

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:

Enterprise Cloud Standard Services Stack (EC3S)

2. DOD COMPONENT NAME:

Defense Security Cooperation Agency

3. PIA APPROVAL DATE:

September 26, 2019

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 EC3S provides enterprise level shared services to DSCA virtual provide clouds (e.g., two cloud environments). The types of personal information about individuals are as follows:

Active Directory Information: First Name, Last Name, EPIDI, including Users Login and Passwords.

Reporting capability consisting of a table (Person) that receives data feeds from each DSAMS service database containing the following columns: User ID, Case Signatory, Service, Activity, Lease Signatory, Training PGM Coordinator, Point of Contact, Program Manager, POC Title, Training Track Organization, Program Manager, Person Middle Name, Person Phone Extension, Defense Switched Network ID, Case Manager, Finance Manager, Person Last Name, Person Nickname, Rank, International Phone, Person Phone, Person Communication Fax, Person Symbol, Person First Name, Person Last Name, Activity Site, Email Address, Person Role, Person Title, Date, Last Update, Create User ID, Last Update User ID, FBH Tool Name, and FBH User ID.

Hosting Platform: DSCA Public Website, Security Assistance Network (SAN), GlobalNet and Regional Center Persons Activity Management System (RCPAMS). Defer to each system's approved Privacy Impact Assessment (PIA) for the specific types of PII maintained within the respective systems.

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 PII is collected from users for purposes of identification and authentication.

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.

Employees implicitly consent to the capture and use of their PII at the time of employment. Upon the collection of personal information, the agency provides the employee with appropriate Privacy Act Statements and given an opportunity to object to any collection of PII at that time.

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.

Employees and other participants implicitly consent to the capture and use of their PII at the time of employment.

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

Upon the collection of personal information, individuals subject to the Privacy Act are provided appropriate Privacy Act Statements. For access, DD Form 2875, System Authorization Access Request (SAAR) is completed, and the form includes the following Privacy Act Statement:

Authority: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.

Purpose: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.

Routine Use: None.

Disclosure: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

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.

DSCA Headquarters and Defense Institute of Security Cooperation Studies (DISCS)

☒ Other DoD Components

Specify.

Security Cooperation Offices, Combatant Commands, Military Departments, Defense Finance and Accounting Services, DoD Schoolhouses, Regional Centers, and International Host Nation Organizations

☐ 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.

CONTRACTORS: 1) General Dynamics Information Technology, 2) Alion Sciences and 3) Information Gateway Inc.

The contracts contain provisions to ensure the confidentiality and security of PII are in place to manage PII in the workplace, including language addressing the completion of initial and annual privacy training for contractor employees. See Privacy Clauses 52.224-1, 52-224-2 and 52-224-3.

☒ Other (e.g., commercial providers, colleges).

Specify.

Amazon Web Services GovCloud

i. Source of the PII collected is: (Check all that apply and list all information systems if applicable)

- | | |
|--|---|
| <input checked="" type="checkbox"/> Individuals | <input type="checkbox"/> Databases |
| <input checked="" type="checkbox"/> Existing DoD Information Systems | <input type="checkbox"/> Commercial Systems |
| <input type="checkbox"/> Other Federal Information Systems | |

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

- | | |
|---|---|
| <input type="checkbox"/> E-mail | <input checked="" type="checkbox"/> Official Form (Enter Form Number(s) in the box below) |
| <input type="checkbox"/> Face-to-Face Contact | <input type="checkbox"/> Paper |
| <input type="checkbox"/> Fax | <input type="checkbox"/> Telephone Interview |
| <input checked="" type="checkbox"/> Information Sharing - System to System | <input type="checkbox"/> Website/E-Form |
| <input type="checkbox"/> Other (If Other, enter the information in the box below) | |

DD Form 2875

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.

Because EC3S is not a system of records for purposes of the Privacy Act, a SORN is not required to be published in the Federal Register.

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.

EC3S is not a single purpose system, and a records disposition is not required.

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.

10 U.S.C. 134, Under Secretary of Defense for Policy; DoD Directive 5105.65, Defense Security Cooperation Agency (DSCA); DSCA Security Assistance Management Manual, Chapter 10, International Training; DoD Directive 5132.03, DoD Policy and Responsibilities Relating to Security Cooperation; Army Regulation 12-15, SECNAVINST 4950.4B, AFI 16-105, Joint Security Cooperation Education and Training; Public Law 97-195, Foreign Assistance and Arms Export Act of 1961, as amended; E.O. 9397 (SSN), as amended; and E.O. 10450.

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 8810.01, 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.

The EC3S is not subject to the Paperwork Reduction Act (PRA) requirement and OMB approval because it is a cloud compute, storage, and network resource.