Privacy Impact Assessment
for

Direct Access

DHS/USCG/PIA-024

November 9, 2016

Contact Point
Michael Fijalka
Commandant (CG-631)
HR Systems Management Division
United States Coast Guard (USCG)
202-475-3678

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

Direct Access is the primary system for Human Resources and payroll for over 50,000 Department of Homeland Security, United States Coast Guard, Department of Health and Human Services, United States Public Health Service, and Department of Commerce, National Oceanic and Atmospheric Administration active duty and reserve personnel. It also provides human resources and pay support to a customer base of approximately 68,000 U.S. Coast Guard, Public Health Service, and National Oceanic and Atmospheric Administration retirees, annuitants and Former Spouse Protection Act recipients, while providing non-pay customer service support to an additional 2,500 personnel.

Overview

The United States Coast Guard (USCG) Direct Access system is a full-lifecycle military Human Resources (HR) and payroll solution using commercial/government off-the-shelf products from Oracle and PeopleSoft. It is internet-accessible and web-based, providing USCG-wide access. Direct Access is the primary system for HR and payroll for over 50,000 USCG, Department of Health and Human Services, United States Public Health Service (USPHS), and Department of Commerce, National Oceanic and Atmospheric Administration (NOAA) active duty and reserve personnel. It also provides HR and pay support to a customer base of approximately 68,000 USCG, PHS, and NOAA retirees, annuitants and Former Spouse Protection Act (FSPA) recipients[1], while providing non-pay customer service support to an additional 2,500 personnel.

The purpose of the United States Coast Guard Direct Access system is to provide full lifecycle HR and payroll support (*i.e.*, recruiting through death) for active duty, reserve, and retired active duty and retired reserve personnel.[2]

Direct Access:

- provides military assignment processing;
- aids in the management of personnel housing and occupancy;
- posts official positions of the USCG;
- supports recruitment and accession processes;
- schedules training, manages personnel assets and readiness;

[1] Pub. L. 97-252 (96 Stat. 718, 1982, codified at 10 U.S.C. § 1408 et seq.).
[2] Direct Access is required to meet personnel tracking requirements and military payroll requirements documented predominately in Titles 10 and 14 of the U.S. Code.

- processes promotions and disciplinary actions;
- maintains all personnel attributes (personal identifiers such as name, address, etc.);
- tracks and processes retirements; and
- provides military payroll.

The USCG may also use the data collected for accountability and assessment reporting exercises, and the system is also used to administer USCG civilian personnel and USCG auxiliary members formal USCG training course management; maintain security clearance data, competency, and accomplishment data; as well as track housing; information technology (IT) training; and IT system accounts, roles, and permissions for military, civilian, and contractor personnel. The system is used to provide necessary information to: the Department of Commerce for NOAA Officers; and to the Department of Health and Human Services for Officers of the Commissioned Corps of the PHS to administer their respective pay and personnel/HR management.

Information is entered by Direct Access end users (*i.e.*, individuals who have an approved login account and associated privileges and access within the system) and information is also received via encrypted data feeds from the Department of Veterans Affairs (VA), Department of Treasury (IRS), Defense Manpower Data Center (DMDC), and third-party benefits providers for military employees. Interfaces from these external entities is not received for applicant information. Applicants do not have a login/password access to Direct Access. Attachment A presents detailed descriptions of the Direct Access Roles and Attachment C presents details regarding Responsibilities.

DHS/USCG-014, titled Military Pay and Personnel System of Records Notice (SORN)[3] delineates the external sharing allowed under Direct Access. The main privacy risk associated with Direct Access is the improper handling or use of Personally Identifiable Information. Access to Personally Identifiable Information from the general public (*i.e.*, applicants) such as name, address, and phone number is prohibited since members of the public do not have accounts in the system. Access to this PII is limited to users with a need to know and is considered for official use only. Individuals who require access to organizational information and information systems must complete appropriate access agreements (*e.g.*, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements) before authorizing access, which help mitigate improper handling of PII.

[3] DHS/USCG-014 - Military Pay and Personnel, 76 FR 66933 (October 28, 2011).

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

10 U.S.C. 503; 1043; 1147 and 14 U.S.C. 92(I) 92(r); 93(g); 350-373; 475; 512; 620; 632; 645; 681; 687. In addition, further authority is provided in 5 U.S.C. 301; 5 U.S.C. 5501-5597; 37 U.S.C. 406; 42 U.S.C. 213; 253; 49 CFR 1.45, 1.46; and COMDTINST M1100.2F, Coast Guard Recruiting Manual.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

DHS/USCG-014 Military Pay and Personnel System of Records Notice covers the information retained by Direct Access.[4]

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes, Direct Access has a three (3) year Authority to Operate (ATO) dated September 10, 2013. It completed the Security Assessment Process (SAP) in early September 2015, underwent a subsequent SAP in the summer of 2016, and a new 3 year ATO will be issued once this PIA is approved by the DHS Privacy Office. Direct Access has a FIPS 199 categorization of Moderate-Moderate-Moderate and its Systems Security Plan (SSP) underwent an annual review and is dated July 2016.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

No, a Request for Records Disposition Authority (SF-115) has been completed and submitted to NARA on September 11, 2015, and is pending approval.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

There is only one official form covered by the PRA and an OMB Control number has not been issued as of the date of this PIA. As part of this proposed collection, the system only collects information from potential applicants via the GOCOASTGUARD.COM website in order for the applicant to begin the screening and qualification process.

[4] DHS/USCG-014 Military Pay and Personnel, 76 FR 66933 (October 28, 2011).

