PRIVACY IMPACT ASSESSMENT (PIA)

DoD Information System/Electronic Collection Name:

Security Control System (SCS)

DoD Component Name:

U. S. Navy,

Echelon III - SPAWAR Service Center Pacific (SSC Pacific)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate personally identifiable information (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.
Yes, because of the access by foreign nationals.

☐ (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) 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 **9115**

☐ **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** **Enter UPI** PB2010: 007-17-01-27-02-3477-00

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

☐ **No**

d. Does the DoD information system or electronic collection have 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** **Enter Privacy Act SORN Identifier** NM05512-2 (Badge and Access Control System)

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.

☐ **No**

e. Does this DoD information system or electronic collection have an 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**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

It has been determined that an OMB Control Number is required and the process to obtain one has been initiated. The PIA will be updated accordingly at a later date.

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 provision of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute and/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. Title 5013, Secretary of the Navy; 10 U.S.C. Title 5041, Headquarters, Marine Corps; OPNAVINST 5530.14C, Navy Physical Security; Marine Corps Order P5530.14; Marine Corps Physical Security Program Manual; and E.O. 9373 (SSN).

In addition, SPAWAR Sytems Command (SPAWARSYSCOM) and SSC Pacific are designated as "Restricted" activities. SECNAVINST 5510.36, SECNAVINST 5510.30A, OPNAVINST 5510.1 (series) and OPNAVINST 5530.14 (series) require a government facility that has been designated as "Restricted" to only admit persons whose duties require access and have been granted appropriate authoritization.

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.

The Security Control System manages physical access to SPAWARSYSCOM and SSC Pacific for over 8,000 people. The system is used to record security clearance information for individuals requiring access to these activities; it produces electronic badges authorizing access for government employees, supporting contractors, and visitors. Additionally the system manages information needed to validate access via electronic turnstiles, electronic gates, and through guarded entrances. The application also manages information related to vehicle access to the two activities. It manages information required to control temporary vehicle decals, and compliance with state regulations. The system also manages individual and group visit and access requests. The Security Control System is the means by which personal security specialists record security clearances of employees and for them to have that information available to the badging clerks for production of permanent badges with the Center's standard picture badge format and clearance color stripe. In addition, these badges are encoded to allow access through an electronic access control system. Gates and turnstiles are configured with card readers that allow the holder to swipe their SSC PAC issued badge and gain, when encoded correctly, access to restricted areas. SCS was designed to minimize the effort involved in storing and indexing paper Visit Requests (VRs) either mailed or faxed to the command and in subsequently issuing a temporary badge that authorized the visitor access to the Center. This system has automated the VR process and produces badges as appropriate.

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

Privacy act data must be accessible only to authorized personnel with a "need-to-know." As a function of providing access to the corporate data, the possibility of a threat by malicious intent is created.

The Corporate Database (CDB) operating environment utilizes the security protection provided at the SSC Pacific Information Systems Computer Operations Facility (ISCOF) combined with the CDB system security design as a response to recognized threats.

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

The data will be shared within the U.S. Navy, specifically SPAWARSYSCOM and SSC Pacific.

☐ **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 the method by which individuals can object to the collection of PII.

Disclosure is voluntary. However, failure to provide theinfo may result in denial of entry to SPAWAR System Command and SSC Pacific facilities/spaces, as both are designated as "Restricted" activities.

(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.

Disclosure is voluntary. However, failure to provide the info may result in denial of entry to SPAWAR System Command and SSC Pacific facilities/spaces, as both are designated as "Restricted" activities. It will not have any affect on the Security or Personnel sides.

(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.

Required Privacy Act disclaimer is displayed throughout the site. The DoD required Privacy and Monitoring Advisory is available at login.

Personnel Roster

THE DATA CONTAINED HEREIN IS PROTECTED BY THE PRIVACY ACT OF 1974. ALL MEASURES REQUIRED TO PROTECT THIS REPORT SHOULD BE TAKEN. WHEN REPORT IS NO LONGER REQUIRED, IT SHOULD BE DESTROYED BY BURNING OR SHREDDING.

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 can restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.