

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:

Joint Worldwide Intelligence Communications System (JWICS)

2. DOD COMPONENT NAME:

Department of Defense Inspector General

3. PIA APPROVAL DATE:

06/05/2026

Mission Support Team, Office of the Chief Information Officer (OCIO)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)

- ☐ From members of the general public ☐ From Federal employees
- ☒ from both members of the general public and Federal employees ☐ 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.

The Joint Worldwide Intelligence Communications System (JWICS) enclave is an information technology (IT) infrastructure that provides end-to-end visibility and management of integrated augmentation processes and automated workflow in support of the DoD OIG's core mission functions. JWICS enables centralized distribution, tracking and accountability, and coordination of classified data. JWICS is accessible to authorized users, and provides a secure communication capability for transmission and receipt of Top Secret information. JWICS is an enclave that provides the underlying infrastructure and hosting services for components such as active directory services; assignment and management of security policies; and hosting and support for servers, network devices, user workstations, applications, to include TeamMate+, User Activity Monitoring (UAM), and Microsoft SharePoint and Outlook, printers, and copiers.

Certain hosted systems and applications within the enclave may collect, maintain, process, or disseminate PII. The purpose of the PII collection and use is governed by the PIA for the system that collects the PII.

The JWICS environment is used to access sensitive administrative and law enforcement records; draft and finalize classified documents; and communicate and transmit classified reports. Access to PII, when present within hosted content, is restricted to the minimum information necessary and is granted to only users with a validated need-to-know and appropriate access authorization.

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)

PII may be present within the JWICS enclave only when included in documents, case files, public website or work products stored or processed by hosted servers and applications. The intended use of PII is to enable official communications in a secure environment in support of the DoD OIG mission. All uses of PII are governed by individual PIAs that collect the PII where collection and use of such information are mandated by law, regulation, security policy or operations necessity.

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.

Individuals do not have the opportunity to object to the collection of their PII because any PII present within the JWICS environment is used to collaborate and coordinate administrative or investigative efforts. The opportunity to object to the collection of PII is governed by the individual PIAs for the systems that collect the PII.

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.

Individuals do not have the opportunity to consent to specific uses of their PII because any PII present within the JWICS environment is used to collaborate and coordinate administrative or investigative efforts. Specific use activities of PII within the JWICS environment are fundamental to the performance of a user's official duties. The opportunity to consent is governed by the individual PIAs for the systems that collect the PII.

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

JWICS is not intended to directly collect PII from members of the public; therefore, a PAS is not required for the environment itself.

However, JWICS provides infrastructure support for systems that do collect PII, such as those used for submitting and processing DoD Hotline complaints. When PII is collected for this purpose, the individual is presented with a PAS at the point of collection during the submission process. In this case, the applicable PAS is tied to the DoD Hotline complaint intake and case processing system, as documented in PIA-16, Defense Case Activity Tracking System Enterprise.

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

☒ Within the DoD Component	Specify.	DoW OIG employees with an established need-to-know and that require access for mission requirements.
☒ Other DoD Components (i.e. Army, Navy, Air Force)	Specify.	PII data is shared consistent with the Privacy Act, 5 U.S.C. 552a(b), Conditions of Disclosure.
☒ Other Federal Agencies (i.e. Veteran's Affairs, Energy, State)	Specify.	PII data is shared consistent with the Privacy Act, 5 U.S.C. 552a(b), Conditions of Disclosure.
☒ State and Local Agencies	Specify.	PII data is shared consistent with the Privacy Act, 5 U.S.C. 552a(b), Conditions of Disclosure.
☒ 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.	FAR privacy clauses 52.224-1, 52.224-2, and 52.224-3, Privacy Act Training apply.
☐ 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	

Hosted systems are TeamMate+, UAM, and Microsoft SharePoint and Outlook.

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)
☐ In-Person Contact	☐ Paper
☐ Fax	☐ Telephone Interview
☒ Information Sharing - System to System	☒ Website/E-Form
☐ Other (If Other, enter the information in the box below)	

JWICS utilizes system-to-system integration protocols at an elevated classification level. The method of collecting information through these integrations is addressed within the PIA of the system that collects the PII. JWICS itself does not perform direct collection of PII for its own purpose. The information collected through website/e-form supports the statutory requirement for processing administrative and investigative complaints.

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.

A SORN is not required as JWICS is an enclave and it is not an ordinary course of business to retrieve information using a personal identifier.

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.

N/A.

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

(3) Retention Instructions.

JWICS is not a system of records. It is an enclave and not a specific program.

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.

5 U.S.C. 4, Inspectors General.

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.

An OMB control number is not required as JWICS is an enclave and does not collect PII directly from any individual.