PRIVACY IMPACT ASSESSMENT (PIA)

For the

Electronic Security & Control System (ESCS)
Department of the Navy - United States Marine Corps (USMC)

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	DITPR DON ID: 22515
☐	**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 DMDC 10

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.

SORN authorities:

5 U.S.C. 301 Departmental regulations
10 U.S.C. 113, Secretary of Defense, Note at Pub.L. 106-65
10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness
18 U.S.C. 1029, Fraud and related activity in connection with access devices
18 U.S.C. 1030, Fraud and related activity in connection with computers
40 U.S.C. Chapter 25, Information technology management
50 U.S.C. Chapter 23, Internal Security
Pub.L. 106-398, Government Information Security Act
Pub.L. 100-235, Computer Security Act of 1987
Pub. L. 99-474, Computer Fraud and Abuse Act
E.O. 12958, Classified National Security Information as amended by E.O. 13142 and 13292
E.O. 10450, Security Requirements for Government Employees
E.O. 9397 (SSN), as amended

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 Electronic Security and Control System (ESCS) is a private network system to control the physical security for the Camp Lejeune pretrial detention facility. The ESCS is designed to maintain the security of prisoners and staff in the facility. ESCS allows operator control of all critical facility doors. The system stores and displays video for operator analysis and event reconstruction. Additionally, ESCS interfaces with a facility intercom/paging system, a key control system, and an officer duress system. Sensor information flows across a dedicated private communications network. Servers in the system process sensor data, display information, and store the results for reconstruction or reports. Operators manage sensor activity (e. g., a sensor detects an open door that should be closed) and take appropriate response action. The system includes automated features such as opening specific doors in the event of a fire alarm.

ESCS is to be initially used by USMC Active Duty, USMC Civilians, and USMC contractors. The system is owned and operated by the USMC Plans, Policy and Operations (PP&O), which furnishes Commercial Off the Shelf (COTS) hardware and software for the system. PP&O through the USMC host installation's Provost Marshal's Office (PMO), is responsible for collecting, storing and protecting PII of personnel who enroll in the system. PMO enters the PII into ESCS and the system is used to electronically authenticate the identity of personnel who are seeking access to the installation and those that are being detained within the facility. PP&O and the PMO share no PII beyond the authority (statutory or otherwise) specified in this document. The system supports three functions: (1) Enrollment, (2) Credentials, (3) Physical Access Control.

The USMC PMO collects certain biometric and privacy information directly from detained USMC active duty personnel. The USMC PMO uses this information to manage and provide the physical access control to the installation, electronic identity authentication, and detainee roster/location.

Personal information collected by the USMC PMO consists of the following:
First name
Middle initial
Last name
Digital Photo
DoD ID Number

Other information collected includes:
Status
Custody level: (Medium out, medium in, minimum, max)
Disciplinary: (Loss of privileges, disciplinary segregation, other)
Category id: (Disciplinary, administrative, protective custody)
Administrative information: (Pending investigation, other, suicide risk, potentially violent and dangerous, escape risk, loss of privileges, indoctrination, awaiting transfer, medical segregation, prevention of injury)
Housing unit: (A1-A-60 SQ-01 - SQ-14)
Location: (A or SQ)
Release date
Counselor's name
Victim witness: (yes or no)
Segregated: (yes or no)
Alert

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

The risks associated with the PII data collected by the ESCS include possible loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure of PII. Disclosure of PII is low due to the nature of the closed system, limited number of users and location of the system. PII collection has been kept to minimum

consisting of name and digital image only to further lessen the impact of any disclosure. All USMC employees and contractors are required to take mandatory security and privacy training prior to accessing a DoD system. This security and privacy training course includes an overview on privacy and personally identifiable information and its appropriate uses.

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 PII will be shared within the U.S. Marine Corps, specifically with personnel who have responsibility for identity management, access control, antiterrorism/force protection and law enforcement.

☐ **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.

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

Detainees PII collection is not voluntary and is required as a condition of incarceration. Employees must provide as a condition of employment. Before information is collected, the individual is provided the opportunity to read the Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3).

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.

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

Detainees PII collection is not voluntary and is required as a condition of incarceration. Employees must provide as a condition of employment. PII entered into the system is used to electronically authenticate the identity of detainees, track and provide access within the facility. Information collected in ESCS is not used for any other purposes or on any other systems.

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.

Before information is collected, the individual is provided the opportunity to read the Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3), concerning the data collection. The Statement advises that participation is mandatory for detainees.

PRIVACY ACT STATEMENT
AUTHORITY: Title 10 U.S. Code §§ 5014 and 5020

PURPOSE: To determine the facts and circumstances surrounding allegations or complaints against Naval personnel and/or Navy/Marine Corps activities. To present findings, conclusions, and recommendations developed from investigations and other inquiries to the Secretary of the Navy, CNO, CMC, or other appropriate Commanders. Disclosure of Social Security Account Number is voluntary, and if requested, is used to further identify the individual providing the information.

ROUTINE USES: The information is used for the purpose set forth above and may be:

- Forwarded to Federal, State, or local law enforcement agencies for their use;

- Used as a basis for summaries, briefings, or responses to Members of Congress or other agencies in the Executive Branch of the Federal Government;

- Provided to Congress or other Federal, State, and local agencies, when determined necessary.

MANDATORY OR VOLUNTARY DISCLOSURE AND EFFECT ON INDIVIDUAL NOT PROVIDING INFORMATION:

For Military Personnel: Disclosure of personal information is mandatory and failure to do so may subject the individual to disciplinary action.
For Department of the Navy Civilians: Failure to disclose personal information in relation to individual's position responsibilities may subject the individual to adverse personnel action.
For All Other Personnel: Disclosure of personal information is voluntary and no adverse action can be taken against individuals for refusing to provide information about them.

ACKNOWLEDGMENT:

I understand the provisions of the Privacy Act of 1974 as related to me through the foregoing statement.

Signature: _____
Date: _____

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.