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:

NISP Central Access Information Security System (PS3)

2. DOD COMPONENT NAME:

Defense Counterintelligence and Security Agency

3. PIA APPROVAL DATE:

04/01/2026

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.

The Defense Counterintelligence and Security Agency (DCSA) National Industrial Security Program (NISP) Central Access Information Security System (NCAISS) program provides identity and access related functionality across DCSA's Information Technology (IT) infrastructure. NCAISS provides DCSA applications with Public Key Infrastructure (PKI)-based authentication services using the Common Access Card (CAC) or other Department of Defense (DoD)-approved PKI certificates, enhanced user account administration, and provisioning and de-provisioning capabilities. User's PKI and organization e-mail address are used in NCAISS as PII.

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)*

NCAISS authentication servers collect PII (First Name, Last Name, organization email address) for authentication purposes.

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.

During NCAISS account registration, users must assert that they have read the Privacy Act Statement (PAS) in order to submit their account request. Individuals may decline the PAS and collection of their PII; however, if a user doesn't consent to the Privacy Act Statement, their account request will not be completed.

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.

During NCAISS account creation, users must assert that they have read the Privacy Act Statement in order to submit their account request. The Privacy Act Statement outlines the Authorities, Purpose, Routine Use(s) and Disclosures for specific use of their PII within the system. The user has the opportunity to consent or decline; however, if a user does not consent to the PAS, their account request will not be completed.

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

Authority: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.
10 U.S.C. 2222; 10 U.S.C. 2224; 10 U.S.C. Chapter 8; 31 U.S.C. 902; OMB M-19-17; DoD Instruction 8320.02; DoD Instruction 8320.07; and DoD Instruction 8520.03.

Purpose: To record names; and Social Security Numbers 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 Uses: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records of information contained therein may specifically be disclosed outside DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows: To a Federal, State, or local law enforcement agency when your agency becomes aware of violation or possible violation of civil or criminal law; to the Department of Justice for purposes of representing the DoD in pending and potential litigation to which the record is pertinent; to the Merit systems Protection Board for the purpose of litigation or investigation of alleged or possible prohibited personnel practices; to a Federal agency when conducting an investigation or inquiry for security or audit reasons; or the General Services Administration in connection with its responsibilities for records management. A complete list of the Routine Uses and the full text of SORN DoD-0015 can be found at: https://www.federalregister.gov/documents/2022/12/16/2022-27356/privacy-act-of-1974-system-of-records

Disclosure: Disclosure of this information (to include social security numbers) is voluntary; however, failure to provide the requested information will impede, delay or prevent further processing of this request.

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.	DCSA (PEO, NISS)
☐ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	
☐ 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.	SAIC ONE IT - SAIC OneIT protects PII using the below FAR clauses within the contract: 52.224-1 Privacy Act Notification. As prescribed in 24.104 , Privacy Act Notification (Apr 1984) 52.224-2 Privacy Act. As prescribed in 24.104, Privacy Act (Apr 1984) 52.239-1 Privacy or Security Safeguards. As prescribed in 39.106 , Privacy or Security Safeguards (Aug 1996)
☐ 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

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 DoD-0015

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. N1-GRS-07-3, item 13b

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

(3) Retention Instructions.

Temporary. Destroy/delete when 7 years 6 months to 20 years 6 months old, based on the maximum level of operation of the appropriate CA and after the information record the PKI is designed to protect and/or access is destroyed according to an authorized schedule, or in the case of permanent records, when the record is transferred to NARA legal custody. Longer retention is authorized if the agency determines that transaction-specific PKI records are needed for a longer period.

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: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.
10 U.S.C. 2222, Defense Business Systems: Business Process Reengineering; Enterprise Architecture; Management; 10 U.S.C. 2224, Defense Information Assurance Program; 10 U.S.C. Chapter 8-Defense Agencies and Department of Defense Field Activities; 31 U.S.C. 902, Authority and functions of agency Chief Financial Officers; Homeland Security Presidential Directive (HSPD) 12, Policies for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; OMB M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management; National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors; DoD Instruction 8320.02, Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense; DoD Instruction 8320.07, Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense; and DoD Instruction 8520.03, Identity Authentication for 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.

The title for OMB Control Number 0705-0006 is the National Industrial Security System (NISS), which involves information collection for the Defense Counterintelligence and Security Agency (DCSA) to oversee the National Industrial Security Program (NISP); Expiration Date: May 31, 2028