defense Enrollment Eligibility Reporting System (DEERS) -** Defense Manpower Data Center (DMDC). COPSC requires use of the Defense Enrollment Eligibility Reporting System (DEERS) personnel data for commissioned Corps Officers.
10. **Enterprise Administrative Support Environment (EASE) system** - HHS/FDA. COPSC provides demographic data for CC officers assigned to the FDA Enterprise Administrative Support Environment (EASE) via sFTP/SSH.
11. **Enterprise Security Controls (ESC)** system - DOT Bureau of Fiscal Services. COPSC sends payment files to ESC system.
12. **Human Resource Management Enterprise Service Bus (HRMESB)** MOU - "HHS Assistant Secretary for Administration (ASA) OFFICE OF HUMAN RESOURCES (OHR) ". COPSC provides Compensation, Benefits, Employee Performance, Employee Relations, Separation Management, HR Development Information to HRMESB
13. **National Directory of New Hires (NDNH) System** - Social Security Administration (SSA) and HHS Administration for Children and Families (ACF), Office of Child Support Enforcement (OCSE). COPSC provides officer payroll data to the ACF/OCSE.
14. **NIH Business Intelligence System (NBIS) system-** HHS NIH CIT. COPSC provides personnel and pay data of active-duty Commissioned Corps officers in a fixed format for the reporting period to support consolidated departmental reporting done by the civilian personnel systems.
15. **Secured Payment System (SPS)** - Dept of Treasury/BFS/FDS. COPSC shares officer payroll data, which is sensitivity CUI, financial information as well as Privacy Act data with SPS.
16. **Unified Financial Management System (UFMS)** - HHS Office of Finance. COPSC provides officer demographic data to the Unified Financial Management System (UFMS) via sFTP/SSH.
17. **Accounting for Pay System (AFPS) ISA** - HHS FINANCIAL MANAGEMENT AND

		PROCUREMENT PORTFOLIO (FMP)/ACCOUNTING SERVICES (AS). COPSC provides officer payroll data to the Accounts for Pay System (AFPS).
PIA 32C:	List any agreements in place that authorize the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	1. **Agency Portal System (APS)** ISA - Accenture Federal Services (AFS)/Federal Retirement Thrift Investment Board (FRTIB). 2. **ASPR Ready System** ISA - ADMINISTRATION OF STRATEGIC PREPAREDNESS AND RESPONSE (ASPR) 3. **BOPNet System** MOU - Department of Justice (DOJ)/Bureau of Prisons (BOP) 4. **Business Intelligence Information System (BIIS)** MOU - HHS OCIO OEAD 5. **CCBPM-C** MOU - HHS-OS OASH/CCHQ 6. **CCP-C** MOU - HHS-OS OASH/CCHQ 7. **CDC Comm Corps Data Feed System** ISA - HHS Centers for Disease Control and Prevention (CDC) 8. **CFC Online Donation System (cfcgiving.opm.gov) ISA -** Office of Personnel Management – Combined Federal Campaign (OPM-CFC) 9. **Defense Enrollment Eligibility Reporting System (DEERS) ISA & MOU -** Defense Manpower Data Center (DMDC) 10. **Enterprise Administrative Support Environment (EASE) ISA** - HHS/FDA 11. **Enterprise Security Controls (ESC)** MOU - DOT Bureau of Fiscal Services 12. **Human Resource Management Enterprise Service Bus (HRMESB)** MOU - "HHS Assistant Secretary for Administration (ASA) OFFICE OF HUMAN RESOURCES (OHR) " 13. **LHI-MedNet** MOU - OptumServe 14. **National Directory of New Hires (NDNH) System** ISA - SSA and HHS Administration for Children and Families (ACF), Office of Child Support Enforcement (OCSE) 15. **NIH Business Intelligence System (NBIS) ISA -** HHS NIH CIT 16. **Secured Payment System (SPS)** ISA - Dept of Treasury/BFS/FDS 17. **Unified Financial Management System (UFMS)** MOU - HHS Office of Finance 18. **ASPR GHS** System MOU - ADMINISTRATION OF STRATEGIC PREPAREDNESS AND RESPONSE (ASPR) 19. **Access Management System (AMS)** MOU - HHS DCIO-OPS 20. **Accounting for Pay System (AFPS) ISA** - HHS FINANCIAL MANAGEMENT AND PROCUREMENT PORTFOLIO (FMP)/ACCOUNTING SERVICES (AS)

