



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Ration Entitlement Verification System (REVS)

Department of the Navy - CNIC

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.

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

REVS does not collect from members of the public.

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 NM05000-2, Program Management and Locator System (January 24, 2008, 73 FR 4193),
authorities:

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps
E.O. 9397 (SSN), as amended.

SORN NM05512-2, Badge and Access Control System Records (April 09, 2014, 79 FR 19593),
authorities:

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps
OPNAVINST 5530.14E, Navy Physical Security
Marine Corps Order P5530.14, Marine Corps Physical Security Program Manual
E.O. 9397 (SSN), as amended.

Additional authorities:

Homeland Security Presidential Directive 12 (HSPD-12) Policy for a Common Identification Standard for
Federal Employees and Contractors
BUPERS Instruction 1710.11C, Operations of Morale, Welfare, and Recreation Programs 2003

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.

Purpose: The requirement for the Ration Entitlement Verification System is to provide a scalable authentication and authorization platform on which the Commander, Navy Installations Command (CNIC) can develop applications, web services, and features that uses a cardholder's CAC or other DoD approved smart card for authentication and authorization services and benefits.

The purpose of this electronic collection is to manage, supervise, and administer programs for all Department of the Navy civilian, military, and contractor personnel. REVS collects CAC holder PII information on Federal personnel and Federal contractors from authoritative data sources to provide CNIC with the ability to interactively check for authentication and verification of Ration-In-Kind (RIK) meal entitlement before it is provided to service members.

REVS provides authentication and revocation services to Federal Personnel and Federal Contractors by ensuring their credentials are still part of REVS databases. This ensures the Department of Navy has an enterprise solution for validating credentials.

The major operational functions of REVS are to authenticate identity of military service members and verify that they are receiving Ration-In-Kind (RIK) meal entitlement via the use of CAC instead of paper meal entitlement card or "meal pass" card.

Types of Personal Information collected: Name, SSN, Duty email, UIC, Branch of Service, and Rank.

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

Privacy Risks:

The privacy risks are minimal as the data collection and data flow are encrypted. Only those persons with the appropriate access, accounts and privileges can view the PII in the system. The minimal risks are as follows:

(a) Since REVS operates on a NIPRNET enclave and Navy Marine Corps Intranet (NMCI) network, there is a risk that security controls could be disabled during maintenance of the system and other purposes. The risk would be that the security controls would not be reset.

(b) All systems are vulnerable to "insider threats". The REVS managers are vigilant to this threat by limiting system access to those individuals who have a defined need to access the information. There are defined criteria to identify who should have access to the REVS system. These individuals have gone through extensive background and employment investigations.

Safeguards:

Encryption: REVS implements strong encryption methodology in accordance with the National Institute of Standards and Technology (NIST) approved (FIPS 140-2 validated) algorithms to protect its data. The REVS system was designed with security in mind. The O/S is a Security Enhanced version of the Linux kernel which enforces various kinds of mandatory access control policies, and Multi-level Security. REVS enforces a two-factor authentication (CAC + CAC Pin) for all kinds of access and transactions. REVS employs industry standard techniques to protect the control points within the system. In general, everything is protected with public/private or symmetric key concepts. Data and communications are encrypted.

Additionally, the REVS system uses a standard suite of hardware encrypted key techniques to ensure the devices talking to each other on the network are authentic. The use of secure network services is also utilized for communications such as HTTPS and LDAP. The servers communicate with each other via the NIPRNET and authenticate between themselves using cryptographic certificates. The information processed by the system is Sensitive Unclassified. Standard DOD security safeguards for logging is also implemented. This includes DOD requirement of user utilizing the CAC for network and system access.

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.

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

[Empty rectangular box]

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.

[Empty rectangular box for describing consent methods]

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

REVS does not collect directly from the individual.

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

- Privacy Act Statement Privacy Advisory
 Other None

Describe each applicable format.

REVS does not collect directly from the individual.



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.