

PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Scalable Workforce Automation Tool (SWAT)

2. DOD COMPONENT NAME:

Department of the Navy

3. PIA APPROVAL DATE:

03/06/20

NAVWAR - NIWC Atlantic

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: foreign nationals are included in general public.)

- | | |
|---|---|
| <input type="checkbox"/> From members of the general public | <input checked="" type="checkbox"/> From Federal employees and/or Federal contractors |
| <input type="checkbox"/> From both members of the general public and Federal employees and/or Federal contractors | <input type="checkbox"/> Not Collected (if checked proceed to Section 4) |

b. The PII is in a: (Check one)

- | | |
|--|---|
| <input type="checkbox"/> New DoD Information System | <input type="checkbox"/> New Electronic Collection |
| <input checked="" type="checkbox"/> Existing DoD Information System | <input type="checkbox"/> Existing Electronic Collection |
| <input type="checkbox"/> Significantly Modified DoD Information System | |

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

The Scalable Workforce Automation Tool (SWAT) is used to configure, develop, and support the integration of the Naval Information Warfare Center (NIWC) Atlantic Command's business processes by automating the data flow through each of the business process and alleviate the work flow burden on the workforce. The Command will be documenting the required data elements within the processes and tools in order to optimize the process to the greatest extent possible.

SWAT will draw data from multiple authoritative and local data sources to meet the Command requirements and address key performance indicators. SWAT is to provide a single point of data entry and viewing, allowing the data elements to move seamlessly between personnel and systems, decreasing the need for multiple manual data entry points and giving visibility to where actions are in process. For example, these data sources include, but are not limited to, an analytical/business intelligence suite, transactional data store, and multiple elements of local data (e.g., PDF, Excel, and Word files). SWAT will include an objectively documented analysis, comparison of alternatives and recommendation to address certain deficiencies with data workflow across the Command, initially focused on contract strategy through advanced planning and human resources processes with pertinent authoritative sources required to present an accurate assessment of the Command's contribution to current readiness and the correct application of Working Capital Fund resources to Naval priorities.

The PII in SWAT will be used within the Command on a need to know basis (e.g., their deputies as authorized by the local human resources organization with a signed Nondisclosure Agreement) and human resources personnel responsible to manage or track employee qualifications and credentials such as: Education, Experience, Cyber Security Workforce and Defense Acquisition Workforce.

Access to this information is controlled within SWAT. Supervisors or Managers can only view detailed information related to the employees they are responsible for. NIWC Atlantic contractors, including those persons charged to maintain the system or who have access to the data and prepare management reports, must first sign a Nondisclosure Agreement before being given access to SWAT.

PII used to address the data work flow across the Command includes:

Person's name, SSN, employment information, official duty address and alternate work addresses, work e-mail address, work related education information, official duty telephone numbers, duty position/title, military rank or government series and grade, security information including security clearance, DoD ID Number, billet number, employee ID number from source system(s), employee series and grade, date reported to command, duty station, work location, organizational code, organizational group, supervisor and their contact numbers, position title and pay plan, scheduling (hours per project), overseas tour begin and end date, number of years at current position or current tour end.

Job specific education includes:

Defense Acquisition Workforce coursework planned or completed, position level and continuous learning points required, Cyber Security Workforce membership including credentials, certifications held, and expiration date; contracting officer's representative status, certifications achieved, demonstrated proficiency levels earned under internal competency development model, projects or portfolio work assigned, credentials held on entry to the mid-career leadership program, security information to include clearance held, award(s); education information including college courses applied for, college degrees held and institutions attended, professional certifications held; employee promotion(s).

Contractor's information, including user account information in Navy ERP by name and unique ID, government sponsor, and whether they are a current member of the command's Cyber Security Workforce for reporting purposes.