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

Direct Access collects information from active service applicants, reserve service applicants, prospective applicants, civilian personnel, active duty, reserve, retired active duty, retired reserve USCG military personnel (and their annuitants and dependents), separated military personnel, USCG auxiliary members, USCG exchange workers, and contractor personnel. Also included are active duty and retired NOAA Officers and their annuitants and dependents, as well as Officers of the Commissioned Corps of the USPHS, their annuitants and dependents, and their civilian supervisors.

Direct Access collects and processes the following information for applicants (who may be members of the public):

- Name;
- Phone number and e-mail address;
- Address;
- Interests;
- Physical Characteristics;
- Date of birth;
- Marital Status and number of dependents;
- Education;
- Citizenship;
- Prior Service Information;
- Minority designation and nationality;
- Background investigation and security clearance-related information;
- Limited medical-related information;

Direct Access may collect, generate, or process the following information for non-applicants (*e.g.*, civilian personnel, active duty, reserve, retired active duty, retired reserve USCG

military personnel (and their annuitants and dependents), separated military personnel, USCG auxiliary members, USCG exchange workers, and contractor personnel). Also included are active duty and retired NOAA Officers and their annuitants and dependents, as well as Officers of the Commissioned Corps of the USPHS, their annuitants and dependents, and their civilian supervisors):

- Name;
- Social Security number (SSN);
- Employee identification number (EMPLID);
- Electronic Data Interchange Personal Identifier (EDIPI);
- Date and place of birth;
- Gender;
- Minority designation and nationality;
- Marital status;
- Limited medical related information to include dates of physical examinations, color blindness, immunizations, weight, and body mass index (and compliance to standards);
- Other Health Insurance Portability and Accountability Act (HIPAA) related/protected data;[5]
- Addresses;
- Phone number and e-mail address;
- Total current monetary earnings, including overtime, computed to the nearest dollar;
- Number of hours worked;
- Leave accrual rate;
- Leave requests and balances;
- Health and life insurance requests and eligibility;
- Payroll deduction requests;
- Information for the purpose of validating legal requirements for garnishment of wages;
- Salary rate;

[5] Pub. L. 104-191 (110 Stat. 1936, 1996, codified at 42 U.S.C. § 1320d); see generally 45 CFR Part 160, 164 subparts A and E.

- Cash awards;
- Retirement withholdings;
- Background information to include work experience;
- Education records, including: highest level achieved; specialized education or training obtained in and outside of military service; non-traditional education support records; achievement and aptitude test results; academic performance records; correspondence course rate advancement records; military performance records; admissions processing records; grade reporting records; academic status records; and transcript maintenance records;
- Military duty assignments;
- Ranks held;
- Allowances;
- Personnel actions such as promotions, demotions, or separations;
- Record of instances of Uniform Code of Military Justice infractions;
- Performance evaluations;
- Background investigation, and security clearance information;
- Government credit card status;
- Individual's desires for future assignments, training requested, and notations by assignment officers;
- Information for determinations of waivers and remissions of indebtedness to the U.S. Government;
- Travel claims, transportation claims, Government bills of lading, and applications for shipment of household effects;
- USCG housing records, including: housing surveys, computer data summaries, and correspondence from the individual seeking housing;
- Information regarding IT training, IT system accounts, roles, permissions;
- Names, dates of birth, addresses, SSNs, and gender of annuitants and dependents of active duty, reserve, and retired active duty and reserve military and uniformed members; and

- Total current monetary earnings, including overtime, computed to the nearest dollar – calculated by the application based upon configuration of payroll rules to include eligibility, effective pay rate, hours worked, etc.

2.2 What are the sources of the information and how is the information collected for the project?

Information is entered by Direct Access end users (*i.e.*, individuals who have an approved login account and associated roles and privileges and access within the system which are presented in *Attachment B Direct Access Application and Database Roles*). Information is also received via encrypted data feeds from the Department of Veterans Affairs (VA), Department of the Treasury (IRS), Defense Manpower Data Center (DMDC), and third-party benefits providers for military employees. The inbound data for the below organizations is not received for applicants, these inbound data feeds are for "employees" only.

The shared information consists of the following external data feeds:

Veteran's Affairs (VA): Salary offset amounts for disability and other information needed to determine eligibility for other earnings.

- U.S. Department of the Treasury (IRS): Account number and amount to support distribution of payee net, allotment recipients, tax payments, and bond purchases.
- Defense Manpower Data Center (DMDC): Demographic data on payees such as electronic data interchange personal identifier (EDIPI), gender, age, marital status, and home address (city and state).
- Third-Party Benefits Providers: Participant information such as start date, stop date, change date, and premiums paid.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No, the system does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

Direct Access uses commercial/government off-the-shelf products from Oracle and PeopleSoft that have built in integrity controls that are used at time of input (*e.g.*, validation of screen entry fields when the data is entered), during processing (*e.g.*, codified business rules are executed by the system when the data is being processed), and post processing (*e.g.*, reconciliation reports can be run to verify any changes to the data). End user self-service

accounts allow users to correct their personal information (*e.g.*, mailing address, phone number). The underlying Oracle database also has implemented numerous database controls to prevent unauthorized changes to the data stored in the database (*i.e.*, database integrity controls). Information within the system is also checked for consistency and accuracy against the external feeds from the Department of Veterans Affairs (VA), Department of Treasury (IRS), Defense Manpower Data Center (DMDC), and third-party benefits providers for military employee data.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that applicant information is not accurate, complete, and current.

Mitigation: GOCOASTGUARD.COM collects the applicant information directly from the individual. The applicant confirms this information before it is officially submitted to the Coast Guard. The applicant data is transmitted via a secure encrypted feed into Direct Access without other Coast Guard or external user intervention. It is an automated process with no public (applicant) user login to Direct Access. The applicant may also change the information after submission by contacting a Coast Guard recruiter or filing a request under the Privacy Act to amend her or his responsive record. Coast Guard also verifies the applicant information during the subsequent recruiting process.

