



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

OGCONLINE (OGCONLINE)

Department of the Navy - DON/AA

### **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
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

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: 5283    DITPR DON ID: 20910
- 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

UJI: 007-000002493

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

NM05800-1 (new) (currently N05800-1 is being revised)

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.

20161018

**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 NM05800-1 authorities:  
5 U.S.C. 571 Administrative Dispute Resolution Act of 1996; 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5019, General Counsel; 10 U.S.C. 5031, Office of the Chief of Naval Operations; 10 U.S.C. 5041, Headquarters, Marine Corps; Executive Order 12988, "Civil Justice Reform," February 5, 1996; DoD Directive 5145.5, Alternate Dispute Resolution (ADR); DoD Instruction 5505.02, Criminal Investigations of Fraud Offenses; SECNAVINST 5430.25E, The General Counsel of the Navy, Assignment of Responsibilities; SECNAVINST 5430.92B, Assignment of Responsibilities to Counteract Acquisition Fraud, Waste, and Related Improprieties within the Department of the Navy; SECNAVINST 5800.13A, Alternative Dispute Resolution (ADR) Policy and Mission of the DON ADR Program Office; 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.

This system is the primary communication and management tool for the Office of the General Counsel (OGC). It is used to defend the DON in litigation in federal and state courts and in administrative forums, to administer the Acquisition Integrity Program as well as the Alternative Dispute Resolution (ADR) Program, to manage the personnel of the OGC, to distribute and promote communications worldwide among the DON legal community, and to administer access to the above information using appropriate permission sets.

Personal Information collected (see Section 3, question (a) of this PIA):

Statements; affidavits/declarations; investigatory and administrative reports, personnel, and promotion information; hotline complaints; police reports; social security numbers; indictments; criminal information filings; sentencing orders; discovery and discovery responses; motions; pleadings; subpoenas; briefs; legal opinions; orders; rulings; letters; memoranda; messages; related correspondence; forms; reports; surveys; audits; summons; and other relevant documents required for litigation, acquisition integrity, or administrative matters; and photographs.

ADR participant information including name, work address, work telephone number, and work e-mail address; mediator information including name, experience, training, status of mediator certification, evaluation data, work address, work telephone number, and work e-mail address; records pertaining to dispute resolution activities conducted including date, time, and location of ADR session; form of ADR; case type; subject matter of the mediation or facilitation; outcomes of ADR activity; and notes pertaining to the ADR activity

Correspondence and records pertaining to performance, employment, pay, classification, security clearance, personnel actions, retirement, bar membership, bar certification, professional qualifications, employee profile, education, training, location, recall information, and administration of Office of the General Counsel civilian personnel and contractor employees.

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

Data could be compromised by hackers, a disgruntled employee, or an act of nature.

This information is protected with both user and advanced system administrator training, defense in depth network perimeter protection including firewalls, host based security systems, intrusion protection systems, two factor user authentication using DoD PKI, strict adherence to DoD configurations standards, server separation using DMZ concept, continuous monitoring both inside and outside the system, state of the art physical security, system authorization through the appropriate Navy authority, top security clearances for all system administrators with root access on production systems, compliance with all encryption standards, off-site COOP data center with backup data, granular user access based on need to know, and privacy alerts for forms that will expose input to the entire community.

**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.

There are no connections with other systems, sharing is a manual process. OGC, Naval Criminal Investigative Service, Naval Inspector General, Naval Audit Service, Navy Office of the Judge Advocate General, USMC Staff Judge Advocate to the Commandant; as well as DON Civilian Personnel/Human Resources Offices, DON Management Officials at Commands.

[Empty box]

**Other DoD Components.**

Specify.

Offices of General Counsel, Judge Advocates, Inspector Generals, and DoD law enforcement, i.e. Army Criminal Investigative Division, Air Force Office of Special Investigations, and DoD's Defense Criminal Investigative Service. (Manual exchange only)

**Other Federal Agencies.**

Specify.

Department of Justice (Manual exchange only)

**State and Local Agencies.**

Specify.

[Empty box]

**Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

OSUM Solutions - SOW addresses PII, each contractor employee signs a non-disclosure agreement that requires protection of PII, and each contractor employee is required to attend PII training. Contractor personnel shall at all times comply with federal, DOD, and DON information assurance statutes, regulations, and policies. This includes the Privacy Act, Title 5, U.S.C., Section 522a and other related privacy policies, rules, and regulations. The FAR Privacy Clauses are included in the current contract.

**Other** (e.g., commercial providers, colleges).

Specify.

[Empty box]

**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.

For organizational personnel data, individuals can appeal the collection of data to the Deputy General Counsel.

ADR management personnel may object to the collection of information identifiable to them. In such cases the ADR event may be scheduled using other means, and the individual may be identified as "Anonymous" or a pseudonym may be used for case management purposes.

For some categories of information an individual employee can refrain from providing information; e.g., personal profile in Web 2.0 area of the information system. For some information fields within the organizational management area, the individual can refrain from providing information (non-mandatory fields of data). For online forms and surveys, an individual is provided with a privacy alert and a choice of whether to provide PII for a specific use.

Individuals involved in mediations may elect not to provide identifying information in which case their cases will be assigned anonymous identities. Mediators can decline to provide qualifying information at the risk of not being certified as a mediator.

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

[Empty box]

**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.

Information is used for litigation, fraud cases, and related law enforcement matters where OGC is not the collecting agency.

**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.

Provided on web site.



**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.**