The following unique identifiers come from the source system(s) (i.e. Data Warehouse Business Intelligence System (DWBIS), Business Portfolio Mapping Module (BPMM) and Lightweight Directory Access Protocol (LDAP)) and are needed for computer matching:

- Navy ERP unique Identifier Personnel Number (PERNR) for civilians, military and contractors, including names.
- Total Workforce Management Services (TWMS) System unique Identifier for civilians, military and contractors, including names.
- Total Force Manpower Management System (TFMMS) unique Identifier and Billet Identification Number (BIN) for each civilian including name.
- DoN Director, Acquisition Career Management (eDACM), for civilians, military and contractors, including names.
- Defense Civilian Personnel Data System (DCPDS), unique identifier and Billet Identification Number (BIN) for each civilian including name.
- Navy Enlisted System (NES) unique Identifier for military, including names.
- Officer Personnel Information System (OPINS) unique Identifier for military, including names.
- DoD Common Access Card Electronic Data Interchange Personal Identifier (DoD ID) unique identifier, for civilians, military and contractors, including names.
- Business Portfolio Mapping Module (BPMM) unique Identifier for civilians, military and contractors, including names and position/titles.
- SPAWAR Directory Services (LDAP) unique Identifier as a crosswalk for the above for civilians, military and contractors, including names.

d. Why is the PII collected and/or what is the intended use of the PII? (e.g., verification, identification, authentication, data matching, mission-related use, administrative use)

Administrative Use

e. Do individuals have the opportunity to object to the collection of their PII? Yes No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

PII is not collected directly from the individual.

f. 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.

PII is not collected directly from the individual.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. (Check as appropriate and provide the actual wording.)

Privacy Act Statement Privacy Advisory Not Applicable

PII is not collected directly from the individual.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? (Check all that apply)

Within the DoD Component

Specify.

Naval Information Warfare Center (NIWC) Atlantic (i.e., government supervisors and managers with a need to know (or their deputies as authorized by the local human resources organization with a signed Nondisclosure Agreement) and human resources personnel responsible to manage or track employee qualifications and credentials such as: Education, Experience, Cyber Security Workforce and Defense Acquisition Workforce.

Other DoD Components

Specify.

Other Federal Agencies

Specify.

State and Local Agencies

Specify.

Contractor (Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)

Specify.

ISHPI Information Technologies Inc.

Support contractors must comply with all privacy protections under the Privacy Act when accessing PII. The following contract clauses are incorporated into the base contract or task order in accordance with DoN CIO Privacy Tip "Rules for Handling PII by DON Contractor Support Personnel" by the DON Privacy Team - Published, March 10, 2011: 52.224 - 1 - Privacy Act Notification, 52.224 - 2 - Privacy Act and FAR 39.105.

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

Specify.

i. Source of the PII collected is: (Check all that apply and list all information systems if applicable)

Individuals

Databases

Existing DoD Information Systems

Commercial Systems

Other Federal Information Systems

Source systems are as follows:

Data Warehouse Business Intelligence System (DWBIS)

Business Portfolio Mapping Module (BPMM)

SPAWAR Directory Services Lightweight Directory Access Protocol (LDAP)

j. How will the information be collected? (Check all that apply and list all Official Form Numbers if applicable)

E-mail

Official Form (Enter Form Number(s) in the box below)

Face-to-Face Contact

Paper

Fax

Telephone Interview

Information Sharing - System to System

Website/E-Form

Other (If Other, enter the information in the box below)

k. 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 must be consistent.

Yes No

If "Yes," enter SORN System Identifier

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcl.d.defense.gov/Privacy/SORNs/>
or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

I. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority.

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

SWAT does not contain or create record data.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statute or Executive Order.

- (1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.
(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

SORN N05220-1, Data Warehouse Business Intelligence System (DWBIS) (December 23, 2015, 80 FR 79869), authorities: 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C Chapter 87, Defense Acquisition Workforce; DoD 5200.2-R, Department of Defense Personnel Security Program; DoDD 8570.1-M, Information Assurance Workforce Improvement Program; and SECNAV M-5510.30, Department of Navy Personnel Security Program.

SORN N05230-1, Total Workforce Management Services (TWMS) (October 20, 2010, 75 FR 64715), authorities: 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; CNICINST 5230.1, Total Workforce Management Services; OPNAVINST 3440.17, Navy Installation Emergency Management Program and E.O. 9397 (SSN), as amended.

Other authorities: DoD Instruction 5000.66, Defense Acquisition Workforce Education, Training, Experience, and Career Development Program; DoD Manual (DoDM) 5200.02, Procedures for the DoD Personnel Security Program (PSP); SECNAV Manual (SECNAV M) 5239.2, DoN Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification Manual.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 No Pending

- (1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

The system does not collect or store information on members of the Public or Foreign Nationals.