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:

OIG Teammate+ (Teammate+)

2. DOD COMPONENT NAME:

Defense Counterintelligence and Security Agency

3. PIA APPROVAL DATE:

04/17/26

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.

TeamMate+ is utilized by the Office of the Inspector General Audits, Inspections, and Evaluations staff to plan, track, conduct, and uphold quality standards for internal audits and inspections, as mandated by Generally Accepted Government Auditing Standards (GAGAS) and the Council of the Inspector General of Integrity and Efficiencies (CIGIE). It is also utilized to track and report on external audits as required by the DCSA Director. Internal audits are conducted by the OIG audits team on internal DCSA directorates and processes to ensure agency compliance. External audits are conducted by non-DCSA agencies (such as GAO) on DCSA directorates and processes. The OIG audits team is responsible for overseeing the requests for information and collection of data, and responses to the requests on these external audits.

The software collects information regarding audits/inspections/evaluations of DCSA processes and procedures. The information is manually entered into the system by the OIG Audits, Inspections, and Evaluations staff. The system maintains names, titles, contact information, personal and facility clearances, and other identifiers (e.g., employee IDs) for personnel within OIG, DCSA, DoD, Federal Agencies, and members of the public to include clear industry (e.g., contractors) as part of the audit or inspection. For some audits, the information collected (i.e. audit sampling) could also include documents and names regarding background investigations, which would potentially include source names or other names listed on case papers. Audits/Inspection records are indexed/retrieved by inspection/audit number/name

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)*

The software collects PII information regarding audits/inspections/evaluations of DCSA processes and procedures.

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 ability to object directly to the use of PII within Teammate+. However, individuals provide consent/knowledge of the use of their PII during the initial collection of information from DCSA databases (e.g., DAI)

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 ability to consent directly to the use of PII within Teammate+. However, individuals provide consent/knowledge of the use of their PII during the initial collection of information from DCSA databases (e.g., DAI).

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

Individuals are not entering their information into the system directly, as PII is collected from other DCSA databases.

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.	Authorized OIG Employees
☐ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	
☐ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	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

Existing DCSA systems are the source of Teammate+ information which is gathered by the auditors. These systems include Defense Civilian Personnel Data System (DCPDS), Defense Agencies Initiative (DAI), Performance Assessment and Recognition System (PARS), Defense Travel System (DTS), National Industrial Security System (NISS), National Background Investigation Services (NBIS), and other personnel vetting systems.

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)*

Existing DCSA systems are the source of Teammate+ information (e.g., DCPDS, DAI, PARS, DTS, NISS, NBIS, other PV systems).

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. The system contains PII, however, records are not stored/retrieved by unique 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. DAA-GRS-2013-0005-0004 ; DAA-0446-2022-0002

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

(3) Retention Instructions.

Temporary. Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use.

Records are to be destroyed 10 years after date of final report or when all follow-up actions are completed, whichever is later.

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.

Authority to collect is on the DD Form 2875. Information is collected from users upon hire whether it be a Contractor or a Civilian. Administrators outside of this specific Information System use this information to create accounts within Active Directory. The information system specific administrators do not handle Active Directory. The IS is integrated with DCSA Database to collect PII information regarding audits/inspections/evaluations of DCSA processes and procedures.

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.

This collection is exempt due to the Inspector General Empowerment Act of 2016 (IGEA) exempts Offices of Inspectors General (OIGs) from the requirements of the Paperwork Reduction Act (PRA). OIGs no longer have to seek Office of Management and Budget (OMB) clearance when conducting surveys of the public as a part of their audit, investigation, inspection, evaluation, and other review work.