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:

05/27/20

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); DoD Manual 5220.22-M, 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 or individuals seeking employment opportunities requiring background checks.
[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 this system will not be furnished with PII. 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
- [X] Existing DoD Information Systems
- [ ] Other Federal Information Systems
- [ ] Databases
- [ ] Commercial Systems

Information is provided by security personnel at the facility or located in JPAS/DISS while conducting a search.

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
- [X] 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

Other: In addition to the above, information can be collected via the NISS itself.

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.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier V10-01 - Submitted to DPCLTD March 1

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. DAA-0446-2017-0001

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

(3) Retention Instructions.

Delete records/data when no longer needed.

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); DoD Manual 5220.22-M, 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.

[X] 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: 0704-0571. Expiration Date: 04/30/2021

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)***?** *(Check all that apply)*

☐ Biometrics	☒ Birth Date	☐ Child Information
☒ Citizenship	☐ Disability Information	☐ DoD ID Number
☐ Driver's License	☐ Education Information	☐ Emergency Contact
☒ Employment Information	☐ Financial Information	☐ Gender/Gender Identification
☒ Home/Cell Phone	☐ Law Enforcement Information	☐ Legal Status
☒ Mailing/Home Address	☐ Marital Status	☐ Medical Information
☐ Military Records	☐ Mother's Middle/Maiden Name	☒ Name(s)
☒ Official Duty Address	☒ Official Duty Telephone Phone	☐ Other ID Number
☐ Passport Information	☐ Personal E-mail Address	☐ Photo
☒ Place of Birth	☒ Position/Title	☐ Protected Health Information (PHI)[1]
☐ Race/Ethnicity	☐ Rank/Grade	☐ Religious Preference
☐ Records	☒ Security Information	☒ Social Security Number (SSN) *(Full or in any form)*
☒ Work E-mail Address	☐ If Other, enter the information in the box below	

If the SSN is collected, complete the following questions.

(*DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)*

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

☒ Yes ☐ No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

December 17, 2019
Cindy Allard; Chief, Defense Privacy, Civil Liberties, and Transportation Division

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

The Defense Privacy, Civil Liberties and Transparency Division (DPCLTD) has reviewed this request and has accepted your justification to use the SSN for the purpose of (3) Security Clearance Investigation or Verification, to verify contractors' eligibility for and ability to maintain facility security clearances. Also, Acceptable Use (11) Legacy System Interface, was accepted. NISS interfaces with the Defense Information System for Security (DISS) to create security violation incident reports.

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

DCSA will store all personally identifiable information (PII) electronically which has physical controls. The records are maintained in a controlled facility in servers located within the DCSA Data Center East. Access to the records is limited to person(s) responsible for servicing the record in performance of their official duties and who are properly screened and cleared for need-to-know. Physical entry is restricted by the use of Security Guards, Identification Badges, Key Cards, and Closed Circuit TV, and is only accessible to authorized personnel. Paper records are contained and stored in regulation safes/filing cabinets which are located in a Sensitive Compartmented Information Facility (SCIF) with limited access. Access to the NISS is restricted by User Identification, Intrusion Detection System, Encryption, Firewall, External Certificate Authorities, DoD Public Key Infrastructure Certificates and Common Access Card and PIN. The DCSA reviewed all of the safeguards established for the system to ensure they are compliant with The Department of Defense (DoD) requirements and are appropriate to the sensitivity of the information stored within the system, including the use of SSNs. The proposed specific routine uses have been reviewed to ensure the minimum amount of personally identifiable information shared has been established.

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

☒ Yes ☐ No

Access to the records is limited to person(s) responsible for servicing the record in performance of their official duties and who are properly screened and cleared for need-to-know. Physical entry is restricted by the use of Security Guards, Identification Badges, Key Cards, and Closed Circuit TV, and is only accessible to authorized personnel. Paper records are contained and stored in regulation safes/filing cabinets

which are located in a Sensitive Compartmented Information Facility (SCIF) with limited access. Access to the NISS is restricted by User Identification, Intrusion Detection System, Encryption, Firewall, External Certificate Authorities, DoD Public Key Infrastructure Certificates and Common Access Card and PIN.

b. What is the PII confidentiality impact level[2]? ☐ Low ☐ Moderate ☒ High

[1]The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2]Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

- ☐ Cipher Locks
- ☐ Combination Locks
- ☒ Key Cards
- ☒ Security Guards
- ☒ Closed Circuit TV (CCTV)
- ☒ Identification Badges
- ☐ Safes
- ☐ If Other, enter the information in the box below

The Primary system consists of servers located within the DCSA Data Center East, which has physical controls (e.g., security cards, restricted access) and virtual (e.g., encryption, firewalls) access control measures in place and is located at Telegraph Rd. Quantico, VA.

The back-up system consists of servers located within the DCSA Data Center West, which has similar physical and virtual access control measures in place and is located in Monterey, CA.

(2) Administrative Controls. *(Check all that apply)*

- ☒ Backups Secured Off-site
- ☒ Encryption of Backups
- ☒ Methods to Ensure Only Authorized Personnel Access to PII
- ☒ Periodic Security Audits
- ☒ Regular Monitoring of Users' Security Practices
- ☐ If Other, enter the information in the box below

(3) Technical Controls. *(Check all that apply)*

- ☐ Biometrics
- ☒ Encryption of Data at Rest
- ☐ Firewall
- ☒ Role-Based Access Controls
- ☐ Virtual Private Network (VPN)
- ☒ Common Access Card (CAC)
- ☒ Encryption of Data in Transit
- ☒ Intrusion Detection System (IDS)
- ☐ Used Only for Privileged (Elevated Roles)
- ☐ If Other, enter the information in the box below
- ☒ DoD Public Key Infrastructure Certificates
- ☒ External Certificate Authority Certificates
- ☒ Least Privilege Access
- ☒ User Identification and Password

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

Role Based Access Control. Risk Management Framework (RMF) Security Controls applied at High/High/Moderate categorizations.