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 Information Technology Support (OIGITS) NIPRNet

2. DOD COMPONENT NAME:

Department of Defense Inspector General

3. PIA APPROVAL DATE:

11/09/20

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

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
- [x] 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
- [x] 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 Information Technology Support (OIGITS) is an IT infrastructure that provides enterprise wide authentication, messaging, backup, and recovery, file and print services, application hosting, enclave boundary security and obtain registration/provisioning data from the Joint Services Provider (JSP).

OIGITS serves a customer base for the DoD OIG and its field offices to include OCONUS. The OIGITS has the capabilities to capture individual's name, employment information, military records, electronic data interchange person identifier (EDIPI) (aka DoD ID number), rank, title, personnel type, DoD component, DoD sub-component, Non-DoD agency, position title, business email address, and display name(s), office commercial and Defense System Network (DSN) phone and business mobile phone numbers, Internet Protocol (IP) phones, business location and mailing addresses, distinguished name from source record(s), directory publishing restrictions, country of citizenship, US citizenship status, DoD job skill, reserve component code, billet code, and pay grade.

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 is collected for verification, identification, authentication, data matching, mission-related use and administrative use.

e. Do individuals have the opportunity to object to the collection of their PII? [ ] Yes [x] 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.

The data retained in OIGITS is provided via system-to-system interfaces. Individuals are added to the OIGITS when a NIPRNet Personal User Network Security Agreement (DD2875) is submitted.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [ ] Yes [x] 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.

The accredited system is the enclave not a specific program. In order to be granted access to OIGITS a NIPRNet Personal User Agreement must be submitted through NAAR. The NIPRNet Personal User Agreement does not contain a mechanism for individuals to limit use of PII and the data elements are 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.)*

- [x] Privacy Act Statement
- [ ] Privacy Advisory
- [ ] Not Applicable

The OIGITS does not collect this info directly from the individual, however the Privacy Act Statement applies when collection happens.

PRIVACY ACT STATEMENT AUTHORITY: Executive Order (EO) 10450, Security Requirements for Government Employment; EO 9397, Federal Agency Use of Social Security Numbers; and Public Law 99-474, the Computer Fraud and Abuse Act of 1986.
PURPOSE(S): To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to DoD systems and information. NOTE: Records may be maintained in both electronic and/or paper form.
ROUTINE USE(S): None.
DISCLOSURE: Voluntary; however, failure to provide the requested information may impede, delay, or result in denial of access to information technology systems.

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

[X]	Within the DoD Component	Specify.	All DoD OIG components that require access for mission requirements.
[X]	Other DoD Components	Specify.	OSD, Joint Chiefs of Staff, MCIOs, members of DoD law enforcement or auditing agencies, Military departments and combatant commands, Defense agencies.
[ ]	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)*

[X]	Individuals	[X]	Databases
[X]	Existing DoD Information Systems	[X]	Commercial Systems
[ ]	Other Federal Information Systems		

Individual DoD OIG information systems: CRIMS, DCATS, EARMS, DMEN, ETS, Contract Disclosure Program, Footprints, Defense Ready, Exchange NIPR, Internet DMA, Intranet Cold Fusion, Subpoena Program, Kiteworks, OIGnet, Sharepoint, Teammate NIPR

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

[X]	E-mail	[ ]	Official Form (*Enter Form Number(s) in the box below)*
[ ]	Face-to-Face Contact	[X]	Paper
[ ]	Fax	[ ]	Telephone Interview
[X]	Information Sharing - System to System	[X]	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 [X] 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 as it is not an ordinary course of business to retrieve information in OIGITS by using PII.

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.

OIGITS 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.

The authority to collect information in this system derives from:

Executive Order 10450, "Security requirements for Government Employees", April 27, 1953
DoD 5200.2-R, "Personnel Security Program", January 1, 1987

U.S. Code:
5 U.S.C. § 301, Regulations for the Government of the Department;
44 U.S.C. 3101 Records Management by Federal Agencies.

DoD Directives:
DoD Directive 5015.2, "DOD Records Management Program," August 17, 2017.

DoD IG Instructions:
IGDINST 5015.2, "Records Management Program," November 7, 2007.

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.

OMB Control number not required, OIGITS does not collect records from 10 or more members of the public.