Privacy Risk: There is a privacy risk that information received from partner agencies may not be accurate.

Mitigation: The information received from external partners, the IRS, VA, and DMDC, is from Privacy Act systems of records covering the respective source data compiled by those agencies. As such the requirements for data integrity, security, and accountability imposed upon DHS systems of records by the Privacy Act are also required to be met by systems of records for these partner federal agencies. Similarly, should a Direct Access user identify inaccuracies in their data, they may seek redress to correct their information through a Privacy Act access and amendment request as cited in Sections 7.1 and 7.2 of this PIA; additionally, users may submit Privacy Act access and amendment requests to the IRS, VA, or DMDC to address inaccurate information maintained in those agencies respective systems.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

The system collects and manages the data elements presented in Section 2.1 to support full lifecycle HR and payroll processing. Direct Access reporting and analysis products containing PII are based on documented USCG requirements, USCG reporting policies, and DHS and congressional inquiries. SSNs are used within the system for employee, retiree, and annuitant payroll processing, leave approvals by supervisors, and for the purposes of transmission of payment information to federal and state taxing authorities. SSNs are sent to DMDC and VA in accordance with existing laws and instructions governing the sharing of military employee data. SSNs are also used during the hiring and screening processes for applicants and potential applicants to determine citizenship status as well as during background investigation screenings. Use of SSN for citizenship verification is a manual external process performed by Coast Guard military recruiters during the applicant review and processing step. There are no interfaces from Direct Access to other DHS systems that use SSN to verify citizenship.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

3.3 Are there other components with assigned roles and responsibilities within the system?

No.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that users with elevated roles/permissions could exceed their authority and access or use data for unofficial purposes.

Mitigation: The accounts of users with elevated roles/permissions are reviewed under the direction of the Direct Access security administrators on an annual basis as part of the account recertification process. Whenever a user has a change of employment status (*e.g.*, position change, transfer) all of the roles are revoked and a new set of roles associated with the changed status are applied. Finally, all of the roles in the system are reviewed on an annual basis to ensure that the roles are limited to those functions required for the specific job function associated with each role.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

A Privacy Act Notice is displayed on the login page of Direct Access and applies throughout the user's entire session. The GOCOASTGUARD.COM web site displays a similar Privacy Act Notice to a potential applicant who might enter information into the applicant page (see http://www.gocoastguard.com/privacy-policy). USCG also provides notice through the publication of this PIA and the DHS/USCG-014 Military Pay and Personnel SORN.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

There are two categories of individuals: those with an approved user account with information in Direct Access and a potential applicant using the GOCOASTGUARD.COM web site. For Direct Access users, individuals do not have the opportunity to consent to particular uses of the information they provide nor can they withhold a specific portion of the information. Information in Direct Access is used in accordance with Titles 10 and 14 of the U.S. Code, USCG personnel and pay policy, which covers members of the uniformed services including PHS and NOAA uniformed services. If a member of the public voluntarily submits applicant information during the recruitment process via GOCOASTGUARD.COM and declines to provide the required information, the application is considered incomplete and the applicant is dropped from consideration. The required fields are clearly stated on the applicant page "*Please note: all fields are required unless marked "optional".*"

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Potential applicants may be unaware that Direct Access is collecting and using their data.

Mitigation: Direct Access only collects information from potential applicants via the GOCOASTGUARD.COM website in order for the applicant to begin the screening and qualification process. The GOCOASTGUARD.COM web site displays a Privacy Act Notice to potential applicants who might enter information into the applicant page (see http://www.gocoastguard.com/privacy-policy). As noted in the Privacy Act Statement, submission of this data is voluntary for applicants, however should the applicant decline to

submit the required information, the application is considered incomplete and the applicant will be dropped from consideration. The required fields are clearly stated on the applicant page "*Please note: all fields are required unless marked "optional".*" USCG also provides notice through the publication of this PIA and the DHS/USCG-014 Military Pay and Personnel SORN.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

Direct Access follows the Information Life Cycle and Management Manual, COMDTINST M5212.12 (series), Standard Subject Identification Code (SSIC) 1070, Item 1, and SSIC 1100 as described below:

The Official Military Personnel File (OMPF) record documents the career of each officer and enlisted member of the military (including civilian personnel or contractual groups who were later accorded military status under the provisions of Public Law 95-202 (*see* 38 U.S.C. § 1682 et seq.)) from time of entry into service until final separation. During service (active, guard, or reserve) these records are used by the Coast Guard to manage the member's assignment, training, advancement, and separation. After the OMPF record becomes inactive at the completion of the service member's obligated service, they are retained for a period of 62 years and are used for a variety of purposes, but primarily to protect the legal and financial rights of veterans, their families and survivors, and the U.S. Government. Depending on the period of service, OMPF records of officers and enlisted military service members are maintained in three different formats: paper, microfiche, and digital (including images). Current active, reserve, or guard OMPF records are maintained in Direct Access.

The Individual Personnel Applicant Record documents an applicant's initial screening information. An applicant is a person who expresses a desire to join the Coast Guard by completing and signing a USMEPCOM Form 680-3A-E. An Applicant Record provides the qualifications, medical, Delayed Entry Program (DEP), and accession data of an applicant. Records are retained for a period of 12 years after submission of the application and are used for tracking purposes and coordination with recruiting efforts by the other U.S. Military branches. Information on selected applicants (those who accessed) is forwarded for inclusion in an OMPF record.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: USCG may retain data in Direct Access for longer than is necessary to perform mission functions.

