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:

Zoom for Government

2. DOD COMPONENT NAME:

Defense Counterintelligence and Security Agency

3. PIA APPROVAL DATE:

04/16/26

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
- [x] 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.

The Zoom for Government Platform is a Zoom product offering for the US Federal community and is operated by US Persons only. The Zoom for Government Platform unifies cloud video conferencing, simple online meetings, and a software-defined conference room solution into one easy-to-use platform. The solution offers video, audio, and wireless screen-sharing across Windows, Mac, Linux, Chrome OS, iOS, Android, Blackberry, Zoom Rooms, and H.323/SIP room systems. Zoom for Government Products include:
1. Zoom Cloud Video Conferencing – a cloud-based collaboration service which includes video, audio, content sharing webinars and collaboration.
2. Zoom Phone - a cloud-based phone system with traditional PBX features, integrated PSTN connectivity, enhanced emergency services, and support for calling from mobile apps, desktop apps, and legacy desk phone devices.
3. Zoom Chat - send chat messages in public or private channels organized by projects, teams, or topics with the ability to share files, emojis, screenshots, and more.
4. Zoom Rooms – software-based group video conferencing for conference and huddle rooms that run off-the-shelf hardware including a dedicated MAC or PC, camera, and speaker with an iPad controller.
5. Zoom Room Connector – a gateway allowing H.323 and Session Initiation Protocol (SIP) systems to connect to Zoom meetings. Room Connector is available in both cloud computing and as software (VM) for installation on the customer premise.
6. Meeting Connector – a software (VM) version of the Zoom Cloud infrastructure intended for installation on the customer premise.
7. Zoom API - provides the ability for developers to easily add Video, Voice and Screen Sharing to your application. Our API is a server side implementation designed around REST. The Zoom API helps manage the pre-meeting experience such as creating, editing and deleting resources like users, meetings and webinars. Zoom for Government API documentation can be located at marketplace.zoomgov.com
8. Zoom Client – a local client that allows users to start/join a meeting, employ in-meeting controls for participants, hosts, and co-hosts, webinar controls, manage participants, share screen controls, chat, establish channels, add contacts, and modify settings.

Note: Data elements collected includes First/Last name, business or personal email address, phone number, passcode, and role. Zoom for Government is considered a PII system due to first/last name and email address are being used in Rev5 systems. However, information is not retrieved by the PII, so a SORN is not applicable.
Federal General Government Admin runs meeting reports to capture participants information, which would be maintained withing the appropriate system of record for the event (i.e., training).

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 collected by the Zoom for Government application is for mission-related and administrative use. The application does not have the capability to retrieve the PII. Users are only asked to provide PII (first name, last name, business email, personal email, phone number and passcode) to facilitate the identification and authentication of records. Add that The information is collected for application use/purpose. Not that individuals can decline to join meeting.

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.

Collected directly from the individual to attend the meeting.

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.

Collected directly from the individual to attend the meeting. However, circumstances in which the PII is processed does not provide significant or sensitive information about the individual.

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 [X] Not Applicable

Zoom for Government (ZoomGov) does not have its own Privacy Act statement because it is not considered a Privacy Act System of Records.

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)*

[X] Within the DoD Component	Specify.	DCSA- PII is based on invitees to meetings from organization(s) within these categories
[X] Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	PII is based on invitees to meetings from organization(s) within these categories
[X] Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	PII is based on invitees to meetings from organization(s) within these categories
[X] State and Local Agencies	Specify.	PII is based on invitees to meetings from organization(s) within these categories
[X] 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.	PII is based on invitees to meetings from organization(s) within these categories
[X] Other *(e.g., commercial providers, colleges).*	Specify.	PII is based on invitees to meetings from organization(s) within these categories

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

[X] Individuals
[ ] Databases
[ ] Existing DoD Information Systems
[ ] Commercial Systems
[ ] Other Federal Information Systems

PII is collected from the individual to facilitate the identification and authentication of users.

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
[X] Website/E-Form
[X] Other *(If Other, enter the information in the box below)*

collects first name, last name, business email, personal email, phone number and passcode from facilitator/participant

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.

Information is not stored in a way that can be retrieved by the PII, so a SORN is not applicable.

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-2016-0013-0002

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

(3) Retention Instructions.

Disposition: Temporary. Destroy when 5 years old, but longer retention is authorized if needed 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.

Authority to collect is on the DD Form 2875. Information is collected from users upon zoom for government account is created after receiving the meeting link sent via email whether it be a Contractor or a Civilian. Administrators outside of this specific Information System use this information to run meeting reports to capture participants' information. The information system specific administrators do not handle Active Directory. The IS is integrated with AWS Govcloud which is an IL4 system (CUI). User name and email address are entered when it is specifically told to do so for users to join meeting.)

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.

No OMB is required, only contact information is collected