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:

DoD OIG Secret Internet Protocol Router Network (SIPRNet)

2. DOD COMPONENT NAME:

Department of Defense Inspector General

3. PIA APPROVAL DATE:

07/01/2025

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 DoD OIG SIPRNet is an IT infrastructure that provides end-to-end command visibility and control of integrated augmentation processes and automated workflow in support of the DoD OIG's core business functions. This includes centralized distribution, tracking and accountability, and data collection and coordination. SIPRNet is not public facing and allows for a secure communication capability for transmission and reception of sensitive secret information. SIPRNet is an enclave that provides the infrastructure and hosting services that include, but are not limited to, Active Directory services and assignment and management of security policies, computer servers, network devices, applications, user workstations, printers, and copiers.

SIPRNet does not collect, maintain, process, or disseminate personally identifiable information (PII). However, hosted systems and applications within the enclave may contain PII on documents stored in file servers and shared drives. SIPRNet currently hosts the following systems and applications: SharePoint, Share Drives, TeamMate+, and Microsoft Outlook. The process of collection, purpose, and the intended use of the PII is specific to a system component and is addressed in the hosted system's PIA.

The system has been used to maintain data containing details for accessing sensitive law enforcement documents; drafting and finalizing classified reports; and communicating and transmitting classified reports. The access level to PII is limited to the details necessary to determine employee access and confirm their need-to-know.

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)*

SIPRNet does not collect, maintain, process, or disseminate PII. However, hosted systems and applications within the enclave may contain PII stored on file servers and shared drives. The process of collection, purpose, and the intended use of collected PII is specific to a system component and is addressed in the hosted system's PIA. PII may be used during the course of an employee's duties for verification, identification, authentication, data matching, and other mission-related and 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.

SIPRNet does not collect, maintain, process, or disseminate PII. However, hosted systems and applications within the enclave may contain PII on documents stored on file servers and shared drives. Individuals granted access to SIPRNet acknowledge and consent to routine intercepts and monitoring, inspection, and seizure of information within the enclave upon logging onto the system. DoD OIG personnel must complete IG Form 22, Network Access User Agreement - SIPRNet, and DD Form 2875, System Authorization Access Request (SAAR), prior to gaining access.

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.

SIPRNet does not collect, maintain, process, or disseminate PII. However, hosted systems and applications within the enclave may contain PII stored on file servers and shared drives.

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

SIPRNet does not collect PII directly from an individual to be stored in a system of records. Therefore, a Privacy Act Statement or Privacy Advisory is not required. However, hosted systems and applications within the enclave may contain PII stored on file servers and shared drives. The process of collection, purpose, and the intended use of collected PII is specific to a system component and is addressed in the hosted system's PIA.

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.	DoD 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.	Sharing is consistent with 5 U.S.C. 552a(b), Conditions of Disclosure.
☒ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	Sharing is consistent with 5 U.S.C. 552a(b), Conditions of Disclosure.
☒ State and Local Agencies	Specify.	Sharing is consistent with 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.	
☐ 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

Not applicable for the enclave; the source of the PII collected is specific to the information system component and is addressed in the hosted system's PIA.

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)*

Not applicable for the enclave; the source of the PII collected is specific to the information system component and is addressed in the hosted system's PIA.

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://dpcld.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 because SIPRNet does not collect or store information in a system of records. Furthermore, it is not an ordinary course of business to retrieve information using a personal identifier.

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. N/A.

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

(3) Retention Instructions.

SIPRNet 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 statue 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. 301, Regulations for the Government of the Department
5 U.S.C. Chapter 4, Inspector General Act of 1978
10 U.S.C. 2222, Defense Business Systems
44 U.S.C. 3101, Records Management by Federal Agencies
Public Law 99-474, the Computer Fraud and Abuse Act of 1986
Executive Order 10450, Security requirements for Government Employment
DoD Instruction (DoDI) 5200.2, Personnel Security Program
DoDI 8500.1, Cybersecurity
DoDI 8520.03, Identity Authentication for Information Systems
DoD Directive 5015.2, DoD Records Management Program
IG Instruction (IGDINST) 5015.2, Records Management Program
IGDINST 8170.04, Government Furnished Electronic Devices

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 SIPRNet is an enclave and does not collect PII directly from any individual.