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:

Corporate Management Information Systems (CMIS)

2. DOD COMPONENT NAME:

Defense Information Systems Agency

3. PIA APPROVAL DATE:

05/21/24

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
- [x] 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
- [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.

DISA Manpower & Personnel Directorate (MPD) activities collect and maintain personal data for internal security and human resource management purposes and to meet agency reporting requirements. The system collects SSN, DoD ID number, names, addresses, grades, home phone numbers, areas of employment, supervisors and other information necessary to execute an effective human resource capability.

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 required for identification purposes for mission-related use only, verification, and authentication of the user of the CMIS modules. Identification and authentication is defined using of the PKI cert in conjunction with the DoD ID Number.

e. Do individuals have the opportunity to object to the collection of their PII? [x] 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 can object to the collection of their PII by not completing and submitting the information required.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [x] 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 can object to the specific uses of their PII by not completing and submitting the information required.

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

A "Privacy Act Statement" is affixed to each web-page where PII data is collected. Statement states "This system contains Privacy Act information, which is covered by the Privacy Act of 1974, as amended, 5 U.S.C. Section 552a, and it must be protected from unauthorized access or use. For Official Use Only (FOUO)."

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.	DISA Human Resources, Manpower and Security, DODNet-Unclassified Domain Services.
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	DFAS and DAU as appropriate
☐ 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.	Integral Federal, Inc. IAW FAR 52.212-4(C) DFARS 252.232-7007, FAR 52.212-4
☐ 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

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)*

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 DoD-0015/OPM/Govt1

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.

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. GRS 2.1, 2.2, 2.3, 2.4, 2.5, 2.7, 3.1, 5.3, 5.4

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

(3) Retention Instructions.

Human Resources Module Records
2.1

#20: Destroy 2 years after position is abolished or description is superseded, but longer retention is authorized if required for business use.
#21: Destroy in accordance with disposal instructions for associated file. (See GRS 2.2 section on OPFs.)
#22: Destroy when position description is final, but longer retention is authorized if required for business use.
2.2
#10: Destroy when 3 years old, but longer retention is authorized if required for business use.
#30: Destroy when 2 years old or 2 years after award is approved or disapproved, whichever is later, but longer retention is authorized if required for business use.
#41: Destroy when superseded or obsolete, or upon separation or transfer of employee, whichever is earlier.
#50: Destroy when business use ceases.
2.3
#10: Destroy when 3 years old, but longer retention is authorized if required for business use.
#90: Destroy 3 years after close of case, but longer retention is authorized if required for business use.
#100: Destroy 3 years after final resolution of case, but longer retention is authorized if required for business use.
2.4
#30: Destroy when 3 years old, but longer retention is authorized if required for business use.
2.5
#10: Destroy when no longer required for business use.
#20: Destroy 1 year after date of separation or transfer, but longer retention is authorized if required for business use.
2.7
#20: Destroy when 6 years old, but longer retention is authorized if needed for business use.
#63: Destroy when 3 years old.
#65: Destroy when 1 year old. For Federal Employees.
#66: Destroy when 30 days old. For Contractors and visitors.
5.3
#10: Destroy when 3 years old or 3 years after superseded or obsolete, whichever is applicable, but longer retention is authorized if required for business use.
5.5
#10: Destroy when 3 years old, or 3 years after applicable agreement expires or is canceled, as appropriate, but longer retention is authorized if required for business use.

Administrator Module - (Overview)
2.6
#10: Destroy when 3 years old, or 3 years after superseded or obsolete, whichever is appropriate, but longer retention is authorized if required for business use.
3.1
#20: 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.
3.2
#30: Destroy when business use ceases.
5.1
#10: Destroy when business use ceases.

Training Module - (Overview)
2.6
#10: Destroy when 3 years old, or 3 years after superseded or obsolete, whichever is appropriate, but longer retention is authorized if required for business use.
#30: Destroy when superseded, 5 years old, or 1 year after separation, whichever comes first, but longer retention is authorized if required for business use.
5.6
#20: Destroy 3 years after return of key, but longer retention is authorized if required for business use.

Travel, Military, and Security Resource modules
5.1
#10: Destroy when business use ceases.

Facilities Module
5.4
#10: Destroy when 3 years old or 3 years after superseded, as appropriate, but longer retention is authorized if required for business use.
#20: Transfer to new owner after unconditional sale or Government release of conditions, restrictions, mortgages, or other liens.

5.6
#20: Destroy 3 years after return of key, but longer retention is authorized if required for business use.
#40: Destroy 3 months after expiration or revocation, but longer retention is authorized if required for business use.
#80: Destroy 5 years after updating the security assessment or terminating the security awareness status, whichever is sooner, but longer retention is authorized if required for business use.

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.

Account must be provisioned via the On-Boarding Tool through IdM.
DoDI 1000.30 of 01 August 2012, Incorporating Change 2, November 30, 2022; The Privacy Act of 1974.

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 approval is not required in accordance with Section 8.b.11 of Enclosure 3 of DoD Manual 8910.01 - Volume 2. CMIS does not collect information directly from individuals therefore it does not require an OMB control number.