PRIVACY IMPACT ASSESSMENT (PIA)

For the

CLAIMS & FOIA MANAGEMENT SYSTEM (CFMS)
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: 14116 DITPR DON ID: 22323
☐	**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: 007-000004581

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 N05890-1 and NM05720-1

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:

N05890-1

Federal Tort Claims Act (28 U.S.C. 1346(b), 2671-2680); 32 CFR 750.21-750.40; Medical Care Recovery Act (42 U.S.C. 2651-2653); Collection From Third Party Payers Act (10 U.S.C. 1095); Federal Claims Collection Act (31 U.S.C. 3701, 3711, 3716-3719); 32 CFR 757.1-757.21; Foreign Claims Act (10 U.S.C. 2734); Military Claims Act (10 U.S.C. 2733); 32 CFR 750.41-750.60; 'Nonscope' Claims Act (10 U.S.C. 2737); 32 CFR 750.60-750.69; Military and Civilian Employees Claims Act (31 U.S.C. 3701, 3721); 32 CFR 751.0-751.3; 10 U.S.C. 1552; 39 U.S.C. 406 and 2601; 5 U.S.C. 301, Departmental Regulations; 44 U.S.C. 3101; and 31 U.S.C. 3729.

NM05720-1

5 U.S.C. 552, the Freedom of Information Act, as amended; 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; Secretary of the Navy Instruction 5720.42F, Department of the Navy Freedom of Information Act Program; and 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 CFMS consists of all Claims applications (MCRA, Torts, PCU and Investigations) used by the JAG Corps to meet the legally mandated requirements to track, pay, and recover personal, property and medical claims.

The JAG Corps uses the CFMS to manage and evaluate, and process claims both for and against the Department of the Navy for purposes of adjudication, collection and litigation. It also provides the Armed Forces Institute of Pathology with closed claims files and investigations for use in the medico-legal quality assurance and risk management matters for the DoD.

Electronic and hard copy files within the system may contain personal information including: Name, other names used, SSN, birth date, personal cell telephone number, home telephone number, personal e-mail address, mailing/home address, marital status, military records, disability information: type of disability and disability code;

Other : Information contained within CFMS electronic databases include branch of service, pay grade date, status (active, retired, reserves, etc.) , and insurance policy and claim numbers;

Spouse and child information: name, address, phone number, social security number, rank, branch of service, and relationship to claimant or injured party, is collected to show the relationship between multiple claimants, a sponsor-dependent relationship for medical treatment purposes, or authority to file a claim for damage to personal property incident to service on behalf of a spouse service member;

Financial information: banking account numbers and assets and liabilities, is collected for depositing funds made to settle claims and to assess requests for compromise of affirmative claims; and

Law enforcement and Medical information: Files may also contain claims filed, correspondence, investigative reports, witness statements, personnel, medical and dental records, x-rays, allied reports (such as police and U.S. Postal Service investigations), photographs and drawings, legal research and memoranda, opinions of experts and others, court documents, reports of injuries to individuals entitled to care at Navy expense, reports of damage to Navy property, statements of charges for medical and dental treatment, copies of orders, copies of insurance policies, government bills of lading, copies of powers of attorney, estimates of loss or damage, inventories, demands on carriers for reimbursement, copies of correspondence with claimant, potential claimants, insurers or representatives of claimants or third parties, copies of finance vouchers evidencing payment of claims, and similar relevant information.

(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 CFMS information could be compromised. Because of this possibility, appropriate security and access controls listed in this PIA are in place. Since CFMS 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". CFMS 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.

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 and Dept of the Navy personnel pursuant to routine use provisions of SORN

☒ **Other DoD Components.**

Specify. DFAS, and other DoD agencies that may have a need to know certain information about an ongoing claim,

☒ **Other Federal Agencies.**

Specify. Treasury Deptartment and with DoJ attorneys who defend the USG when a lawsuit is filed against us (if we deny certain claims the claimant has the right to file a lawsuit in Federal court).

☐ **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.

Disclosure of PII is voluntary, however, individuals must provide certain PII in order to have claims processed and, if applicable, paid. Failure to disclose information needed to process a claim may render the claim invalid.

Under the statutory and regulatory guidelines for assertion of affirmative US Government claims to recover the costs of medical care furnished or paid for by the Federal Government, beneficiaries are obligated to provide the agency information with data necessary to pursue the claim. Further, the US Government is authorized to retrieve that information from individuals, entities and government systems of records, and to provide that information to other entities, to pursue payment of our claim.

(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.

Claimants are advised that the PII collected is to be used in the processing of their claims.

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.	A Privacy Act Statement is provided on each claim form (paper or electronic), or with the paperwork accompanying the notice/request for information for use by the US Government when pursuing an affirmative claim.

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.