Mitigation: Ownership of paper, microfiche, and/or electronic OMPF records will transfer in blocks to the National Archives for permanent retention in accordance with the pending NARA retention schedules:

- 62 years after the date of retirement to the storage facility of the newest record within the block. Applicable to pre-Registry blocks.
- 62 years after the date of OMPF record retirement to the storage facility. Such ownership transfers to the National Archives will be accomplished in annual increments and are applicable to Registry blocks maintained at NPRC.
- 62 years after the completion of service member's obligated service. Such ownership transfers will be accomplished in annual increments and are applicable to OMPF records in electronic format.

Individual Personnel Applicant records will transfer in blocks to the National Archives for permanent retention in accordance with the pending NARA retention schedule:

- 12 years after the date of record retirement to the storage facility. Such ownership transfers to the National Archives will be accomplished in annual increments.

Information on selected applicants (those who accessed) is forwarded for inclusion in OMPF.

Privacy Risk: There is a risk that users may not follow the retention schedules because they require manual action.

Mitigation: This risk is partially mitigated. Direct Access does not automatically transfer or purge data, so USCG staff must manually move data in order to adhere to retention schedule requirements. To ensure that this process is maintained, USCG has written rules for manually moving PII contained in the Information Life Cycle and Management Manual, COMDTINST M5212.12 (series). Additionally, users are trained to follow the retention schedules.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Yes, Direct Access shares Military employee data externally with other federal agencies, state agencies, and insurance companies, in order to support full lifecycle HR and payroll processing as required by Title 10 and Title 14 of the U.S. Code and USCG personnel and pay policy. Direct Access shares with:

- Department of Commerce (DOC) for NOAA Officers and the Department of Health and Human Services (HHS) for Officers of the Commissioned Corps of the USPHS to administer their respective pay and personnel/HR management.
- USDA National Finance Center
- Veteran's Affairs
- U.S. Department of the Treasury / IRS
- Defense Manpower Data Center (DMDC), and
- Federal Retirement Thrift Investment Board (FRTIB).

The shared information consists of the following subject matter:

- **USDA National Finance Center:** HR and payroll information
- **Veteran's Affairs (VA):** Salary offset amounts for disability and other information needed to determine eligibility for other earnings.
- **U.S. Department of the Treasury:** Account number and amount to support distribution of payee net, allotment recipients, tax payments, and bond purchases.
- **Defense Manpower Data Center (DMDC):** Demographic data such as gender, age, marital status, home address (city and state), and other readiness information.
- **Third-Party Benefit Providers:** Participant information such as start, stop, change, and premiums paid.
- **USPHS:** Billet data, license data, awards data, applicant data, administrative code data, course information data, and fitness and medical data.
- **FRTIB:** USCG and NOAA (and eventually PHS military member) TSP contribution and loan payment data.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The information contained in Direct Access as described above may be shared with entities outside of DHS in support of the requirements associated with full lifecycle HR/ Payroll processing and is compatible with the SORN which allows:

- DOC and HHS in order to administer their respective pay and personnel systems for NOAA Officers and Officers of the Commissioned Corps of the PHS, respectively.
- DoD and VA for determinations of benefit eligibility for military members and their dependents.
- Department of the Treasury (DOT) for the purpose of disbursement of salary, U.S. Savings Bonds, allotments, or travel claim payments.
- Appropriate insurance agencies/companies for the purpose of health and life insurance requests and eligibility.
- Federal, state, and local government agencies to disclose earnings and tax information, including the IRS and the Social Security Administration (SSA), as required by law.
- DoD for manpower and readiness planning (including preparing for and during actual emergencies, exercises or COOP tests for the purpose of responding to emergency situations, or to allow emergency service), and preparing the Register of Officers and Register of Reserve Officers, which is provided to all USCG officers.

6.3 Does the project place limitations on re-dissemination?

Yes, all external sharing agreements are governed by a memorandum of understanding (MOU), memorandum of agreement (MOA), public law/regulation, or other contractual arrangement, which have strict data usage and dissemination clauses protecting any transferred information. These agreements are reviewed as part of the system's security accreditation process (SAP), with the most recent being completed in September 2015. External agencies are prohibited from sharing the information provided by the USCG unless the MOA, MOU, public law /regulation, or other contractual arrangement specifies that they are allowed to share this information.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Any organization disclosing the information records the disclosures manually. Depending upon the type and scope of disclosure, application and/or database audit logs may also capture the disclosure event, such as a change request for a specific data query. All requests

for data access are managed through the Program Sponsor's Office, CG-1, based on Congressional, Government Accountability Office (GAO), Office of Personnel Management (OPM), Office of Management and Budget (OMB), Freedom of Information Act (FOIA), or servicing agency (USPHS and NOAA) requests.

Records released through FOIA are tracked by the USCG Management Programs and Policy Division, Commandant (CG-611) STOP 7710, 2703 Martin Luther King Jr. Avenue SE, Washington D.C. 20593.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: The primary risk in collecting and storing PII is the possibility of information being improperly accessed, used, or externally shared beyond the reason for which it was collected.

Mitigation: In addition to MOUs/MOAs/ISAs, Direct Access mitigates these risks through internal and external controls. Internally, Direct Access uses a role-based security model for both the application and the underlying database. This security employs logical access controls that are codified based upon business processes to allow users access to only those functions and information required for their official duties. Externally, Direct Access protects against the unauthorized access of information by employing confidentiality controls, such as data encryption, for the protection of data in transit and at rest. Finally, Direct Access has the capability of generating audit trails to assist in identifying any misuse of the system.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

Individuals seeking notification and access to any record contained in Direct Access, or seeking to contest its content, may submit a Privacy Act access request in writing to COMMANDANT (CG-611), 2703 Martin Luther King Jr. Avenue SE, STOP 7710, ATTN: FOIA Coordinator, Washington, D.C. 20593-7710. A request may also be submitted to EFOIA@uscg.mil.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Members of the public (*i.e.*, applicants) may seek to correct their information through a Privacy Act request as cited in Section 7.1 above. For Direct Access end users with accounts in the system, the easiest method for accessing and correcting their records is by using the self-service function, contacting the help desk, or direct interaction with a Coast Guard Personnel Servicing Office; individuals may also formally request access or correction by making a Privacy Act request.

