



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Naval Inspector General Hotline Tracking System (NIGHTS)
--

Department of the Navy - DON/AA - NAVIG

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
- 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

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

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. 5014, Office of the Secretary of the Navy
10 U.S.C. 5020, Naval Inspector General: details; duties
SECNAVINST 5430.57 series, Mission and Functions of the Naval Inspector General
SECNAVINST 5370.5 series, DON Hotline Program
E.O. 9397 (SSN), as amended

Other authorities:

Statutory (Title 5 - DoD Hotline Program)

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 Naval Inspector General Hotline Tracking System (NIGHTS) is an enterprise case management system that facilitates the efficiency and effectiveness of the DoN Hotline program and its relevance to Navy leadership. NIGHTS supports important Secretary of the Navy (SECNAV), Chief of Naval Operations (CNO) and Department of Defense (DoD) initiatives. It also provides improvements in matters of Navy and DoD Hotlines, Congressional inquiries, Whistleblower, Procurement Fraud, and Senior Navy Official investigations. Implementation of NIGHTS resulted in the termination of more than 300 separate hotline investigation tracking and management programs across the Navy and Marine Corps Intranet (NMCI), some of which were non-NMCI compliant legacy systems. Equally important, NIGHTS enables the management's critical task of capturing data and metrics needed to identify, rectify, and manage areas of risk in a timely and responsive manner.

The types of personal information about individuals collected in the system are as follows:

Name (Last, First and middle if known), full SSN required for only those Department of Navy subjects that result in full investigations, personal cell phone number, home telephone number, personal e-mail address, home address and employment information.

In addition, unsolicited PII collected as part of an interview may become part of the record.

(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.). Because of this possibility, access is limited to officials/employees of the office who have a need to know. Files are stored in locked cabinets and rooms in a building with controlled access. Computer files are protected by software systems which are Common Access Card (CAC) protected, account restricted.

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.

Inspectors General staff at all Echelon II commands and below, Chief of Naval Personnel Selection Boards, NCIS, SECNAV, CNO, Commandant of the Marine Corps, Commanding Officers, HR and legal office personnel.

Other DoD Components.

Specify.

DOD IG, SECDEF, DOD OGC, DOD P&R, FOIA and PA offices

Other Federal Agencies.

Specify.

FBI, OLA, Congress, OPM, OSC, OSHA, DOL, GAO and other federal law enforcement agencies

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.

Individuals are provided the opportunity to object to the collection of PII during interview(s).

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

If the individuals fail to provide PII when requested, the minimally required PII is obtained via other means (i.e. DoD Employee Interactive Data System & Electronic Military Personnel Record System).

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.

Individuals are provided the opportunity to consent to the specific uses of their PII during interview(s). If the individuals fail to provide PII when requested, the minimally required PII is obtained via other means (i.e. DoD Employee Interactive Data System & Electronic Military Personnel Record System).

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 hard copy of the Privacy Act Statement is given to individual at the time of collection.

Sample Privacy Act Statement

AUTHORITY: Title 10, U.S. Code, Sections 5014 and 5020

PURPOSE: To determine the facts and circumstances surrounding allegations or complaints against Naval personnel and/or Navy/Marine Corps activities. To present findings, conclusions, and recommendations developed from investigations and other inquiries to the Secretary of the Navy, CNO, CMC, or other appropriate Commanders. Disclosure of Social Security Account Number is voluntary, and if requested, is used to further identify the individual providing the information.

ROUTINE USES: The information is used for the purpose set forth above and may be:

- Forwarded to Federal, State, or local law enforcement agencies for their use;
- Used as a basis for summaries, briefings, or responses to Members of Congress or other agencies in the Executive Branch of the Federal Government;
- Provided to Congress or other Federal, State, and local agencies, when determined necessary.

MANDATORY OR VOLUNTARY DISCLOSURE AND EFFECT ON INDIVIDUAL NOT PROVIDING INFORMATION:

For Military Personnel: Disclosure of personal information is mandatory and failure to do so may subject the individual to disciplinary action.
For Department of the Navy Civilians: Failure to disclose personal information in relation to individual's position responsibilities may subject the individual to adverse personnel action.
For All Other Personnel: Disclosure of personal information is voluntary and no adverse action can be taken against individuals for refusing to provide information about them.

ACKNOWLEDGMENT

I understand the provisions of the Privacy Act of 1974 as related to me through the foregoing statement.

Signature: _____
Date: _____

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.