PRIVACY IMPACT ASSESSMENT (PIA)

For the

Case Management Tracking Information System (CMTIS)
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 ID: 13426 DITPR DON ID: 22215
☐	**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: 007-000002922

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 N05801-1, N05801-2, N05813-2 thru 6, N05814-3 , N05814-6

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:

N05801-1

5 U.S.C. 301, Departmental Regulations; Manual of the Judge Advocate General; and E.O. 9397 (SSN).

N05801-2

5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 1044; and 32 CFR part 727, Legal Assistance.

N05813-2

5 U.S.C. 301, Departmental Regulations.

N05813-3

5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 865; and 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 Procedures.

N05813-4

5 U.S.C. 301, Departmental Regulations; 42 U.S.C. 10606-10607; E.O. 9397 (SSN); and Rule for Court-Martial 502(d)(5), Manual for Court-Martial; and the Victims' Rights and Restitution Act of 1990.

N05813-5

5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 865; 10 U.S.C. 866(b); and 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 Procedures.

N05813-6

5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 865; and 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 Procedures.

N05814-3

5 U.S.C. 301, Departmental Regulations; 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 Procedures; and E.O. 9397 (SSN).

N05814-6

5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 866, 867; and E.O. 9397 (SSN).

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 system collects data in all areas of a legal trial and defense practice, while also containing modules for Legal Assistance, Personnel Representation, and Staff Judge Advocate/Command Services. It enables the JAG Corps to meet its organizational strategic goals by providing the mechanism to track and manage cases and workloads across the Enterprise in all areas of legal practice while capturing attorney productivity and ensuring timely disposition of military justice cases. The system data is utilized to assess manning needs worldwide (both in the judiciary and also for counsel assignment), and to track trends that may be developing in regard to the types of crimes being committed. The data contained in the database has also is used in responding to inquiries from Congress concerning individual court-martial cases or concerning various trends throughout the Navy and Marine Corps relating to criminal infractions, sentences awarded, clemency recommendations, and other facts important to criminal justice in general. Data is used to assess the timeliness of the court-martial process from date of referral of charges through the date of authentication of the record of trial. This information is critical to ensuring the constitutional mandate to provide every accused a "speedy trial" upon demand. It allows the legal practitioner to identify where in the business process delays may be occurring, thus giving the legal practitioner a more accurate picture of how to resolve the issue. The data from military justice cases as well as legal assistance, command services, and other legal support areas flows from the first request for services all the way through the appeals process. This allows JAG to do reports required by SECNAV, CNO, and other DoD and Navy entities is support of manning issues.

PII collected: Name, other names used, social security number (full and/or truncated), gender, birth date, personal cell number, home telephone number, personal email address, mailing/home address, spouse information (full name, maiden name, and last 4 of the spouse's social security number if the individual seeking legal assistance is a military dependent), marital status, child information (name, gender, last four), financial information (as applicable), medical information (as applicable), disability information (as applicable), law enforcement information (description and classification of legal issues, pleas, records of trial or inquiry), employment information, military records (rank, duty station, phone number), fax number. Similar information, as applicable is collected from the opposing party, if known. For the administration of military

justice information about the accused is also collected.

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

Privacy risk is the same for any automated computer system - data could be breached by a hacker, disgruntled employee, social networking or act of nature. 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 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; 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.

Individuals are asked for PII on intake sheets for Legal Assistance and Personnel Representation appointments. Individuals can refuse to provide information, but they may be denied an appointment if we cannot perform an appropriate conflicts check under legal ethics rules. Individuals have the opportunity to object to the collection of CERTAIN (but not all) PII. In order to run conflict checks, we collect the individual's full name, social security number, their date of birth, and home address. Individuals are given the opportunity to refuse to provide the social security number. In order to run effective conflict checks, however, we must have at least one item of PII along with the individual's full name. Thus, the individual cannot object to the collection of all PII unless they want to be denied an appointment.

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

Individuals charged with a crime under the UCMJ cannot object to the collection of data for military justice purposes. Individuals processed for administrative separation cannot object to information collected to carry out the administrative separation process.

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.

The information is integrated into a single database and is used for administrative purposes within the JAGC only. It is not shared with outside sources for other purposes, unless properly and lawfully requested under FOIA or the Privacy Act, and in many cases is subject to the attorney-client privilege.

Individuals do not have the opportunity to object to specific uses for their PII. We collect PII in order to ensure that a prospective client is not an opposing party to a client we have already seen. We store PII for all former clients (as well as their self-reported opposing parties) in the CMTIS database, and then compare a prospective client's PII to that database. If a prospective client matches as an "opposing party," or if the "opposing party" information that the prospective client provides matches a client the office has already seen, the prospective client will be referred to another office. We cannot provide legal assistance services without running this type of "conflict check." Thus, the only way the individual can avoid this use of their PII is by not obtaining legal assistance services.

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.	The information/privacy act statements/privacy advisories are provided on intake sheets. Clients are reminded that information they provide during appointments is protected by the attorney-client privilege. We provide the following two notices on the legal assistance intake sheet: FOR OFFICIAL USE ONLY – PRIVACY ACT SENSITIVE. Any misuse or unauthorized disclosure may result in both civil and criminal penalties. PRIVACY ACT STATEMENT: AUTHORITY 5 U.S.C. 301 & 44 U.S.C. 3101 (Executive Order 9397) SSN PRINCIPAL PURPOSE(S): Information is to monitor the caseloads in legal assistance office. ROUTINE USE (S): In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows: The 'Blanket Routine Uses' that appear at the beginning of the Navy's compilation of system of record notices apply to this system. To victims and witnesses to comply with the Victim and Witness Assistance Program, the Sexual Assault Prevention and Response Program, and the Victims' Rights and Restitution Act of 1990. To governmental, public and private organizations and individuals, as required. MANDATORY/VOLUNTARY DISCLOSURE, CONSEQUENCES OF REFUSAL TO DISCLOSE: Disclosure of SSN is voluntary and there will be no adverse consequence from refusal to disclose; however, an individual may be requested to establish eligibility for legal assistance by other means (e.g., production of military identification). Refusal to establish eligibility may preclude the requested assistance. Disclosure of all other requested information is voluntary, but failure to provide such information may limit this Command's ability to provide assistance

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.