7.3 How does the project notify individuals about the procedures for correcting their information?

Formal notice is given to the individual through the publication of this PIA and the DHS/USCG-014 Military Pay and Personnel SORN.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not be able to correct or access their records.

Mitigation: Members of the public (*i.e.*, applicants who are not end users of the system) can correct their information through a Privacy Act request as cited in Section 7.1 above. Direct Access end users (*i.e.*, individuals who have an approved login account and associated privileges and access within the system) can access and correct those portions of their HR data allowed through self service permissions by using the self-service function, contacting the help desk and submitting a service request ticket to correct data, or direct interaction with a Coast Guard Personnel Servicing Office; individuals may also formally request access or correction by making a Privacy Act request.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

Direct Access employs a defense in-depth security strategy to better ensure the information is used in accordance with stated practices in this PIA. Roles are mapped to positions and provide a least-privilege approach to access. The default role is self service, in

which an individual can only access and modify his/her own records. Other roles must be requested and approved and recertified on a regular basis by the respective business process owner. A privileged user program is in place and followed. Overlapping role-based access controls at the web interface, application, and database levels restrict access to information based upon an individual's role/position within the organization. Automated audit logging and analysis is performed at the application, database, and operating systems and is used for after the fact event/violation analysis.

Direct Access is a Chief Financial Officer (CFO)-designated system in addition to being a privacy designated system. As a result, it undergoes a Chief Information Security Officer (CISO) required annual security control self-assessment, annual internal controls assessment by the USCG CFO's Office, and an annual integrated financial audit by the DHS Office of the Inspector General (OIG). Since Direct Access provides services to entities external to Coast Guard, it undergoes an annual Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization audit (SSAE-16). Any findings are documented and mitigation strategies are implemented.

In addition, the PIA and the DHS/USCG-014, titled Military Pay and Personnel SORN are reviewed and updated on a regular basis.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

Direct Access users[6] follow a robust IT security training program. Computer security awareness and training, in various forms, is used to elevate and sustain personnel awareness of proper operational, and security-related risks and procedures. Security training encompasses instruction on individual responsibilities under the Privacy Act of 1974 and specific guidance is provided to personnel who design, implement, use, or maintain Direct Access resources. Training also includes annual instruction on personal duties and responsibilities under the privacy and security provisions of HIPAA.

Furthermore, Direct Access users are trained that appropriate administrative action consistent with their respective organization's policies will be taken against individuals found responsible for unauthorized disclosure of information in violation of Privacy Act and/or HIPAA provisions. Individuals found responsible for unauthorized disclosure of sensitive information protected under the Privacy Act of 1974 and HIPAA may be faced with civil and/or criminal action.

[6] This training is not required for Retirees or Annuitants since they can only use self service functionality nor is it required for potential applicants since they do not have accounts in the system.

DHS USCG, NOAA, and USPHS users receive annual privacy and security training from their respective organizations. These organizations track and report on training compliance through their respective training management systems (*e.g.*, the USCG Learning Management System (LMS)). Tracking includes the role-based training programs conducted for contractors and privileged users.

All USCG personnel must complete annual mandated trainings titled, *DHS Protecting Personal Information and DHS Records Management for Everyone*.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Direct Access's access control policies (*e.g.*, identity-based, role-based, and business rule-based policies) and associated access enforcement mechanisms (*e.g.*, access control lists) are employed by Direct Access to control access between users (or processes acting on behalf of users) and objects (*e.g.*, devices, files, records, processes, programs, domains) in the information system. Access to the security aspects of the operating system, database, and application is restricted to trusted administrators (*i.e.*, privileged users) who have received additional security training and have signed Non-Disclosure Agreements (NDA). End-users do not have access to the security portions of the system. Access levels are designated based on roles and privileges. Direct Access accounts are role-based accounts. Permissions are granted to roles and not to individual user accounts. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security.

For Coast Guard active duty and reserve employees, the user account is automatically created as part of the hire process within Direct Access. The initial account is created and assigned the Member Self Service role only. No user access is required for creation of this account or assignment of the role - read-only access accounts for self-service activities are automatically granted upon joining the Coast Guard.

For civilian employees, the user account is automatically created as part of the hire process. The initial account is created and assigned the "Civilian Self Service" role only. No user access is required for creation of this account or assignment of the role.

Non-Coast Guard employees/user accounts are created manually using the process described below:

- The user initiates the Direct Access User Access Authorization/Revocation process.
- Supplied information is reviewed and acted on (approved/disapproved) by the Chief, Retiree and Annuitant Services Branch, Chief, Military Accounts Support Branch, PPC

Topeka, or Government employee assigned to the Human Resource Management Systems Division.

- If approved, the Direct Access Security Administrator is then contacted via email by the Chief, Retiree and Annuitant Services Branch, Chief, Military Accounts Support Branch, PPC Topeka, or Government employee assigned to the Human Resource Management Systems Division, of the accounts to be created and the roles for each account.
- If not approved, the request is deleted and no further processing is performed.
- When completed, the Direct Access security administrator advises the approval authority of the account creation.

The addition of specific roles required to perform specific HR and payroll-related business functions for non-Coast Guard employees / accounts are created / updated manually using the process described above.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Current Direct Access information sharing MOUs / MOAs have been reviewed by the program manager, system owner, counsel, and authorizing official. Any revised MOUs / MOAs will be sent to the USCG Privacy Officer for review.

