

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:

SPAWARSYSCEN (NAVWAR) Security System (SSCSS)

2. DOD COMPONENT NAME:

Department of the Navy

3. PIA APPROVAL DATE:

03/06/20

NAVWAR - Naval Information Warfare Center (NIWC) Atlantic

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

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

- | | |
|--|--|
| <input type="checkbox"/> From members of the general public | <input type="checkbox"/> From Federal employees and/or Federal contractors |
| <input checked="" type="checkbox"/> From both members of the general public and Federal employees and/or Federal contractors | <input type="checkbox"/> Not Collected (if checked proceed to Section 4) |

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

- | | |
|--|---|
| <input type="checkbox"/> New DoD Information System | <input type="checkbox"/> New Electronic Collection |
| <input checked="" type="checkbox"/> Existing DoD Information System | <input type="checkbox"/> Existing Electronic Collection |
| <input type="checkbox"/> 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.

SSCSS consists of access control, video surveillance, and intrusion detection devices, workstations, server and alarms that protect all of NIWC Atlantic's Controlled and Classified Areas for NIWC Atlantic and each of the Atlantic Offices (Wash DC, Norfolk area, Charleston, Fayetteville, Pax River, New Orleans, Tampa). The system is based on the Lenel OnGuard 2013 software suite operating on 2 servers and monitoring remote sensors and field devices, controlled by several administrative workstations in the Security Office, with alarms and video delivered to Security Monitoring stations at the remote offices and in Charleston.

PII: Name, citizenship, race, date of birth, rank/grade, DoD ID, gender, photo, SSN.

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)

Identification, mission-related use

e. Do individuals have the opportunity to object to the collection of their PII? 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 may object to the collection of PII. They may refuse to provide the required PII via their CAC or on any NIWC security access form required for building access or for visitor control. If the individual objects to the collection of the data, they forfeit their request for access to NIWC Controlled Access Areas and will not be able to enter NIWC spaces.

f. 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.

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

Once PII is provided by the individual, consent is assumed.

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.)

- | | | |
|---|---|---|
| <input checked="" type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory | <input type="checkbox"/> Not Applicable |
|---|---|---|

PRIVACY ACT STATEMENT:

AUTHORITY: SORN NM05512-2, 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 5530.14A. Marine Corps Physical Security Program Manual; and E.O. 9397 (SSN), as amended.

PURPOSE(S): To control physical access to Department of Defense (DoD), Department of the Navy (DON) or U.S. Marine Corps Installations/Units controlled information, installations, facilities, or areas over which DoD, DON, or U.S. Marine Corps has security responsibilities by identifying or verifying an individual through the use of biometric databases and associated data processing/information services for designated populations for purposes of protecting U.S./Coalition/allied government/national security areas of responsibility and information; to issue badges, replace lost badges, and retrieve passes upon separation; to maintain visitor statistics; Collect information to adjudicate access to facility; and track the entry/exit times of personnel.

ROUTINE USE(S): To designated contractors. Federal agencies, and foreign governments for the purpose of granting Navy officials access to their facility.

DISCLOSURE: Providing registration information is voluntary. Failure to provide requested information may result in denial of access to benefits, privileges, and DoD installations, facilities and buildings.

AUTHORITY: SORN DMDC 16 DoD, 10 U.S.C. 113, Secretary of Defense; DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Instruction 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB); DoD 5200.08-R, Physical Security Program; DoD Directive 5200.27, Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense (Exception to policy memos); Directive-Type Memorandum (DTM) 09-012, Interim Policy Guidance for DoD Physical Access Control; DTM 14-005, DoD Identity Management Capability Enterprise Services Application (IMESA) Access to FBI National Crime Information Center (NCIC) Files; and E.O. 9397 (SSN), as amended.

PURPOSE(S): To evaluate individuals' eligibility for access to DoD facilities or installations and implement security standards controlling entry to DoD facilities and installations. This process includes vetting to determine the fitness of an individual requesting or requiring access, issuance of local access credentials for members of the public requesting access to DoD facilities and installations, and managing and providing updated security and credential information on these individuals. To ensure that identity and law enforcement information is considered when determining whether to grant physical access to DoD facilities and installations.

ROUTINE USE(S): In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the records contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3).

DISCLOSURE: Providing registration information is voluntary. Failure to provide requested information may result in denial of access to benefits, privileges, and DoD installations, facilities and buildings.

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. Government employees and contractors assigned to the NIWC security program.

Other DoD Components

Specify. _____

Other Federal Agencies

Specify. _____

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. The Command-Wide Administrative Support Services Contract with Liberty Business Associates, LLC is being modified to include the following FAR Clauses 52.224-1, 52.224-2, 52.224-3 and 39.105. When the clauses are included, we will update the PIA.

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

The individual either presents their CAC or the required access form.

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

- | | |
|---|--|
| <input type="checkbox"/> E-mail | <input type="checkbox"/> Official Form (Enter Form Number(s) in the box below) |
| <input checked="" type="checkbox"/> Face-to-Face Contact | <input checked="" type="checkbox"/> Paper |
| <input type="checkbox"/> Fax | <input type="checkbox"/> Telephone Interview |
| <input type="checkbox"/> Information Sharing - System to System | <input type="checkbox"/> Website/E-Form |
| <input type="checkbox"/> Other (If Other, enter the information in the box below) | |

SECNAV Form 5512/1, DON Local Population ID Card/Base Access Pass Registration

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 Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcl.dod.mil>
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.

i. 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.

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

(3) Retention Instructions.

SSIC: 5521.1b - Big Bucket SSIC: 5000-82

TEMPORARY: Cutoff at end of end of calendar year. Destroy 3 years after cutoff.

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 statute 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.

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 and Law Enforcement Program; Marine Corps Order P5530.14, Marine Corps Physical Security Program Manual; and E.O. 9397 (SSN), as amended.

SORN DMDC 16 DoD, Identity Management Engine for Security and Analysis (IMESA) (December 21, 2015, 80 FR 79310) authorities:
10 U.S.C. 113, Secretary of Defense; DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Instruction 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB); DoD 5200.08-R, Physical Security

Program; DoD Directive 5200.27, Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense (Exception to policy memos); Directive-Type Memorandum (DTM) 09-012, Interim Policy Guidance for DoD Physical Access Control; DTM 14-005, DoD Identity Management Capability Enterprise Services Application (IMESA) Access to FBI National Crime Information Center (NCIC) Files; and E.O. 9397 (SSN), as amended.

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.

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.

OMB #0703-0061.

Navy Access Control System and U.S. Marine Corps Biometric and Automated Access Control System

Expires: 01/31/2021