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:

FULL CONTENT INSPECTION (FCI)

2. DOD COMPONENT NAME:

Defense Information Systems Agency

3. PIA APPROVAL DATE:

08/24/23

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

☐ 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

☐ 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.

FCITC is designed to provide services in place of the existing DISA provided Internet Access Point (IAP) to direct outbound DISA traffic directly from the FCITC to the Internet as well as provide an ingress point for DISA users to connect back into the DoDIN network when working remotely. Packet Capture (PCAP) data will contain PII information, should it be included in any packets that traverse the DoDIN, but it is not indexed or recoverable except by the packet header information. In other words, if the DoDIN captures PII data, the DoDIN is not associating it with an individual. That is not to say that the PCAP data may not have this other identifying information or that it may or may not be in the same index, but the indexing is not by individual. Indexing of packet capture data will be by the 5 tuple (source and destination IP address and port, plus protocol) along with a timestamp of the packet. Those fields serve as the index for information we use to correlate security incidents, not individual indicators such as name, DOB, etc.

Types of PII Potentially Collected during break and inspect: Biometrics, Citzenship, Dirver's License, Employment INformation, Home/Cell Phone, Mailing/Home Address, Military Records, Official Duty Address, Passport Information, Place of Birth, Race/Ethnicity, Records, Work E-mail Address, Birth Date, Disability Information, Education Information, Financial Information, Law Enforcement Information, Marital Status, Mother's Middle/Maiden Name, Official Duty Telephone, Personal E-mail Address, Position/Title, Rank/Grade Security Information, Child Information, DoD ID Number, Emergency Contact, Gender/Gender Identification, Legal Status, Medical Information, Name(s), Other ID Number, Photo Protected Health Information (PHI), Religious Preference, Social Security Number (SSN)

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 because the FCITC requires that DISA shall continue to work with mission partners to do comparative analysis to show that the FCITC capabilities (from boundary to host) provide “equal or better technical security and mission risk mitigation” than the NIPRNet. To meet those capabilities the FCITC must perform Break and Inspect and PCAP to protect the NIPRNET.

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.

The PII is collected because the FCITC requires that DISA shall continue to work with mission partners to do comparative analysis to show that the FCITC capabilities (from boundary to host) provide “equal or better technical security and mission risk mitigation” than the NIPRNet. In order to meet the capabilities of the NIPRNET the FCITC will be performing Break and Inspect and PCAP on all traffic they have DoD certifications for destined to the Internet or from Remote Access end users.

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.

The PII is collected because the FCITC requires that DISA shall continue to work with mission partners to do comparative analysis to show that the FCITC capabilities (from boundary to host) provide “equal or better technical security and mission risk mitigation” than the NIPRNet. In order to meet the capabilities of the NIPRNET the FCITC will be performing Break and Inspect and PCAP on all traffic they have DoD certifications for destined to the Internet or from Remote Access end users.

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

Authorities: Title 10 United States Code (U.S.C.) 9013, Secretary of the Air Force; 5 U.S.C. 301, Departmental Regulation; DoD Directive 5105.19, Defense Information Systems Agency (DISA).
Purpose: FCITC is designed to provide high performance internet services, remote access VPN, and IPSEC tunnels for DISA. The DoDIN requires Break and Inspect and Full Packet Capture of data that traverses the DoDIN if an end user is using one of these services.
Routine Use: To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.
To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.
In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.
To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. §§ 2904 and 2906.
To a Member of Congress or staff acting upon the Member’s behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.
To appropriate agencies, entities, and persons when (1) the DoD suspects or has confirmed that there has been a breach of the system of records; (2) the DoD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD’s efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.
To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government when necessary to accomplish an agency function related to this system of records.
Disclosure: Voluntary; however, failure to provide the information may result in a denial of service.

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
☒	Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify. DOD Components service users connecting to FCITC.
☐	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.
☐	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

DISA and DoD Service Users access the Internet, Remote VPN, and IPSEC tunnels at FCITC.

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

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.

Indexing of packet capture data will be by the 5 tuple (source and destination IP address and port, plus protocol) along with a timestamp of the packet. Those fields serve as the index for information DoDIN CNOSC personnel to correlate security incidents, and not individual indicators such as name, DOB, SSN, etc.

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 3.1 #10- DAA-GRS- 2013-0005- 0006
GRS 3.1 #11- DAA-GRS- 2013-0005- 0007
GRS 3.1 #40- DAA-GRS- 2013-0005- 0010
GRS 3.2 #10- DAA-GRS- 2013-0006- 0001
GRS 3.2 #30- DAA-GRS- 2013-0006- 0003

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

(3) Retention Instructions.

For 3.1 #10: Temporary. Destroy 5 years after project is terminated, but longer retention is authorized if required for business use.
For 3.1 #11: Temporary. Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use.
For 3.1 #40: Temporary. Destroy 5 years after the project/activity/transaction is completed or superseded, but longer retention is authorized if required for business use.

For 3.2 #10: Temporary. Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system.
For 3.2 #30: Temporary. Destroy when business use ceases.

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 following authority allows FULL CONTENT INSPECTION - TRINITY CYBER (FCITC) to collect the following data:
Title 10 United States Code (U.S.C.) 9013, Secretary of the Air Force;
5 U.S.C. 301, Departmental 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 approval is not required in accordance with Section 8.b.11 of Enclosure 3 of DoD Manual 8910.01 - Volume 2.