



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

ENABLER FRAMEWORK (EF)

DEPARTMENT OF THE NAVY, COMMANDER, NAVY INSTALLATIONS COMMAND

### **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.

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

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; DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP); OPNAVINST 1000.23C, Pay/Personnel Administrative Support System (PASS) Management Manual (PASSMAN); OPNAVINST 5530.13C, Department of the Navy Physical Security Instruction for Conventional Arms, Ammunition, and Explosives (AA&E); and OPNAVINST 3591.1E, Small Arms Training and Qualification.

**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.

Preface: The Enabler Framework has an existing Privacy Impact Assessment (PIA) that requires an update to address the addition of a Card Credentialing feature that will generate smart-card Visitor Day Passes to the members of the general public. The Enabler Framework Card Credentialing feature will help centralize, organize, and account for issuing Department of Navy (DON) Visitor Day Passes which will be smart cards instead of non-token cards to civilians who are visiting base installation and require temporary access to a building or facility. The issuance of the temporary smart card to a visitor or guest will provide the ability to track his / her access to buildings and facilities during the visit using the token on the smart card through the Enabler Framework Card Credentialing feature.

Purpose: The requirement for the Enabler Framework 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 of 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. The Enabler Framework collects CAC holder PII information on Federal personnel and Federal contractors from the authoritative data source Defense Enrollment Eligibility Report System (DEERS) database and the Department of Navy Total Workforce Management System (TWMS) by using Secure Socket Layer (SSL) as defined in the Enabler System Security Authorization Agreement (SSAA). This provides Enabler with the ability to interactively check for authentication, permissions and privileges before any benefit, service or privilege is provided.

The Enabler Framework provides authentication and revocation services to Federal Personnel and Federal Contractors by ensuring their credentials are still part of the DEERS database. This ensures the Department of Navy has an enterprise solution for validating credentials. The non-contract personnel (visitors) are not part of the DEERS database. Their credentials are verified via a Sponsor and a Visitor Control Center Security Representative, a valid Federal or State government identification containing a photograph, a current State identification or other government issued identification, and vehicle information along with proof of insurance.

The non-contract personnel (i.e. visitors who are members of the general public) are not part of the DEERS database. Their PII data credentials are verified via a Sponsor, a valid Federal or State government identification containing a photograph, a current State identification or other government issued identification, and vehicle information along with proof of insurance.

The major operational functions of the Enabler Framework are physical access to buildings and front gates, access to food service galleys by replacing the paper meal entitlement card with the CAC, issuance and recovery of weapons in armories to those individuals whose weapons qualifications are active, and for the issuance of a temporary Visitor's Day pass (smart card) to a sponsored visitor or guest which will provide the ability to track his / her access to buildings and facilities during the duration of the visit.

**Types of Personal Information:**

The types of personal information collected are as follows: Name, Truncated SSN, Citizenship, Driver's License, Legal Status, Birth Date, Biometrics, Social Security Number, Other ID Number, Gender, Place of Birth, Assigned UIC, Branch of Service, Cadency, Dates of Visit, Duty Address, Duty City, Duty Email, Duty Phone, Duty State, Duty Zip, Electronic Data Interchange Personal Identifier, Entity Status, Eye Color, Hair Color, Height, Non-U.S. Government Agency, Pay Grade, Personnel Category, Photograph, Purpose of Visit, Rank, U.S. Government Agency, Vehicle Information, Visitor's Sponsor Name, Visitor's Point of Contact Information, and Weight.

(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 is 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 the Enabler Framework system operates on the Navy Marine Corp.. Intranet (NMCI) Network, there is a risk that security controls could be disabled for maintenance and other purposes. The risk would be that the security controls would not be reset.

(b) All systems are vulnerable to "insider threats". The Enabler Framework 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 Enabler Framework. These individuals have gone through extensive background and employment investigations.

