PRIVACY IMPACT ASSESSMENT (PIA)

For the

The Judge Advocate General Personnel System (JAGPERS)
Department of the Navy - DON/AA - OJAG

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: 22214
- ☐ **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 007-000002455

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 N01070-1

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

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:

10 U.S.C. 806, Judge Advocates and Legal Officers
5 U.S.C. 301 Departmental Regulations
5 U.S.C. 3111 Acceptance of Volunteer Service,
10 U.S.C. 87 Defense Acquisition Work Force Rule,
Rule 13A Student Practice Rule
E.O. 9397 (SSN), as amended

Other authorities:
10 U.S.C. 5148, Judge Advocate General Corps
DoD 6025.18-R, DoD Health Information Privacy Regulation

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.

To evaluate applicant qualifications for selection to participate in the JAGC; to evaluate applicant performance in the JAGC internship/externship program; to evaluate and improve the JAGC application and selection process; to conduct predictive analysis for internal management purposes; to manage the officers of the JAGC since the Judge Advocate General is statutorily required to make a recommendation on the assignment of all active-duty JAGC officers; to determine qualifications of an officer to receive a JAGC designation and to be certified as a trial or defense counsel; to determine the rotation dates and release from active-duty dates of JAGC officers, as well as the date new officers will be available for duty; to prepare JAGC strength plans for submission to the Office of the Chief of Naval Operations; and to obtain an officer's preference for duty assignment, as well as eligibility for consideration for postgraduate education and overseas assignments. Certain information is promulgated to all active-duty JAGC officers in an annual publication known as the Directory of Navy Judge Advocates. The information is promulgated in the directory for general informational purposes within the JAGC, including provision of position (billet) availability information to officers contemplating rotation. Information obtained from predictive analysis command evaluations are separate and distinct from evaluations required in accordance with Navy Regulations (i.e., officer fitness reports). The data will not be used to impact judge advocates' evaluations or fitness reports in any way.

Personal information collected includes: Last name, first name, middle initial, maiden name, Social Security Number (SSN), gender, race/ethnicity, date of birth, personal cell telephone number, home telephone number, personal e-mail address, mailing/home address, maiden name (if applicable), spouse name, marital status, emergency contact information, and education information (schools, degrees, grade point average, and class rank). Other information that may be collected includes: work telephone, official work e-mail address, language skills, type of schooling (undergraduate, graduate, etc.), school names, grade point average, class rank, major, degree date, honors, organizations, achievements, grade, designator, previous designator,awards, rank, Navy judge advocate continuation pay eligibility date, date of rank, pay entry base data, active duty service date, active commission base date, year and month of graduation from Naval Justice School, service date, lineal number, year group, current billet, future billets that are finalized, sub-specialty code, law school and year of graduation from law school, state bar membership and year admitted.

Records and correspondence concerning surveys, personal history, education, professional qualifications, physical qualifications, mental aptitude, character qualities, and interview appraisals are created. Such information includes: marital status, LSAT score and percentile, extracurricular activities, employment experience/history, foreign language proficiency, criminal history, self-disclosed drug use, self-disclosed drug/alcohol treatment, motivational statement, branch of service, photo, letters of evaluation/ recommendation, writing sample, clearances granted, and predictive analysis command evaluations.

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

The perceived threats are primarily computer hackers, disgruntled employees, state-sponsored information warfare, and acts of nature (e.g., fire, flood, etc.). All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. There are risks that JAGPERS information could be compromised. Because of this possibility, appropriate security and access controls listed in this PIA are in place. Since JAGPERS operates on the NMCI Network, there is a risk that security controls could be disabled for maintenance and other purposes. The risk would be that the security controls would not be reset. All systems are vulnerable to "insider threats." JAGPERS managers are vigilant to this threat by limiting system access to those individuals who have a defined need to access the information. There are defined criteria to identify who should have access to this system. These individuals have gone through extensive background and employment investigations.

The computer system uses PKI authentication and using TLS/SSL 3 to encrypt data. PII data is stored in SQL Server which is access restricted to Database Administrator/Manager. Backed up data is encrypted

with a complex decipher password. PII will be redacted by data owner before making it available to requestor. Security training is provided on a continuous basis to keep users alert to the security requirements. Visual effects are used as constant reminders to ensure users always remain aware of their responsibilities. Physical security is addressed by placing servers that contain privileged information in a secure and protected location, and to limit access to this location to individuals who have a need to access the servers.

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 OJAG Personnel; Naval legal Service command (NLSC) personnel; Navy recruit and detailing personnel; Navy Personnel Research, Studies and Technology (NPRST); Department of the Navy Assistant for Administration (DON/AA) personnel;

☐ **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. Segue (OJAG) and Booz Allen Hamilton (DON/AA), while development/system maintenance is in progress. Information is included in all service contracts to ensure that the development contractor has a minimum of a SECRET Clearance and that the individual(s) will be required to sign a non-disclosure agreement. Additionally, companies are required to have at least a Secret FACILITIES CLEARANCE. We do not accept a contractor with a clearance if the facility itself has not gone through and attained a facilities clearance.

☐ **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.

By providing information, individual consent is given.

(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.

Can withdraw consent verbally or in writing

(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.

Privacy Act is posted on login screen.

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.