



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Naval Audit Service Information Management System (NASIMS)
--

Department of the Navy - DON/AA - NAVAUDSVC

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
- 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.

10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness;
10 U.S.C. 5013, Department of the Navy;
10 U.S.C. 5014, Office of the Secretary of the Navy;
10 U.S.C. 5041, Headquarters, Marine Corps;
5 U.S.C. 301, Departmental Regulations;
E.O. 9397 (SSN), as amended;
DoD Directive 8320.1, DoD Data Administration;
DoD Manual 7600.7-M, DoD Audit Manual; and
SECNAVINST 7510.7F, Department of the Navy Internal Audit.

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.

NASIMS is a web-based query and reporting application which serves the Naval Audit Service. NASIMS tracks and manages information used to manage and produce corporate metrics. It is an integrated corporate management system linking all functions of the Naval Audit Service, which will increase the effectiveness and efficiency of the overall organizational management. NASIMS provides internal controls over management requirements by creating workflows that integrate all functions of the audit service when specific actions take place.

NASIMS information is used to maximize staff resources and to provide project cost summary data; to track audit milestones and staff hours allocated towards project preparation and active projects which will allow for more effective scheduling of unassigned personnel and to categorize indirect time expended for end-of-year reporting; to plan workloads, to assist in providing time and attendance to the centralized payroll system; and to request, schedule, and track auditor training requirements established by the Generally Accepted Government Auditing Standards.

Race, gender, photograph, entered on duty date, position, directorate, division, team, pay plan, pay grade, series, security clearance, location, room, Electronic Data Interchange Personal Identifier (EDIPI), first name, last name, middle name, nickname, last four digits of Social Security Number (SSN), birth date, home address, mailing address, work cell phone number, work e-mail address, personal e-mail address, work phone number, home phone number, personal cell phone number, emergency contact name, emergency contact home phone number, emergency contact cell phone number, emergency contact work phone number, and education information.

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

Administrative: Access to NASIMS is controlled by Common Access Card (CAC) authentication. Naval Audit Service personnel are assigned roles which control the level of information a user can view and actions the user can perform within NASIMS. Individuals assigned to the HR Admin role will add employee's profile information into the system. When the user visits the NASIMS URL the system verifies the individual based on the CAC credentials against the new profile created by the HR Admin. Upon successful verification, the employee's EDIPI is associated with that employee's profile. NASIMS users are restricted to viewing/editing records controlled by their predetermined roles within the system; however, all users are able to view certain organizational information required for internal government operations (name, office location, office phone, office email, etc.). NASIMS administrators have access (view and edit) to all NASIMS records.

Technical: NASIMS data is stored on a database server. An end user, using their web browser, will pass through a firewall to the web server. The web server will interface with the database server, process the transaction, and pass data back to the end user's browser. Development and test web and database environments are also used throughout the change management process to test system upgrades before changes are made to the production (live) servers. Access to NASIMS will be controlled by CAC authentication. NASIMS users are authenticated by using their EDIPI (from CAC) and a database record to match. Any invalid attempts to access the application are recorded by the system and unauthorized users are denied access. All transactions are encrypted using Secure Sockets Layer (SSL).

Physical: All personnel entering the building must have appropriate identification, visitors are escorted. Server room is secured and access is restricted to authorized personnel only, visitors are escorted. Servers require login account credentials or other privileged authentication and access is limited to approved administrators.

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.

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.

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 can object to the collection of PII by declining to provide the information. However, failure to provide or update information may require manual HR processing or HR entering information from another authorized System of Record on behalf of the Naval Audit Service workforce member. All requested data (e.g., last four digits of SSN, entered on duty date, security clearance, and emergency contact) is available from other authorized Systems of Records. Additionally, failure by any Naval Audit Service workforce member to either provide or verify the accuracy of NASIMS data may result in employees or their emergency POCs not being contacted in the event of mustering, emergencies, or other work or personal planning outcomes.

(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.

Collected data is utilized for mission essential reporting; PII is collected and maintained for the purpose of effectively and efficiently managing the personnel and administrative functions of the agency.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- | | |
|--|--|
| <input checked="" type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input checked="" type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

NASIMS login page contains a Privacy Act Statement that informs the user of the authority, purpose, routine uses for the collection of PII and a disclosure statement regarding the collection mandate status and possible consequences of non provision. Further, every web page displaying the PII collected actively displays the following Privacy Banner: This system contains privacy sensitive information that requires protection for unauthorized disclosure. Do not disseminate information from this system to anyone who does not have an official need for access.

The Privacy Act Statement reads:

PRIVACY ACT STATEMENT

Authority: 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 5013, Department of the Navy; 10 U.S.C. 5014, Office of the Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; 5 U.S.C. 301, Departmental Regulations; E.O. 9397 (SSN), as amended; DoD Directive 8320.1, DoD Data Administration; DoD Manual 7600.7-M, DoD Audit Manual; and SECNAVINST 7510.7F, Department of the Navy Internal Audit.

Purpose: To collect personal and work-related information necessary to manage, supervise, and administer all aspects of the Naval Audit Service and contact members of the workforce.

Routine Uses: The DOD "Blanket Routine Uses" set forth at the beginning of the Department of the Navy's compilation of record system notices apply to this system of records. Information collected is available to Naval Audit Service personnel with an official "need-to-know". Work contact information is available to the entire Naval Audit Service workforce. Administrative personnel will have access for purposes of maintaining the NASIMS database.

Disclosure: Voluntary. However, failure to provide or update information may require manual HR processing or HR entering information from another authorized System of Record on behalf of the Naval Audit Service workforce member. All requested data (e.g., last four digits of SSN, entered on

duty date, security clearance, and emergency contact) is available from other authorized Systems of Records. Additionally, failure by any Naval Audit Service workforce member to either provide or verify the accuracy of NASIMS data may result in employees or their emergency POCs not being contacted in the event of mustering, emergencies, or other work or personal planning outcomes.

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.