PIA 32D:	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.	The System owner (SO) and Information System Security Officer (ISSO) for the COPSC system maintains Interconnection Security Agreements (ISAs)/ Memorandum of Understanding for PII shared with external/internal agencies. Information related to PII, the fields, encryption type and sharing frequency are documented in the ISAs/MOUs. COPSC is hosted in Amazon Web Services (AWS) GovCloud. AWS CloudTrail is configured to ensure logging and accountability is implemented for all COPSC PII information maintained in the system; all actions involving PII are logged, including who accessed the data, when, and from where. AWS CloudWatch Logs collects application-level logs for accounting for PII maintained within any COPSC application. Access to PII is controlled via AWS Identity and Access Management (IAM), granting permissions based on COPSC system administrators and Commissioned Corps Headquarters (CCHQ)/US Public Health Services (USPHS) user roles and individuals accessing PII in the system. All PII is encrypted at rest and in transit using AWS Key Management Service (KMS), allowing for tracking of key usage when PII is accessed.
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary
PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	Individuals consent regarding PII is obtained when the individuals apply to the Commissioned Corps (CC). They are also notified at that time about the PII being collected from them and how it will be used. Individuals are informed of how the data will be used and who it will be shared with as part of their on-boarding process. Individuals can opt-out of information collection by refusing to apply for available positions within the Commissioned Corps.
PIA 35:	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). If they cannot be notified or have their consent obtained, explain why.	The Corps notifies its users of major changes to the system via electronic email and via a splash screen shown before the login screen. The splash screen also includes a consent clause indicating that the Government will use the data contained within the system to conduct legitimate Government HR business. Users must agree before continuing on to the system log in.

PIA 36:	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 Headquarters (CCHQ) Help Desk via a dedicated email account, cchelpdesk@psc.gov. Individuals must supply their name and Public Health Service (PHS) Serial number. This individual escalates concerns to the Director, who contacts security staff for the Occupational Safety and Health Administration (OASH) Security staff are well-versed in HHS incident handling procedures, which are HHS-wide and consistent with federal requirements.
PIA 37:	Describe the process in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of the PII in the system. Please address each element in your response. If no processes are in place, explain why not.	Information in COPSC is not routinely or automatically validated or updated against an external record, but corrections can be made as indicated. Specifically, in response to a request for correction, a technician can enter a Nature of Action (NOA) code that will permit an edit in the CC Payroll system. This can only be done if the data subject submits written documentation to the CC Personnel office. Staff will then validate the information and enter it into the System via an NOA Code update. The software then updates the CC Payroll system, which provides information to the database (COPSC) with the new data. In a broader sense, integrity of the data is also managed via an audit process. An annual SSAE-16 (Service Organization Control Report) Type II Assessment is conducted each year by an independent Auditing firm of the security controls that are in place in the Lyceum system. This is an annual requirement by the HHS Auditors. The final SSAE-16 report is provided to the HHS Auditors and is a report on Lyceum's description of the system and the Suitability of the design and operating effectiveness of controls for the Audit period October 1 through June 30th of each year. The SSAE-16 examines each security control to ensure that they are proper and effective for the type of information/data that is stored.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA 38A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA 38B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes

PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Administrators have access rights to view PII to make changes or edits to incorrect information and link to other databases that are linked to the COPSC system to generate payroll files. Developers only have access for user acceptance testing (UAT) testing for significant changes that require tests to use real PII data to determine the system is pulling correctly to generate payroll to ensure there is no system failure and Commission Corp officers are paid correctly and on time. Level of access is determined by the user role. All roles except Administrator limited to read only access. Access accounts are locked after 60 days inactivity and quarterly reviews of login activity are used to deactivate accounts. Accounts are also deactivated when request is received from account holder's supervisor.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Access levels are provided and restricted based on the user's role and responsibilities.
PIA 41:	Describe the technical methods in place to allow those with access to PII to access only the minimum amount of information necessary to perform their job.	Roles are assigned to each individual within the system; only specific roles can access specific information. Only those with a need to know can access sensitive information.
PIA 42:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) 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 include Information Systems Security Awareness Privacy Awareness Training and training for Privileged Users. This training is conducted through the HHS Learning Management System (LMS).
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	A quarterly COPSC training session is presented to system users as part of Quarterly CC All-Hands meeting. Topics include how to securely work with CC 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; and discussion of planned future enhancements of the system.

