PRIVACY IMPACT ASSESSMENT (PIA)

For the

DEPARTMENT OF THE NAVY

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: 1664    DITPR DON ID: 20918
☐ 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 UII: 007-000001590

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 NM03760-1

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

DECKPLATE does not collect on members of the public.

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 NM0370-1, Naval Flight Records Subsystem (NAVFLIRS) (February 23, 2004, 69 FR 8186) authorities:

10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; and E.O.9397 (SSN).

Other authorities:

COMNAVAIRFORINST 4790.2 and OPNAV Instruction 3710.7U Naval Air Training and Operating Procedures (NATOPS) General Flight and Operating Procedures.
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.

| Decision Knowledge Programming for Logistics Analysis and Technical Evaluation (DECKPLATE) is the over-arching Naval Aviation Logistics Data System of Systems, providing comprehensive, accurate & timely aviation logistics data, analysis & reporting capabilities; utilizing the most current hardware, software, and technology processes. As the primary source for Naval Aviation Maintenance and Logistics Information, DECKPLATE provides comprehensive aircraft maintenance, flight, and aircraft & engine inventory information from around the world which is collected, fused, and correlated to provide visibility of aircraft, engines, and aeronautical components across the Naval Aviation Enterprise. The analytical capabilities provided by DECKPLATE provide the underpinnings of Sea Enterprise efforts to monitor Naval aviation readiness and identify cost drivers and logistic process inefficiencies. Data could be painstakingly collected from each local reporting activity, but DECKPLATE collects data from around the world and provides a view of aircraft, engines, and aeronautical components across the entire Naval Aviation Enterprise. The DECKPLATE Data Warehouse and Reporting System was developed to provide a single consolidated repository for current and historical naval aviation flight, maintenance and usage data for naval aircraft, engines, components, related support equipment, and personnel capability and qualification data for the purpose of reporting and logistic/engineering analysis. DECKPLATE will be the authoritative data source for over 20 years of detailed maintenance and flight data. The system will provide enhanced user reporting and analysis capability allowing users to access correlate and analyze from multiple sources. DECKPLATE provides an on-line, integrated life cycle logistics readiness and operational weapons systems database, and the tools to sustain critical support analysis. DECKPLATE Provides the Capability to Support Policy Mandated by COMNAVAIRFORINST 4790.2. and OPNAV Instruction 3710.7U Naval Air Training and Operating Procedures (NATOPS) General Flight and Operating Procedures. By adhering to these policies DECKPLATE captures Social Security Numbers (SSN) and stores them in three up line repositories. DECKPLATE does not display SSN to users of the systems, the SSN table is hidden from the normal user community and is only accessible by a select group of database administrators (DBA) and program office subject matter experts. This system is tied to Flight Records and is dependent on a system called Naval Aviation Logistics Command Management Information System (NALCOMIS). PII collected: Name, SSN (full and truncated), DoD ID Electronic Data Interchange Personal Identifier (EDIPI) Number, Military Records. |

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

| The harm of disclosing privacy act information could be detrimental to DECKPLATE military and civilian users. The release of personal identifiable information could possibly lead to identification theft and have financial repercussions. DECKPLATE may be subject to multiple threats throughout its life cycle. These threats vary depending on the scale of installation, geographical location, and whether the system is being used in a peace or wartime environment. For security considerations and in order to reduce the risk of inadvertent violations of the Privacy Act, data shall be transferred via SFTP over the Internet via a TecTIA client that makes use of a public key infrastructure that supports access control, user authentication, and data encryption to enhance security. PII form will be used for personnel enabling DECKPLATE the capability to quickly single out a member’s record from any function and to act on or review the information for that member in all functions to which the user has been granted access. Military flight crew may request a re-creation report of their individual flight logs, which does not contain PII. In order to associate the flight data with an individual and pull a report, the requester must provide their SSN to the |
Functional Data Management (FDM) Lead. The FDM Lead pulls the report by associating the requesters SSN to their flight information. The flight log itself does not contain any PII and is only available to the individual to whom the flight data belongs.

The data is protected at all phases of the information life cycle. DECKPLATE is secured through many tiers; Common Access Card (CAC) credentials, private key encryption, signature authentication, and/or assigned user name and password for those whose roles require access. DECKPLATE is fully DIACAP compliant. Tables containing PII are encrypted and stored with data at rest protection and inaccessible to the average user.

Records in this system are destroyed in accordance with the policies and guidance set out in SECNAV Manual 5210.1.

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. NAVAIR users that belong to the DECKPLATE Sensitive Data Users Group.

- **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. Contractor: Kbr-Wyle. The FAR Privacy Clauses are in the Contract.

Request for Proposal W15QKN-16-R-0056 page 22 of 113:

7.8 Personally Identifiable Information (PII). Any section of the PWS that requires the Contractor to design, develop or operate a system of records on individuals, to accomplish an agency function will be subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a). The Contractor shall comply with the Privacy Act and all applicable agency regulations on individual privacy, to include DoD Directive 5400.11, "Department of Defense Privacy Program" and DoD 5400.11-R, "Department of Defense Privacy Program". The Contractor shall be responsible for compliance with the Privacy Act whenever performance will require the Contractor access to PII regardless of whether the PWS section is explicitly identified.

Page 42 of 113:


All Information Technology systems, software, and website development, modification or support shall be performed in accordance with all applicable Federal, DoD, DON, and NAVAIR policy, guidance, standards, and strategies, and should be integrated within the NAVAIR Enterprise portal and collaboration environment whenever possible. Any Web sites/servers hosted/located in contractor facilities, or outside NAVAIR enclave, will transition to NAVAIR architecture and infrastructure in accordance with Legacy Shutdown guidance.
"All IA shall be in compliance with the following listed instructions to include those referenced within the below listing:
As a minimum, hardware, firmware, software, documentation (data deliverables) and/or Information Technology (IT) services delivered by this contract shall be in compliance with the following References:

a. DoDI 8500.01 Cybersecurity, 14 March 2014
b. DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), 12 March 2014.

☐ 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.

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

PII is not collected directly from the individual. The source of PII is Naval Aviation Logistics Command Management Information Systems (NALCOMIS).

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.

PII is not collected directly from the individual. The source of PII is NALCOMIS.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- [ ] Privacy Act Statement
- [ ] Privacy Advisory
- [ ] Other
- [x] None

Describe each applicable format.

PII is not collected directly from the individual. The source of PII is NALCOMIS.
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.