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:

National Industrial Security System (NISS)

2. DOD COMPONENT NAME:

If Other, enter the Component name in the box below.

Defense Counterintelligence and Security Agency (DCSA)

3. PIA APPROVAL DATE:

03/28/23

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
- [x] 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
- [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.

NISS is DCSA's electronic repository of industrial security facility clearance information. NISS data is indexed and retrieved by the name or Cage code associated with a NISP facility and provides users with a nationwide perspective on NISP facilities as well as facilities under DCSA oversight in the DoD conventional Arms, Ammunition, and Explosives (AA&E) program. All industrial security personnel use NISS to track industrial security facility clearances and actions in connection with any NISP or AA&E facility. For Key Management Personnel (KMP) and for Culpable individuals involved in Security violations, NISS collects first, middle, and last name, SSN, date of birth, place of birth (city, state, country), citizenship data, and personnel security clearance information.

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)*

All industrial security personnel use NISS to track industrial security facility clearances and actions in connection with any NISP or AA&E facility.

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.

Participation in the NISP is voluntary. During system 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 uses of their PII within the system. If a user doesn't consent to the Privacy Act Statement, their account request will not be approved.

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.

During system account creation, users must assert they have read the Privacy Act Statement in order to submit their account request. The Privacy Act Statement outlines the specific uses for their PII information within the NISS system.

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.)*

- [x] Privacy Act Statement
- [ ] Privacy Advisory
- [ ] Not Applicable

Authority: E.O. 12829, National Industrial Security Program (NISP); 32 CFR Part 117, National Industrial Security Program Operating Manual; DoD Instruction 5220.22, National Industrial Security Program; and E.O. 9397 (SSN), as amended.

Purpose: The National Industrial Security System (NISS) maintains and processes unclassified company and personal information necessary to conduct the DCSA security oversight mission. It will provide the United States Government (USG) and Industry stakeholders with a data-driven, collaborative, capability to assess and mitigate the risk of the loss or compromise of classified information. DCSA is responsible for an industrial base of more than 12,000 cleared facilities, 40,000 classified information systems, and 900,000 cleared industry personnel.

Routine Uses: In addition to those disclosures generally permitted under 5 U.S.C. 552a (b) of the Privacy Act of 1974, as amended, the records contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552(b)(1) as follows:

To DCSA personnel for the purpose of being issued an Internal NISS user account, those individuals will have access to Personal Identification Data information.

To security and contracting personnel for other (non-DoD) Federal agencies, in connection with FCL Verification Requests, Facility Security Officer (FSO) name and telephone number will be available for any cleared company. Special requests for additional information may be made, and these requests will be coordinated and adjudicated in accordance with Agency standard procedures.

To security personnel working for cleared companies. Information in NISS regarding a particular cleared company will be available for review by authorized security personnel working for that company. Authorized personnel working for cleared companies who are verifying the facility clearances of other companies may obtain core facility information and FSO name and telephone number.

Disclosure: Voluntary; however, failure to provide all the data requested may result in our inability to maintain accurate historic facility security information, may slow down the performance against classified contracts and provides an area of error in the maintenance of transparency between Industry and Government stakeholders.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

[x] Within the DoD Component	Specify.	Authorized DCSA personnel may be issued an internal NISS user account; those individuals will have access to all Personal Identification Data (PID) Information. The primary user is the Industrial Security Program (ISP) for maintaining information of those facilities participating in the NISP.
[x] Other DoD Components	Specify.	Information provided to external users at a given facility will include KMP List and name/telephone/email of those persons associated with the facility. For general FCL information requests for all external users, FSO name and telephone number will be available for any valid company searched.
[x] Other Federal Agencies	Specify.	Information provided to external users at a given facility will include KMP List and name/telephone/email of those persons associated with the facility. For general FCL information requests for all external users, FSO name and telephone number will be available for any valid company searched.
[x] State and Local Agencies	Specify.	To any criminal, civil, security, or regulatory authority (whether Federal, State, territorial, local, or tribal) for the purpose of providing background search information on individuals for legally authorized purposes.
[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.	The contractors developing and sustaining this system may have access to PII for the purpose of operations and sustainment of the system, for no other use. Contractors who will be the users of the system will be provided notices regarding PII protections applicable to all users.
[ ] 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)*

- [x] Individuals
- [ ] Databases
- [x] 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)*

- [x] E-mail
- [x] Face-to-Face Contact
- [x] Fax
- [ ] Information Sharing - System to System
- [ ] Other *(If Other, enter the information in the box below)*
- [ ] Official Form (*Enter Form Number(s) in the box below)*
- [x] Paper
- [x] Telephone Interview
- [x] Website/E-Form

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
- [x] 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.

As discussed with the Program Managers of NISS, it was determined that the NISS IT system does not meet the definition of a Privacy Act System of Records; therefore there's no requirement to establish a NISS standalone System of Records Notice.
When data is retrieved from NISS, the records are not retrieved by PII of key management personnel. Data is only retrieved by company name or cage code associated with a NISP facility. Records are company based, and the data unique to key management personnel is contained within the company's record. There is no functionality in NISS to search by individual user information or SSN.
The NISS Privacy Impact Assessment was updated to reflect no SORN is required.

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-0446-2017-0001

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

(3) Retention Instructions.

Maintain at a minimum 6 months of activity data prior to archival. Archived data must preserve metadata, and the metadata must be linkable to archived data at all times in case of a system migration. All other data will be archived based on the DCSA retention policy for facility information.

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.

E.O. 12829, National Industrial Security Program (NISP); 32 CFR Part 117, National Industrial Security Program Operating Manual; DoD

Instruction 5220.22, National Industrial Security Program; and E.O. 9397 (SSN), as amended.

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: 0705-0006. Expiration Date: 02/29/2024