



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Central Registry/Digital Time Card (CR/DTC)

Department of the Navy - COMPACFLT

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel* and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- New DoD Information System
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- Yes, DITPR Enter DITPR System Identification Number
- Yes, SIPRNET Enter SIPRNET Identification Number
- No

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- Yes
- No

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- Yes
- No

If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

Yes

Enter OMB Control Number

Enter Expiration Date

No

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

SORN authorities:

5 U.S.C. 301, Departmental Regulations

10 U.S.C. 5013, Secretary of the Navy

10 U.S.C. 5041, Headquarters, Marine Corps

E.O. 9397 (SSN), as amended

5 USC:

Chapter 53 PAY RATES AND SYSTEMS

Chapter 55 PAY ADMINISTRATION

Chapter 61 HOURS OF WORK

Chapter 63 LEAVE

31 USC:

Chapter 35 ACCOUNTING AND COLLECTION

DoD Financial Management Regulation (DoDFMR) 7000.14-R, Vol. 8, Chapter 5

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

Central Registry/Digital Time Card (CR/DTC) provides administrative functions requiring personnel information. It is a central consolidation utility that hosts personnel data management requirements. This MS SQL and Web interface tool provides one master list of employees and several modules intended to reduce internal MS Excel and MS Access proliferation of PII data. CR/DTC is a highly scalable bi-lingual centralized information system which contains multiple modules including, USCS/Military Recall Roster, Emergency POC, Supervisor/Employee/Dependent Reports, Government Driver's License tracking, USCS Position List, Directory Service, Parking Lot Maintenance, Security Clearance Access, Private Vehicle Parking Validation, NEO Tracking, Collateral Duty Tracking, Language Testing and Scoring, Digital Attendance System for capturing training attendance for large audiences, Master Labor Contract (MLC) / Japanese Position Description, Prospective Gain/Loss Position Details, Personnel Action History Retention, Length of Service Computation. Central Registry/Digital Time Card (CR/DTC) most significantly contains legal Japanese characters for names and home addresses unique to Japan for the Government of Japan compliance in foreign labor reporting and not available in any other application. Digital Time Card enables Japanese required Time Clock information used to audit GOJ MLC Pay Reports.

Personnel information collected includes: name, citizenship, gender, birth date, place of birth, personal cell phone number, home telephone number, personal e-mail address, mailing/home address, security clearance, spouse information, marital status, child information, emergency contact information, training information, time and attendance information, pay rates, and leave information.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The privacy risks associated with the PII collected are the unauthorized disclosure of the PII. CR/DTC mitigates the risk through the implementation of administrative and technical access controls that meets the requirement in NIST 800-53, 5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; and E.O. 9397 (SSN); 5 U.S.C. Chapters 53, 55, 61 and 63; 31 U.S.C. Chapter 35; DoD Financial Management Regulation (DoDFMR) 7000.14-R, Vol. 8, Chapter 5.

These risks are addressed to safeguard privacy by protecting the data collection resource with strong SSL encryption, programmatically restricting the system from releasing PII data through its interfaces. Periodic Information Assurance certification on system. Physical location of the system servers are controlled by a cipher lock and alarm, in addition, only authorized Ship Repair Facility and Japan Regional Maintenance Center (SRF-JRMC) users must have a valid PKI certification to access the system.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

Within the DoD Component.

Specify.

Other DoD Components.

Specify.

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

Contractor (Enter name and describe the language in the contract that safeguards PII.)

Specify.

Other (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

Yes

No

(1) If "Yes," describe method by which individuals can object to the collection of PII.

However, failure to provide the requested information may result in delayed payroll entries and not able to contact an employee or a family member in an emergent situation.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

Yes

No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

PII information stored within CR/DTC is initially collected when each employee completes a hard copy form. At the top of this hard copy form is a PRIVACY ACT STATEMENT, stating the intended use of the information being requested. By signing the form, the individual consents to the use and accuracy of the information provided within the form. For disputes to the specific uses of employee PII, employee may contact SRF-JRMC C1120, Administration Department.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- | | |
|--|--|
| <input checked="" type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

The Privacy Act Statement, as required by 5 U.S.C. 552 is provided on approved SRF-JRMC US Civil Service/Contractor AIM/Central Registry/NEMAIS user agreement form for the purpose of requesting information of employee.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.