US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

07/06/2016

OPDIV:

OS

Name:

Commissioned Corps Payroll

PIA Unique Identifier:

P-3698706-967309

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Contractor

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

N/A

Describe the purpose of the system.

The Commissioned Corps Payroll (CCP) system is a secure, web-based system, available only to the Human Recourse and Payroll Technicians at the Commissioned Corp (CC) Headquarters, providing payroll and personnel services for more than 6,700 Commissioned Corps Active Duty Officers. CCP 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 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 system generates the Commissioned Corps 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. (note: It is now Oracle 11G version of the database)

The COPS10GDB system then takes the transaction files from CCP and formats the data, and then transmits the data to both the Treasury for Electronic Funds Transfer (EFT) payments, and to the Thrift Savings Plan (TSP).

Describe the type of information the system will collect, maintain (store), or share.

CCP will collect, maintain, store, and/or share the following information:

1) HHS staff who are Human Recourse (HR) and payroll technicians, direct contractors, and contractors – have minimal PII stored on the system (SSNs, emails, phone numbers, and names). The names, email addresses and passwords are used as login credentials to access the system.

2) The CCP system provides payroll and personnel services for more than 6,700 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 an 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 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 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.

This is a function that the Contractor is responsible for. The Division of 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.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

CCP is a web-based system that provides payroll and personal services for the 6700+ Commissioned Corps Active Duty 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).

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Social Security Number

Date of Birth

Name

E-Mail Address

Mailing Address

Phone Numbers

Financial Accounts Info

Education Records

Military Status

Employment Status

Unique serial number called SERNO

Marital status

Gender

User Credentials (name, email address, password)

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees

Vendor/Suppliers/Contractors

CC officers - for whom payroll services are provided

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

PII is primarily used for:

1) CC officers and others for providing full pay and personnel services.

2) 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 (2 and 3), is only for the user access to the system.

The primary use for the PII collected on the Commissioned Officers (1) is for running HR and Payroll operations, and providing a monthly payroll.

Describe the secondary uses for which the PII will be used.

There are no secondary uses of the PII contained in CCP.

Describe the function of the SSN.

The SSN is used in support of the legacy Commissioned Corps personnel and payroll system, it's data and reporting requirements. The SSN has been encrypted in the legacy reporting database.

Cite the legal authority to use the SSN.

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.

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.

Also: 5 U.S.C. 1302, 2951, 4118, 4308, 4506, 7501, 7511, 7521 and Executive Order 10561.

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

09-40-0006 Pub. Health Service CCP Records

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Hardcopy

Email

Government Sources

Within OpDiv

Other HHS OpDiv

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

Office of Management & Budget (OMB) No. 0937-0025
Expiration: 11/30/2016

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Within HHS

The PII of contractors and HHS staff is not disclosed. The PII information on the CC officers is shared only as part of payroll processing. Human Resources and the Commissioned Corps compensation branch have access to the information. Payroll data is sent to COPS10GDB.

Private Sector

The purpose of disclosure is to perform system administration duties.

Describe any agreements in place that authorizes the information sharing or disclosure.

When the Applicant fills out the PHS-50 document and signs it, the applicant is acknowledging and providing permission for the sharing of their PII data as necessary for the Military personnel and Payroll systems.

Contractors are working on behalf of Office of the Secretary (OS) and access the PII as part of their roles and responsibilities.

Describe the procedures for accounting for disclosures.

Disclosures from this system are unlikely to be made, except in furtherance of the primary purpose of the system. If any nonstandard disclosures were to be made for any unanticipated reason, such that the disclosure was not a routine use, the system owner would maintain a record in a designated file.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the 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 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 (on page 6) 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 collects 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", "HHS/PSC/HRS." 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 Division of Commissioned Corps Personnel and Readiness, ATTN: Records Manager, Suite 100, 1101 Wootton Parkway, Rockville, MD 20852 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.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

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.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

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, including providing notices on physical pay stubs and using e-mail listservs.

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.

Individuals that suspect their information has been misused can contact the Commissioned Corps' Help Desk via a dedicated email account, cchelpdesk@psc.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 HHS-wide and consistent with federal requirements.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

On a monthly basis, the Compensation Branch reconciles payroll against transactions and the Commissioned Corps Systems Branch 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 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 Commissioned Corps Payroll system with the new data.

Identify who will have access to the PII in the system and the reason why they require access.

Users:
Operation and maintenance

Administrators:
Operation and maintenance

Developers:
Operation and maintenance

Contractors:
Operation and maintenance

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.
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.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.
Access levels are provided and restricted based on the user's role and responsibilities.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.
The HHS Office of the Secretary complies with the Federal Information Security Management Act's (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
Privacy Awareness Training

Describe training system users receive (above and beyond general security and privacy awareness training).
A quarterly CCP 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.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?
Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.
Information is maintained in the system as long as it is needed for servicing pay and personnel actions. When officers retire or separate from duty, the records are marked with the appropriate status, removed from the active duty status, and then archived. The information is not destroyed.

NARA retention schedule(s) are being determined and information will be maintained until that occurs.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Administrative: All requests for user accounts in the system must be justified by the user's supervisor and approved by the system owner. Each Officer's data is maintained and monitored by the officer. Signed Rules of Behavior forms collected from the users on a regular basis. Sign-in log for the server room.

Technical: Accounts are individual, with user names and complex passwords. Role based access to data. Data servers protected by firewalls. Audit tables.

Physical: Building has controlled access, which includes Guards, metal detectors, ID-based access. Server room access controlled by key card and cipher lock.