

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:

Integrated Security Management Tool (ISMT)

2. DOD COMPONENT NAME:

Department of the Navy

3. PIA APPROVAL DATE:

10/28/19

NAVAIR - Naval Air Warfare Center Aircraft Division

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

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

- From members of the general public From Federal employees and/or Federal contractors
 From both members of the general public and Federal employees and/or Federal contractors Not Collected (if checked proceed to Section 4)

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

- New DoD Information System New Electronic Collection
 Existing DoD Information System Existing Electronic Collection
 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.

ISMT (Integrated Security Management Tool) is a web application that is designed to assist NAVAIR Security specialists and SME's in maintaining the health and compliance of Security products within an assigned Security Management Office (SMO), Business Unit (BU) or Organization. ISMT is a multi-user web/database application presenting operators with mostly real-time data including current transactions as they are input from other sources.

PII (personal information about individuals) is critical to the Personnel Security (PERSEC) module of ISMT. Dashboards of metrics and reports address "out of normal" trends and individual records so that the responsible NAVAIR security specialists can take needed corrective actions for both or either individual records or process areas which may require intervention. This module tracks and reports on security clearance status information by individual, unit, site, etc. in order to assist NAVAIR Security specialists in managing and maintaining the various security clearance process elements.

The personal information about individuals includes SSN, work contact information, and clearance status for all DoD civilian, military and contractor personnel under the "clearance oversight responsibility" of NAVAIR. Today much of this effort is done via a variety of excel spreadsheet reports and manual analysis. The data will be used for administrative purposes.

The PII, which is related to the administration of security clearances and monitoring of the clearance process, includes: SSN and EDIPI, addresses, telephone numbers (work and personal), employment and supervisor contact information, DOB and place of birth. The electronic collection consists of electronic database entries only and does not formally include any other records, forms, or hard-copies. The user's access to this information collection has a Privacy Act Statement displayed on the web page and each web page has an FOUO Privacy Sensitive label. This electronic collection has no original PII data (not collected directly from individuals) - all PII data can be reconstructed from external authoritative data sources.

Source systems of PII collected by ISMT are:

Electronic Questionnaire for Investigations Processing (eQIP)
Defense Information System for Security (DISS)/Joint Personnel Adjudication System (JPAS)
Defense Civilian Personnel Database System (DCPDS)/Total Workforce Management System (TWMS)

In the future, we will also require access to the new Defense Civilian Human Resources Management System (DCHRMS).

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)

Verification, Identification, Authentication, and Data matching of an individual for security clearance process oversight purposes.

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. NAVAIR 7.4 Security, NAWCAD 7.4 Security, 7.2 WARS (Data Warehouse)

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.

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

List of systems:
Electronic Questionnaire for Investigations Processing (eQIP)
Defense Information System for Security (DISS)
Joint Personnel Adjudication System (JPAS)
Defense Civilian Personnel Database System (DCPDS)
Total Workforce Management System (TWMS)
In the future, we will also require access to the new Defense Civilian Human Resources Management System (DCHRMS)

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)

Formal data exchange agreements (e.g. MOUs) between ISMT and DCPDS, eQip, and DISS.
eQIP - Web Service Call with returned data stored in the existing NAVAIR Data Warehouse
DCPDS - Existing NAVAIR Data Warehouse Extract
DISS/JPAS - Web Service Call with returned data stored in the existing NAVAIR Data Warehouse

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://dpclld.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.

l. 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.

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.

DMDC 12 DoD, Joint Personnel Adjudication System (JPAS), (September 18, 2019; 84 FR 49101), authorities: 5 U.S.C. 9101, Access to Criminal History Information for National Security and Other Purposes; 10 U.S.C. 137, Under Secretary of Defense for Intelligence; DoD Directive 1145.02E, United States Military Entrance Processing Command (USMEPCOM); DoD 5200.2R, DoD Personnel Security Program (PSP); DoD 5105.21, Sensitive Compartment Information Administrative Security Manual; DoD Instruction (DoDI) 1304.26, Qualification Standards for Enlistment, Appointment and Induction; DoDI 5200.02, DoD Personnel Security Program (PSP); DoDD 5220.6, Defense Industrial Personnel Security Clearance Review Program; DoDI 5220.22, National Industrial Security Program (NISIP); Homeland Security Presidential Directive (HSPD) 12, Policy for Common Identification Standard for Federal Employees and Contractors; and E.O. 9397 (SSN), as amended.

DPR 34 DoD, Defense Civilian Personnel Data System (November 15, 2010, 75 FR 69642), authorities: 5 U.S.C. 301, Department Regulations; 5 U.S.C. Chapter 11, Office of Personnel Management; 5 U.S.C. Chapter 13, Special Authority; 5 U.S.C. Chapter 29,

Commissions, Oaths, Records, and Reports; 5 U.S.C. Chapter 31, Authority for Employment; 5 U.S.C. Chapter 33, Examination, Selection, and Placement; 5 U.S.C. Chapter 41, Training; 5 U.S.C. Chapter 43, Performance Appraisal; 5 U.S.C. Chapter 51, Classification; 5 U.S.C. Chapter 53, Pay Rates and Systems; 5 U.S.C. Chapter 55, Pay Administration; 5 U.S.C. Chapter 61, Hours of Work; 5 U.S.C. Chapter 63, Leave; 5 U.S.C. Chapter 72, Antidiscrimination; Right to Petition Congress; 5 U.S.C. Chapter 75, Adverse Actions; 5 U.S.C. Chapter 83, Retirement; 5 U.S.C. Chapter 99, Department of Defense National Security Personnel System; 5 U.S.C. 7201, Antidiscrimination Policy; minority recruitment program; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; E. O. 9830, Amending the Civil Service Rules and Providing for Federal Personnel Administration, as amended; 29 CFR part 1614.601, EEO Group Statistics; and E. O. 9397 (SSN), as amended.

OPM/GOVT-9, File on Position Classification Appeals, Job Grading Appeals, Retained Grade or Pay Appeals, and Fair Labor Standard Act (FLSA) Claims and Complaints (October 01, 2013, 78 FR 60331), authorities: 5 U.S.C. 5103, 5112, and 5115 for classification appeals, 5346 for job grading appeals, and 5366 for retained grade or pay appeals; 29 U.S.C. 204(f) for FLSA claims and complaints; 31 U.S.C. 3702 for compensation and leave claims; and U.S.C. 5581, 5582, and 5583 and 38 U.S.C. 5122 for disputes concerning the settlement of the account for a deceased Federal civilian officer or employee.

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.

PII is not collected from members of the public.