PIA 44:	Describe the process and guidelines in place for 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 and personnel actions and then moved to historical files. The information is not destroyed. Following is the General Records Schedule (GRS) in use, that applies to the PII maintained in this system; GRS 3.1. Item 012, Disposition Authority: DAA-GRS-2013-0005-0008. Special purpose computer programs and applications - Computer software programs or applications that are developed by the agency or under its direction solely to use or maintain a master file or database authorized for disposal in a GRS item or a National Archives and Records Administration (NARA) approved records schedule. Disposition Instructions - Delete when related master file or database has been deleted, but longer retention is authorized if required for business use. Note: Computer software needs to be kept as long as needed to ensure access to, and use of, the electronic records in the system throughout the authorized retention period to comply with 36 CFR Sections 1236.10, 1236.12, 1236.14, and 1236.20.
PIA 45:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	Physical Controls COPSC maintains stringent physical security to protect the infrastructure hosting Personally Identifiable Information (PII)/ Personal Health Information (PHI): Isolated Regions: Physically isolated from standard AWS regions, with data center access restricted to vetted U.S. citizens. Infrastructure Security: Data centers are secured with 24/7 surveillance, physical security guards, and biometric access controls. Hardware Security: Use of Federal Information Processing Standard (FIPS) 140-2 or 140-3 validated cryptographic modules for data protection. Technical Controls COPSC Technical controls ensure PII data is protected at rest, in transit, and in use: Encryption at Rest & In Transit: Using AWS Key Management Service (KMS) or CloudHSM, data is encrypted at rest in services like S3, RDS, and DynamoDB. Transport Layer Security (TLS) is used to encrypt data in transit. Access Control & IAM: AWS Identity and Access Management (IAM) allows fine-grained access

control based on the principle of least privilege.

Data Classification & Detection: Services like Amazon Macie are used to discover, classify, and protect sensitive PII in S3 buckets.

PII Masking & Redaction: Amazon Comprehend and AWS Glue DataBrew are used to automatically detect, mask, or redact PII in text documents and datasets.

Network Segmentation: Use of Virtual Private Clouds (VPC) and security groups (firewalls) to isolate workloads.

Advanced Protection (HYOK): For highly sensitive PII, customers can use "Hold Your Own Key" (HYOK) to ensure data is encrypted on-premises before being loaded into AWS, preventing even authorized cloud administrators from viewing it.

Administrative Controls
COPSC Administrative controls focus on policies, procedures, and personnel management:

Business Associate Agreement (BAA): Customers must enter a BAA with AWS to process, store, or transmit Personal Health Information (PHI).

Personnel Screening: Only authorized, vetted COPSC U.S. persons are allowed to manage and access account keys and data.

Security Training: COPSC Personnel must undergo regular security awareness training, including PII handling procedures.

Monitoring & Auditing: COPSC has continuous monitoring using AWS CloudTrail (logging Application Programming Interface (API) calls), AWS Config (tracking configuration changes), and Amazon CloudWatch.

Incident Response: Strict policies for breach reporting and response in compliance with Defense Federal Acquisition Regulation (DFAR) and Health Insurance Portability and Accountability Act (HIPAA) rules.

Data Disposal: Procedures for sanitizing, purging, or destroying PHI/PII media when no longer needed.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	4/14/2026
Privacy Analyst Review Comments:	This PIA is ready for your review. All necessary questions have been answered. Thank you, Jon	**# of Days - PA Review:**	1

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	4/15/2026
SOP Review Comments:	Hello, Please review my comments and make the appropriate changes within your responses. Thank you, Muriel.	**# of Days - SOP Review:**	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	4/16/2026
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 4/16/2026 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	1

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	4/21/2026
SAOP Review Comments:		**# of Days - SAOP Review:**	5

SAOP Signature

Date	User	Type	Name	Original Value	New Value
4/21/2026 10:38 AM	BAUR, VANESSA	Signature	SAOP (Email PIN)		Content Signed

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PTA 09	Data Feed Service, pta_pia_OS_Release	4/13/2026	Please state how users access the web site (via public URL, log in, etc.). Please spell out e-DOCU and eOPF at first use.	
PTA 04	Data Feed Service, pta_pia_OS_Release	4/13/2026	Please spell out FedRAMP on first use.	
PTA 05	Data Feed Service, pta_pia_OS_Release	4/13/2026	Please spell out PII and PIA on first use.	
PIA 32D	Data Feed Service, pta_pia_OS_Release	4/13/2026	Please spell out SO and ISSO on first use.	