Responsible Officials

Marilyn Scott-Perez
Chief, Office of Information Management
Commandant (CG-61)
(202) 475-3515

Approval Signature

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security

Attachment A

Direct Access User Roles

Access to Direct Access is limited to greatest extent possible to prevent access to personally identifying information and other sensitive information. To achieve this, many different roles are available for users.

Command User Role

The Command User Role provides the user with the ability to access the Self Service role for Commands functions in Direct Access. It is a powerful, multi-purpose role, intended for use by trusted, mature, and responsible members of the command cadre. Command Users must be designated by the Commanding Officer CO, Officer in Charge (OinC), Executive Officer (XO), or Executive Petty Officer (XPO). The Direct Access command user:

- Schedules reserve Inactive Duty Training (IDT) drills.
- Initiates and views enlisted evaluations.
- Accesses the Airport Terminal, which provides a list of personnel in receipt of orders to or from the unit (both Permanent Change of Station (PCS) and Temporary Duty (TDY) and the ability to view and print travel orders.
- Generates and views member competency reports.
- Prints BAH/Dependency and Emergency Contacts reports.
- Views command information including rosters, absence reports, and personnel allowance lists.
- Views member service record information (USCG Member Info) including assignment history, competencies, training history, contact telephone numbers, and addresses.

Each unit must designate at least one Command User. Additional Command Users are designated based on the need to access the information listed above. Commands can designate as many Command Users as necessary to meet the unit's need and maintain a smooth workflow.

However, designations of Command Users in pay grades E-6 and below are subject to review and approval by Pay and Personnel Center (PPC) and/or Commandant (COMDT) (CG-1). There are alternative access roles available for personnel who do not need access to all of the Command User functions.

Direct Access allows a Command User access to ALL command functions. Any Command User has the ability to enter comments and approve an employee review, enter IDT drills, or view transfer information.

COs/OinCs/XOs/XPOs clearly define an individual's role when making Command User designations.

When considering Command User designations, does the individual need to have the Commands authorization to:

- View enlisted evaluations?
- Initiate enlisted evaluations?
- View pending transfer information?
- Run reports and rosters?
- Input reserve Inactive Duty for Training / Active Duty for Training (IDT/ADT) information?

Granting full command access is not always necessary or appropriate. Granting one or more of the following roles in lieu of full command access may be more appropriate.

Role	Functions	Suggested Users
Airport Terminal Only (CGAIRTRM)	Allows access to the Airport Terminal.	Housing Officers/staffs and Relocation Specialists.
Reserve Orders Manager (CGRSVMGR)	Create, review, and endorse requests for reserve orders.	Allows supervisors to initiate requests for reserve orders on behalf of the member who cannot access Self-Service and allows the user to review and endorse requests for orders.
Human Resource Site View (CGHRSVW)	Allows view only access to Servicing Personnel Office SPO functions.	Pay and Allowance (P&A) Office personnel, unit administration staff. This is a restricted role available only for those needing view access to SPO functions.
Field Admin	User can act as proxy for absence requests (leave), view	Unit administrative staff and

Role	Functions	Suggested Users
(CGFIELDADMIN)	member, run reports, competencies, view Basic Allowance for Housing (BAH) /Dependency Data and Emergency Contact reports, view and print travel orders, and most other non-pay related personnel actions. Enter awards and honors, competencies, and training.	P&A Offices.
Global Workforce Inquiry Solution (CGGWIS)	Allows view-only access to member and unit data. Includes access to Airport Terminal.	HR managers (Command Officer / Officer in Charge)(CO/OinC), Executive Officer / Executive Petty Officer (XO/XPO), Admin Officers, Headquarters / Coast Guard Personnel Services C ommand (HQ/CGPSC) staffs.
Employee Review (CGEMPREV)	Users can initiate, route, and approve enlisted employee reviews.	Supervisors (E-6 and above) and Marking Officials. Note: A user with Command User Role can enter final data entry into Direct Access. It is not necessary for every person in the chain of command to use Direct Access to complete an employee review.

CGHRS Role

The CGHRS role permits a Direct Access user to create transactions that effects changes in a member's pay entitlements. They can also access and maintain non-payroll data, such as competencies, awards, enlisted employee reviews, etc. This role duplicates the Self-Service for

Employees and Self-Service for Commands roles to allow SPO users to service members and commands that do not have access to Direct Access or are administratively limited.

CGHRSUP Role

The CGHRSUP (Supervisor/Auditor) role permits the Direct Access user to approve Direct Access transactions that require approval for payment to the member. CGHRSUP users are also designated as PAOs. Certain Direct Access entitlement transactions require review and approval before they can be released for processing. Authority to approve these transactions is limited to properly designated PAOs. PAOs are assigned the CGHRSUP role in Direct Access.

SPO Staffs

Active duty, reserve, and civilian employees permanently assigned to a position in a SPO can be granted CGHRS or CGHRSUP roles in Direct Access. SPO staff assignments and approval authorities must be documented. SPOs must maintain a "SPO Authorized Personnel Roster" showing the full name, initials, signature (in cursive), their role, and date arrived and departed to the SPO. The roster must be stored locally and continually updated with a historical chronology maintained to substantiate the approval authorities executed by these members.

Attachment B

Direct Access Application / Database Roles

The following is the list of application / database roles that may be assigned to a user.