**Risk Mitigation:**

(a) Access Controls. Access controls limit access to the application and/or specific functional areas of the application. These controls consist of privileges, general access, password control and discretionary access control. The Enabler Framework enforces a two-factor authentication (CAC + CAC Personal Identification Number) for access and transactions. Users are granted only those privileges that are necessary for their job requirements. Each individual user of the Enabler Framework has a uniquely identified account and each user account is assigned a specific role or specific roles within the system for access to a given portal.

(b) Confidentiality. This ensures that data is not made available or disclosed to unauthorized individuals, entities, or processes.

(c) Integrity. This ensures that data has not been altered or destroyed in an unauthorized manner.

(d) Audits. This includes review and examination of records, activities, and system parameters, to assess the adequacy of maintaining, managing and controlling events that may degrade the security posture of the application.

(e) Training. Security training is provided on a continuous basis to keep users alert to the security requirements. Visual effects are used as constant reminders to ensure users always remain aware of their responsibilities.

(f) Physical Security. This consists of placing servers that contain privileged information in a secure and protected location, and to limit access to this location to individuals who have a need to access the servers. An internal policy is set in place to ensure that there are always no less than two users present at a time when privileged information is being retrieved. Since the server and data reside within a DON.

(g) Encryption. Enabler is a Phase III Defense Information Technology Security Certification and Accreditation Process (DITSCAP) accredited system for both NMCI and NIPRNET. Encryption is done with the National Institute of Standards and Technology (NIST) approved algorithms. The Enabler Framework was designed with security in mind. The O/S is a Security Enhanced version of the Linux 2.6.29.4 kernel which enforces various kinds of mandatory access control policies, including those based on the concepts of Role-based Access Control, and Multi-level Security. Enabler enforces a two-factor authentication (CAC + CAC Pin) for all kinds of access and transactions. The Enabler Framework 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 Enabler 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 LDAPS. The servers (ENodes) 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 will be supported. This includes NMCI requirements, standard user name and password (3 attempts) and utilizing the CAC for NMCI communications for compliance with Open SSL FIPS 140-2 validation.

**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.

Navy, Marines, Public Safety Antiterrorism Force Protection, Naval Criminal Investigative Service (NCIS)

**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.

Individuals have the opportunity to object to the collection of their PII by following the procedures outlined in the System of Record Notice (SORN) NM05000-2 and by refusing to provide the requested PII information as disclosure is voluntary; however, failure to provide the information may result in refusal to grant access to DoD installations, buildings, facilities, denial of services, and issuance of a Visitor Day Pass.

(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.

Individuals can give or withhold their consent to the specific uses of their PII following the procedures outlined in the System of Record Notice (SORN) NM05000-2 or by refusing to provide the requested information. Disclosure of PII is voluntary; however, failure to provide the information may result in refusal to grant access to DoD installations, buildings, facilities, denial of services, and issuance of a Visitor Day Pass.

[Empty rectangular box]

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

[Empty rectangular box for providing reasons]

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.

The Privacy Act Statement will be presented to the individual in paper format on the back of the Application for Department of Navy Visitor Day Pass Enrollment form.

**PRIVACY ACT STATEMENT**

**AUTHORITY:** 10 U.S.C. 5013, Secretary of the Navy; and E.O. 9397 (SSN).

**PRINCIPAL PURPOSE(S):** To manage and administer Department of the Navy civilian, military, and contractor personnel applications for Visitor Control Day Pass temporary smart cards; to control access to and movement in or on DoD installations, buildings, or facilities; and to authenticate the identity of the authorizing / verifying official for security or auditing.

**ROUTINE USE(S):** Used by personnel with an official need to know to control and monitor access to DoD installations, buildings, and facilities.

**DISCLOSURE:** Voluntary; however, failure to provide information may result in denial of the Visitor Control Day Pass temporary smart card and denial of access to DoD installations, buildings and facilities.

**PRIVACY ADVISORY**

In the future, the PII may be collected electronically from an individual from a secure web site at which time a Privacy Advisory notice will display on the monitor prior to the actual collection of the PII 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.**