PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Navy Access Control System (NACS)

2. DOD COMPONENT NAME:

Department of the Navy

3. PIA APPROVAL DATE:

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [x] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

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

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.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

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.

e. Do individuals have the opportunity to object to the collection of their PII? [x] Yes [ ] No

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

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

f. Do individuals have the opportunity to consent to the specific uses of their PII? [x] Yes [ ] No

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

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

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

☐ Privacy Act Statement ☐ Privacy Advisory ☒ Not Applicable

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.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒	Within the DoD Component	Specify.	USN
☒	Other DoD Components	Specify.	USMC, USAF, USA, CG
☒	Other Federal Agencies	Specify.	DLA, PFPA
☐	State and Local Agencies	Specify.	
☐	Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	
☐	Other *(e.g., commercial providers, colleges).*	Specify.	

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

☐ Individuals ☒ Databases

☐ Existing DoD Information Systems ☐ Commercial Systems

☐ Other Federal Information Systems

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

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

☐ E-mail ☐ Official Form (*Enter Form Number(s) in the box below)*

☐ Face-to-Face Contact ☐ Paper

☐ Fax ☐ Telephone Interview

☐ Information Sharing - System to System ☐ Website/E-Form

☒ Other *(If Other, enter the information in the box below)*

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.

k. 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 must be consistent.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier SORN NM05512-2

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. NA

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

It does not appear that the system stores any records as it is connected to other systems. NPACS is connected to other systems to include DoDIN, Physical Security Access Control Enterprise Architecture (PSAC-EA) for Authentication, log management and enterprise services, Public Services Network (PSNET) for transport, and Commander Navy Installation Command (CNIC) Cyber Security Operations Center (C2SOC) who is responsible for monitoring technologies such as monthly ACAS Scans via VRAM for verification of applied patches and

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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.

[X] Yes [ ] No [ ] Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)***?** *(Check all that apply)*

[X] Biometrics	[X] Birth Date	[ ] Child Information
[X] Citizenship	[ ] Disability Information	[X] DoD ID Number
[X] Driver's License	[ ] Education Information	[ ] Emergency Contact
[ ] Employment Information	[ ] Financial Information	[ ] Gender/Gender Identification
[X] Home/Cell Phone	[ ] Law Enforcement Information	[ ] Legal Status
[X] Mailing/Home Address	[ ] Marital Status	[ ] Medical Information
[ ] Military Records	[ ] Mother's Middle/Maiden Name	[X] Name(s)
[ ] Official Duty Address	[X] Official Duty Telephone Phone	[X] Other ID Number
[X] Passport Information	[ ] Personal E-mail Address	[X] Photo
[X] Place of Birth	[ ] Position/Title	[ ] Protected Health Information (PHI)[1]
[ ] Race/Ethnicity	[X] Rank/Grade	[ ] Religious Preference
[ ] Records	[ ] Security Information	[ ] Social Security Number (SSN) *(Full or in any form)*
[X] Work E-mail Address	[ ] If Other, enter the information in the box below	

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.

If the SSN is collected, complete the following questions.

(*DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)*

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

[X] Yes [ ] No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

[ ] Yes [ ] No

b. What is the PII confidentiality impact level[2]? [ ] Low [X] Moderate [ ] High

[1]The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2]Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

- [ ] Cipher Locks
- [ ] Combination Locks
- [ ] Key Cards
- [ ] Security Guards
- [ ] Closed Circuit TV (CCTV)
- [ ] Identification Badges
- [ ] Safes
- [x] If Other, enter the information in the box below

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.
DD FORM 2930 NOV 2008 Page 5 of 17
(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.

(2) Administrative Controls. *(Check all that apply)*

- [ ] Backups Secured Off-site
- [x] Encryption of Backups
- [x] Methods to Ensure Only Authorized Personnel Access to PII
- [x] Periodic Security Audits
- [x] Regular Monitoring of Users' Security Practices
- [ ] If Other, enter the information in the box below

(3) Technical Controls. *(Check all that apply)*

- [x] Biometrics
- [x] Command Access Card (CAC)
- [ ] DoD Public Key Infrastructure Certificates
- [x] Encryption of Data at Rest
- [x] Encryption of Data in Transit
- [ ] External Certificate Authority Certificates
- [x] Firewall
- [x] Intrusion Detection System (IDS)
- [ ] Least Privilege Access
- [x] Role-Based Access Controls
- [ ] Used Only for Privileged (Elevated Roles)
- [ ] User Identification and Password
- [x] Virtual Private Network (VPN)
- [ ] If Other, enter the information in the box below

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

Safeguards:
Encryption. Encryption is done with the National Institute of Standards and Technology (NIST) approved algorithms. 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 autilizing the CAC for communications for compliance with Open SSL FIPS 140-2 validation.