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 Classified Voice over IP (ECVOIP) Active Directory Lightweight Directory Service (ADLDS)

2. DOD COMPONENT NAME:

Defense Information Systems Agency

3. PIA APPROVAL DATE:

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 ECVOIP ADLDS server will provide two main functions: 1) provisioning users into the correct ECVOIP cluster as well as 2) provide authentication for the users to achieve single sign-on and Personal Identity Verification (PIV) compliance for softphones and operational administrators using the Security Assertion Markup Language (SAMLv2). The goal will be to provide authentication for users with PIV smartcards so that user passwords will not be transmitted between clients or servers.

The ECVOIP provisioning and authenticating services will collect filtered PII data from the IdSS covered in SORN K890.14. This data will include attributes such as: names, phone numbers, duty locations, email addresses, and user certificates.

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 ECVOIP ADLDS server will serve two functions: 1) provisioning users into the correct ECVOIP cluster as well as 2) provide authentication for the users to achieve single sign-on and Personal Identity Verification (PIV) compliance for softphones and operational administrators using the Security Assertion Markup Language (SAMLv2). The goal will be to provide authentication for users with PIV smartcards so that user passwords will not be transmitted between clients or servers.

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.

In order to have an ECVOIP device, users may not object to the collection of their PII. Users that do not wish to have an ECVOIP device, can indicate so, and their information will not be stored in the ECVOIP ADLDS database. This notification indicating they do not with to have their PII collected must notify/modify their MilConnect entries to leave the appropriate field(s) blank so that filters do not include the user during the scheduled system synchronizations. However, these fields are not yet determined.

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.

Once a user's data is pushed to the ECVOIP ADLDS servers, additional synchronizations will occur to the Cisco Call Managers and Cisco Prime Provisioning servers, but the filters associated with these synchronization agreements will not be customizable on a per-user basis. Individuals seeking to determine whether information about themselves is contained in this system of records can submit written inquiries to Defense Information Systems Agency (DISA), Services Directorate (SE), 6919 Cooper Ave., Fort Meade, MD 20755-7901.

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

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.	DISA administrators to the ECVOIP systems will be able to view a subset of user data (only users with a voice or video device provisioned in the ECVOIP architecture).
☒ Other DoD Components	Specify.	Mission Partner Local administrators with Cisco Prime Provisioning access will be able to view a subset of user data (only users with a voice or video device provisioned in the ECVOIP architecture and under that administrator's local jurisdiction).
☐ 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

The ECVOIP ADLDS obtains search results from the Identity Synchronization Service (IdSS) covered in the associated SORN K890.14.

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)*

The ECVOIP ADLDS will receive a push from the Identity Synchronization Service (IdSS) covered in the associated SORN K890.14.

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 K890.14 - Identity Synchronization Servic

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 5.2, Item 020

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

(3) Retention Instructions.

DAA-GRS2017-0003- 0002. Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, 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.

The authority allows DoD Unified Communications Enterprise Classified Voice over IP (ECVOIP) Active Directory Lightweight Directory Service (ADLDS) to collect the following data:

- 5 U.S.C. 301, Department Regulation.
- DoD Directive 5105.19, Defense Information Systems Agency (DISA).

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: 0704-0415; Expiration Date: None