ROLE NAME	DESCRIPTION
CG_PHYCHR_V	Physical Characteristics View only
CG_ACG_SELF_SERVICE	Member SS access Person Profile
CG_WEIGHIN_V	Employee View of Weigh-In data
CG_HON_AWD_U	Honors and Awards Update
CG_HON_AWD_V	Honors and Awards View
CG_LANG_U	Languages Update
CG_LANG_V	Languages View
CG_LICCERT_U	Licenses and Certifications Update
CG_MEMBERSHIPS_U	Memberships Update
CG_MEMBERSHIPS_V	Memberships View
CG_OSC_U	Officer Specialty Code Update
CG_OSC_V	Officer Specialty Codes View
CG_READINESSROLES_U	Readiness Roles Update
CG_READINESSTEAMS_U	Readiness Teams Update
CG_READINESSTEAMS_V	Readiness Teams View
CG_COMP_V	Competencies View
CG_LICCERT_V	Licenses and Certifications View
CG_ADMINFLAGS_V	Administrative Flags View
CG_BLS_U	Basic Life Support Update
CG_COMP_U	Competencies Update
CG_SWEWAIVERS_U	Servicewide Exam (SWE) Waivers Update
CG_SWEWAIVERS_V	Servicewide Exam (SWE) Waivers View Only
CG_READINESSWAIVERS_U	Readiness Waivers Update
CG_READINESSWAIVERS_V	Readiness Waivers View Only
CG_RESIGWAIVER_U	Resignation Waiver Update
CG_RESIGWAIVER_V	Resignation Waiver View Only
CG_RETIREWAIVER_U	Retirement Waivers Update
CG_RETIREWAIVER_V	Retirement Waivers View Only
CG_PHYCHR_U	Physical Characteristics Update
CG_RSVWAIVERS_U	Reserve Waivers Update
CG_RSVWAIVERS_V	Reserve Waivers View Only
CG_WEIGHIN_U	Weigh-In Update
CG_MEDICALWAIVERS_U	Medical Waivers Update
CG_MEDICALWAIVERS_V	Medical Waivers View Only
CG_EDUC_U	Education (Degrees) Update
CG_EDUC_V	Education (Degrees) View
CG_EMPLRVWWAIVERS_U	Employee Review Waivers Update
CG_EMPLRVWWAIVERS_V	Employee Review Waivers View Only
CG_ADMINFLAGS_U	Administrative Flags Update
CG_ADMINWAIVERS_U	Admin Waivers Update
CG_ADMINWAIVERS_V	Admin Waivers View Only
CG_TESTS_U	Test and Exams update access

ROLE NAME	DESCRIPTION
CG_TESTS_V	Tests and Exams - View only
CG_ADDLTRNG_U	Additional Training - Update
CG_CRSE_V	Courses and Training View only
CG_CRSE_U	Courses and Training
CG_ADDLTRNG_V	Additional Training – View Only

Attachment C

Responsibilities

Seven entities within Direct Access have a responsibility to ensure the system functions properly. These entities interact to perform the personnel and pay functions for the Coast Guard. Below are their responsibilities such as, but not limited to:

Entity	Responsibility
Member	Members are to: • Report changes in mailing address (including allotments), phone numbers, and e-mail addresses. • Understand their Leave and Earnings Statement (referred to as the Payslip) and report any discrepancies via the chain of command. • Understand their Retirement Point Statement (referred to as the Reserve Member Balances) (reservists). • Report changes in family/dependent status. • Report occasions of moving into or out of Government-owned or leased quarters. • Submit changes in allotments or direct deposit in Direct Access. • Advise the Commanding Officer (CO)/Officer in Charge (OinC) of reenlistment/extension intentions. • Submit an E-Resume. • Provide any other personnel data and supporting documentation as requested. • File travel claims for self and dependents, if applicable, within three days of reporting to a new Permanent Duty Station (PDS) or returning from Temporary Duty (TDY). • Maintain a file of historical travel, personnel, and pay transactions. Should a member challenge a travel, pay, or personnel action, the member must produce the necessary documentation to substantiate

Entity	Responsibility
	the member's contention. • Reserves Members – Enter IDT drills and ADT order requests. Submit timely Annual Screening Questionnaires (ASQ).
Unit CO/OinC	Unit CO's/OinC's are to: • Complete Enlisted Employee Reviews (EER) and ensure they are completed on time in accordance with reference (a). • Prepare correspondence for the unit. • Authorize and submit leave authorizations. • Endorse E-Interviews. • Conduct pre-discharge interviews. • Maintain unit Personnel Data Records (PDR) in accordance with reference (b). • Provide data and supporting documentation in support of personnel/pay actions for members in accordance with reference (b). • Conduct annual review of Basic Allowance for Housing (BAH)/Dependency Form and emergency data as prescribed in this publication. • Ensure compliance with Coast Guard weight and body fat standards in accordance with reference (e). • Review orders on the Airport Terminal in Direct Access for attached members. • Review and forward/release travel claims within two days of receipt from member. • Conduct overseas screening for departing members, if applicable. Note: Units with insufficient administrative capability (see "non-administrative shore unit" in Section 7-1-1-c of reference (c)) should seek assistance from their parent command in completing these tasks. In accordance with Section 3-1-7-b of reference (c), the Sector or Group Commander is responsible for providing "support" for the functions

Entity	Responsibility
	performed by assigned subordinate units.
Personnel and Administrative (P&A) Offices	P&A Offices (Admin Offices) are to: • Coordinate and provide expertise in unit administration and personnel actions for active duty, reserve, auxiliary, and civilian members assigned to the unit. • Serve as primary pay, allowances, and benefits counselor for all personnel. • Review, support, and initiate all USCG-mandated pay and/or personnel transactions submitted to the Servicing Personnel Office. • Mail or scan and email any documents authorized by Enclosure (1) of reference (b) for inclusion in the Electronically Imaged Personnel Data Record (EI-PDR) and provide originals to the Servicing Personnel Office. • Manage Temporary and Permanent Change of Station orders for all personnel. • Act as Common Access Card (CAC) issuing authority; perform CAC pin resets. • Provide Defense Enrollment Eligibility Reporting System/Real-Time Automated Personnel Identification System DEERS/RAPIDS services and ID card services to eligible personnel. • Provide travel and transportation administrative support and counseling, including assistance with travel claim submission for the unit and supported units. • Act as Direct Access coordinator for the unit and supported units. • Oversee and promote unit training and personnel development programs including administration of unit Mandatory Training program. • On a collateral duty basis, when no full-time Educational Services Officer (ESO) is assigned or in support of full-time ESO, manage and oversee delivery of ESO services, including processing tuition assistance, administration of voluntary education testing programs

