

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:

Data Center

2. DOD COMPONENT NAME:

Defense Commissary Agency

3. PIA APPROVAL DATE:

09/04/25

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
- ☐ 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
- ☒ 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 Data Center supports the installation, operation, maintenance, patching, mitigation and remediation of virtual and physical servers hosting DeCA business systems and various applications. Data Center provides storage, and backup and recovery operations for DeCA business systems.

Active Directory (AD) and DISA O365 are used to manage domain and email accounts. Personal Identifiable Information (PII) is collected from individuals during the on-boarding process and stored in AD for account creation. A mailbox is then created on the tenant and all user information is inputted into the DISA Global Address List (GAL). Specific server details are outlined below:

DISA O365 is a messaging platform that provides email, scheduling, and tools for custom collaboration and messaging service applications. The GAL is a built-in DISA O365 feature. AD stores data as objects and its integrated security enforces common access card (CAC) logon authentication for access. An object is a single element, such as a user, group, application or device such as a printer. User objects consist of PII collected from the user during on-boarding. The PII is used by DISA O365 to create email accounts and enable users to search the GAL.

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 identification and authentication purposes and domain/email account creation.

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.

PII is collected to create domain and email accounts during new employee on-boarding process with no opportunity to object. All employees are required to have domain and email accounts.

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.

PII is collected to create domain and email accounts during new employee on-boarding process with no opportunity to object. All employees are required to have domain and email accounts.

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

The purpose of the Privacy Act of 1974, United States Code, Section 552a, is to balance the federal government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use and disclosure of personal information about them.

The Privacy Act applies only to records about individuals maintained by agencies in the executive branch of the government. It applies to these records only if they are kept in a "system of records." A system of records is a group of records from which the information was retrieved by an individual's name, social security number, date of birth, or some other personal identifier.

If you are a current employee and wish to obtain records pertaining to yourself, you may submit a request under the Privacy Act. Follow the same filing procedures as for FOIA requests, except that no fees are assessed for search/ retrieval and review. Only reproduction costs may be assessed under the Privacy Act.

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

☒ Within the DoD Component

Specify. DeCA domain and email account users access GAL for official duties

☐ Other DoD Components

Specify.

☐ 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)

☒ Individuals

☐ Databases

☐ Existing DoD Information Systems

☐ Commercial Systems

☐ Other Federal Information Systems

PII is collected by HR during the on-boarding process. Data Center uses the PII to create a user domain and email accounts.

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)

☒ Face-to-Face 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 DISA K890.14

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpclld.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.

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.

GRS 5.5, Item 020, DAA-GRS-2016-0012-0002

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

N/A

(3) Retention Instructions.

This item includes employee directories containing information about employee locations in facilities and work phone numbers. Temporary: Destroy when 1 year old or when superseded or obsolete, whichever is applicable, but longer retention is authorized 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 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.

DoD Manual 1341.02, DoD Identity Management DoD Self-Service (DS) Logon Program and Credential provides procedures for DoD personnel identification.

DoD Instruction 5200.46, DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC) establishes policy, assigns responsibilities, and prescribes procedures for investigating and adjudicating CAC eligibility.

DoD Instruction 8520.03, Identity Authentication for Information Systems assigns responsibilities and prescribes procedures for implementing authentication of all entities to DoD Information systems.

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.

Only DeCA personnel access information and contacts created in the DeCA Enterprise GAL for communicating and conducting official business.