



PRIVACY IMPACT ASSESSMENT (PIA)

For the

NAVY ACCESS CONTROL SYSTEM - LENEL (NACS-LENEL)

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.

SECTION 2: PIA SUMMARY INFORMATION

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

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

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

Pending

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 NM05512-2 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 Orde 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
OPNAVINST 5530.14E, Navy Physical Security and Law Enforcement Program.
DoDD 5400.11R, Department of Defense Privacy Program

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 Navy Access Control System (NACS) is an existing system that automates access control into a Navy Installation. This allows for manpower reduction to staff access control points allowing Navy personnel to return to military focused operations.

Purpose: The requirement for NACS is to provide automated entrance into a naval installation based on two factor authentication leveraging existing authoritative identification sources such as CAC and Teslin cards. The NACS system collects this information from these cards through proximity sensors and/or barcode.

Note: Teslin is the type of card that DMDC DEERS provides for DOD retirees and dependents (it is not PIV or CAC enabled). It is the blue and brown ID cards that you see.

The purpose of this electronic collection is to authorize Department of the Navy civilian, military, and contractor personnel entrance onto the naval installation. NACS compares CAC and Teslin 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) via Socket Layer (SSL) as defined in the Enabler System Security Authorization Agreement (SSAA). This provides NACS with the ability to interactively check for authentication, permissions and privileges before any benefit, service or privilege is provided.

The NACS leverages CNIC's Enabler Framework which provides authentication and revocation services to Federal Personnel and Federal Contractors by ensuring their credentials are still valid in the DEERS database. This ensures that NACS has an enterprise solution for validating credentials.

The major operational functions of NACS is physical access to Naval Installations with the CAC or Teslin cards. The CAC and Teslin card information is collected at the proximity reader and/or barcode, transmitted via direct cable connection to a Lenel/NGP panel and verified against the local Lenel Onguard 2013 database. If card holder information is not present, a request is sent to the CNIC Enabler system via web services request over SSL. The CNIC Enabler system will verify against it's database for record matching. If none exists, a web services call via JGS protocol will be sent to DMDC DEERS database for final and authoritative record matching. Based on validation of card holder data, the card holders information or lack of validation will be sent back to CNIC's Enabler and then back to the requesting Lenel Onguard 2013 database for future local authentication. This will trigger either authorization or denial of the requester. If the card is valid and validated, the Lenel/NGP panel will send a digital signal triggering entrance onto the Naval facility. If the card is invalid or can not be properly read, the card holder will be denied access, forcing the requester to exit the location and proceed to a manned location for resolution.

Types of Personal Information: Name, DoD ID Number, Biometrics, FACS-N, License Plate Picture, Video. When a system user presses the intercom button at a gate to request assistance, the image of their face is transmitted to the Regional Dispatch Center that is assisting them. So, the facial image is the biometric PII element and also the video PII element collected here.

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

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 risks are as follows:

(a) Since the NACS system operates on the Navy's Public Safety Network (PSNet) which is a closed 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 NACS 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 NACS. These individuals have gone through extensive background and employment investigations.

Safeguards:

Encryption. Enabler is a MAC III Sensitive DoD Information Assurance Certification & Accreditation Process (DIACAP) accredited system for All Navy Networks. 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. NACS enforces a two-factor authentication (CAC + CAC Pin) for all kinds of access and transactions. NACS 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, NACS 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 PSNet 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 PSNet requirements, standard user name and password (3 attempts) and utilizing the CAC for 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.

This system only requests PII credentialing data from DMDC (DEERS). This will not be creating or pushing any PII to other DoD components. Each installation site will host their own Navy Access Control System (NACS) server located within their data center and will not exchange data outside their site enclave.

Other DoD Components.

Specify.

Navy, Marines, Public Safety Anti-Terrorism Force Protection, Naval Criminal Investigative Service (NCIS), Air Force Army, BIMA and other DOD Components as needed.

Other Federal Agencies.

Specify.

Federal Agencies depending on need.

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) NM05512-2 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.

(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) NMOS000-2 and NM05512-2 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.

(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.

Privacy Act Statement **Privacy Advisory**
 Other **None**

Describe each applicable format.

No information is provided to the user when requesting PII data. The PII data is resident on the CAC and Teslin card. This information is pulled and verified against the DOD DMDC database for authentication and to allow authorization to enter the Navy base. The system receiving data is fully automated and reads the DOD CAC through the contact-less chip on the CAC as well as bar code on the back of the CAC as a backup or for those individuals that hold Teslin dependent, retired or other federal cards that are able to be authenticated by the DOD DMDC database.

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.