Entity	Responsibility
	(College-Level Examination Program (CLEP), Armed Services Vocational Aptitude Battery (ASVAB), College exam, Dantes Subject Standardized Test (DSST), etc.), managing and processing end of course and correspondence tests, processing Coast Guard Foundation/Mutual Assistance educational grants and loans, processing Educational Assessment requests; and facilitating and supporting educational achievement through voluntary education. • Act as ADT orders-issuing authority as directed by the appropriate level staff. Provide administrative services by coordinating Reserve mobilization administrative support, and the documentation of reserve drills. Maintain file copies of all original signed reserve orders issued to Sector reservists. • Serve as Decedent Affairs Officer (DAO) within Area of Responsibility (AOR). Oversee and coordinate all USCG funeral actions, including Burials at Sea, per the Military Funeral Honors (MFH) program. Maintain Military Funeral Honors Database. • Provide Casualty Assistance Calls Officer (CACO) guidance and support in AOR when responding to a death in the line of duty. Providing training to CACOs. • Manage and oversee the urinalysis and weight standards program for unit and supported units. • Manage and oversee the Government Travel Charge Card (GTCC) program for the unit and supported units; assist units with GTCC issues. Issue funds advances, as appropriate. • Manage and oversee the Mass Transit benefit program for the unit and supported units. • Oversee financial assistance and grants management including Coast Guard Foundation (CGFDN) Grant applications and Mutual Assistance (CGMA) loans or grants. • Serve as the Passport Acceptance Agent (PAA) for the unit and supported units. • Manage and oversees entry approval.

Entity	Responsibility
	• Oversee workforce good order and discipline by coordinating administration of military justice processes. • Manage unit directives program including award preparation, filing, and completing Direct Access personnel transaction entries. • Manage unit directives program including maintenance of unit directives library and promulgation of unit-generated directives. • Provide other personnel services as required by current directives. • Liaison with Servicing Personnel Office organization.
Servicing Personnel Office	Servicing Personnel Offices (SPOs) provide support to COs/OinCs by recording complex pay and personnel events in Direct Access. Even though the SPO has responsibility for DA data entry, the unit CO/OinC is not relieved of authority or responsibility for personnel management functions. The event that results in the generation of Direct Access transactions must still originate at the member's parent unit and must be accurately communicated to the SPO through the P&A Office staff. SPO members that are designated Payment Approving Officials (PAOs) in accordance with (d), certify transactions for payment by the Authorized Certifying Officer (ACO) at PPC. SPOs are to: • Oversee the responsibilities of Military Pay management ensuring all pay and personnel policies and procedures outlined in service directives are properly followed. • Carry out auditor responsibilities of a Payment Approving Official as required by reference (d). • Ensure all Direct Access transactions affecting military pay and allowances (including, but not limited to, enlistments, retirements, discharges, and separations) are first supported by required documentation as outlined in service directives, the transactions are entered accurately, and processed within prescribed timelines. • Process all pay and personnel transactions for active duty and reserve permanent change of station (PCS) orders. • Process and pay and personnel transactions for Reserve recall for

Entity	Responsibility
	mobilization and Reserve mobilization(s) including continuance of Reservists on Active Duty. • Prepare and process appropriate documentation as required for administrative and disciplinary actions. • Maintain and process SPO PDRs, in accordance with reference (b), to manage the day to day activities and transactions, to support members' military payroll and benefits in Direct Access, and to conduct and respond to personnel review and financial audits. • Main or scan and email any documents authorized by reference (b) for the EI-PDR. • Liaison with the Personnel Services organization.
Pay & Personnel Center Topeka	PPC will: • Provide feedback to SPOs when transactions are correctable. • Take corrective action on errors which cannot be corrected by SPOs. • Provide written notice of due process rights to members who are overpaid. • Provide timely and accurate personnel and pay service to all members of the Coast Guard. • Administer leave and retirement point accounting for active and reserve military personnel. • Arrange for settlement of claims on behalf of deceased or separated members and collect out of service debts. • Process application for allotments and garnishments for certain support obligations as set forth in 5 CFR 581, 32 CFR 63 and 33 CFR 50. • Administer the Servicewide Examination (SWE) program and provide enlisted advancement lists to CG Personnel Service Center (PSC) for official issuance. • Develop procedures to support all areas of personnel and pay policy. • Process travel claims. • The ACO at PPC certifies transactions/vouchers prior to release of funds by the U.S. Treasury.

Entity	Responsibility
Coast Guard Personnel Service Center (CG PSC)	CG PSC: • Issues normal promotion/advancement authorizations and eligibility lists. • Approves retirements. • Considers all personnel waivers. • Issues assignment orders.
CG Institute	CG Institute: • Distributes and scores all U.S. Coast Guard correspondence courses. • Distributes educational funding. • Conducts military education credit evaluation.

References:

(a) Enlisted Accessions, Evaluations, and Advancements, COMDTINST M1000.2 (series)
(b) Military Personnel Data Records (PDR) System, COMDTINST M1080.10 (series)
(c) United States Coast Guard Regulations 1992, M5000.3 (series)
(d) U.S. Coast Guard Certifying and Disbursing Manual, COMDTINST M7210.1 (series)
(e) Coast Guard Weight and Body Fat Standards Program, COMDTINST M1020.8 (series)