PRIVACY IMPACT ASSESSMENT (PIA)

For the

<table>
<thead>
<tr>
<th>Corrections Management Information System (CORMIS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department of the Navy - Bureau of Naval Personnel (BUPERS)</td>
</tr>
</tbody>
</table>

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 ID: 12600 DITPR-DON ID: 22076
☐ 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 UI: 007-000003485

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 NM01640-1

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

OPNAV DNS-15 confirmed that an OMB Control Number is not required.

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) Wherever 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 NM01640-1, Individual Confinement Records, July 12, 2013 authorities:

10 U.S.C. 951, Military Correctional Facilities Establishment; Organization; Administration;
10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 1565, DNA Identification Information
42 U.S.C. 10601 et seq., Victim's Rights and Restitution Act of 1990 as implemented by DOD Instruction
1030.2, Victim and Witness Assistance Program
E.O. 9397 (SSN), as amended.

Other authorities:

DoDI 1325.07 3/11/2013 ADMINISTRATION OF MILITARY CORRECTIONAL FACILITIES AND CLEMENCY AND PAROLE AUTHORITY

SECNAV 1640.9C DEPARTMENT OF THE NAVY CORRECTIONS MANUAL
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.

Corrections Management Information System (CORMIS) is a complex database that performs most functions in the management of Navy brigs, prisoners, awardees, deserter apprehension, and appellant leave. CORMIS is used by all Navy and U.S. Marine Corps brigs, the Navy and Marine detachment at the U.S. Army’s Disciplinary Barracks at Ft. Leavenworth, KS, the Navy and Marine Appellant Leave Activity (NAMALA) and the Navy Absentee Collection and Information Center (NACIC). CORMIS collects, tracks and manages data on housing, custody, rehabilitation programs and education, public law mandated sex offender registration and victim and witness notification, Brady Bill reporting requirements, DNA collection, jobs, appointments, mental and physical health histories, offenses, court actions, sentences, supervised release and clemency reviews, transfers, and releases. CORMIS performs as the central repository for Victim and Witness Assistance Program data. CORMIS automatically calculates sentences, parole eligibility, manages service-members with non-judicial punishment, and Correctional Custody Unit residents and also maintains full banking functionality for the accountability of inmate funds and valuables and enhances the transfer of prisoners between brigs. CORMIS uses Business Objects (report tool) to identify data entry errors for brig staff correction purposes, create task lists, daily change sheets, brig logs, statistics, reports, and trend analysis used in manpower, program and budget planning.

PII collected: Name, Other Names Used, SSN (full and truncated), DoD ID Number, Citizenship, Legal Status, Gender, Race/Ethnicity, Birth Date, Place of Birth, Personal Cell Telephone Number, Home Telephone Number, Personal Email Address, Mailing/Home Address, Religious Preference, Security Clearance, Spouse Information, Marital Status, Biometrics, Child Information, Financial Information, Medical Information, Disability Information, Law Enforcement Information, Employment Information, Military Records, Emergency Contact Information, Education Information.

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

User accounts and system privileges are managed in a way as to limit access to PII data. Other potential inherent risks associated with the collection and management of PII in an automated system (e.g., CAC card theft, or cyber attack) are minimized by complying with DoD IT systems security requirements and providing user training on PII.

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. Navy Brigs, Marine Corps Brigs, NACIC, NAMALA, Navy Clemency and Parole Board, Headquarters for Corrections (Marine Corps), Judge Advocate General (JAG), provides data as requested from multiple commands.

☐ Other DoD Components.

Specify. Air Force Confinement Facilities, Headquarters for Corrections (Army, Coast Guard and Air Force)
Other Federal Agencies.
Specify. Multiple Law Enforcement Agencies, Sex Offender Registry, FBI

State and Local Agencies.
Specify. Multiple Law Enforcement Agencies, Sex Offender Registries (every state has their own)

Contractor (Enter name and describe the language in the contract that safeguards PII.)
Specify. Lockheed Martin: Personnel working on this contract may be required to handle information that is covered by the Privacy Act of 1974 (Title 5 of the U.S. Code, Section 552.a). Contractors working directly with Military Personnel Records will be required to sign a Non-disclosure agreement. The requirement to control access to sensitive information applies to all US government IT systems and/or areas where unclassified but sensitive information may be discussed, displayed or maintained. DON policy prescribes that all unclassified data that has not been approved for public release and is stored on mobile computing devices must be treated as sensitive data and encrypted using commercially available encryption technology. Whenever granted access to sensitive information, contractor employees shall follow applicable DOD/DON instructions, regulations, policies and procedures when reviewing, processing, producing, protecting, destroying and/or storing that information. Operational Security (OPSEC) procedures and practices must be implemented by both the contractor and contract employee to protect the product, information, services, operations and missions related to the contract. The contractor shall designate an employee to serve as the Contractor's Security Representative. Within three work days after contract award, the contractor shall provide to the Navy Command's Security Manager and the Contracting Officer, in writing, the name, title, address and phone number for the Contractor's Security Representative. The Contractor's Security Representative shall be the primary point of contact on any security matter. The Contractor's Security Representative shall not be replaced or removed without prior notice to the Contracting Officer.
The FAR Privacy Clauses are not in the current contract but will be added at the next opportune time/contract modification.

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.

The PII collected in CORMIS comes from official DOD Forms (2700 series) completed by the prisoner, prisoner's command (Confinement Order, Initial Reviewing Officer, etc....), OJAG (Court Documents) and the Service Clemency and Parole Boards. A privacy act statement is a part of each DD form on which PII is collected.

Failure to provide requested information could impact the prisoner's Treatment Programs and other rehabilitative efforts as well as time in confinement where information concerning a release on Parole is concerned.

(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.

☐   

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

Once the information has been provided consent has been given/assumed.

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. Information captured directly from the individual is captured on DD Forms (2700 series) which contain a Privacy Act Statement (PAS).
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.