# PRIVACY IMPACT ASSESSMENT (PIA)

## For the

| National Industrial Security System (NISS) |
| --- |
| Defense Security Service (DSS) |

## SECTION 1: IS A PIA REQUIRED?

**a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).**

☐ (1) Yes, from members of the general public.

☒ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

**b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.**

**c. If "Yes," then a PIA is required. Proceed to Section 2.**

## SECTION 2: PIA SUMMARY INFORMATION

**a. Why is this PIA being created or updated? Choose one:**

| | | | |
|---|---|---|---|
| ☒ | **New DoD Information System** | ☐ | **New Electronic Collection** |
| ☐ | **Existing DoD Information System** | ☐ | **Existing Electronic Collection** |
| ☐ | **Significantly Modified DoD Information System** | | |

**b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?**

| | | | |
|---|---|---|---|
| ☒ | **Yes, DITPR** | Enter DITPR System Identification Number | 14954 |
| ☐ | **Yes, SIPRNET** | Enter SIPRNET Identification Number | |
| ☐ | **No** | | |

**c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?**

☒ **Yes** ☐ **No**

**If "Yes," enter UPI** 007-000004700

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

**d. 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 should be consistent.

☒ **Yes** ☐ **No**

**If "Yes," enter Privacy Act SORN Identifier** TBD

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://dpcld.defense.gov/Privacy/SORNs.aspx

**or**

**Date of submission for approval to Defense Privacy Office**
Consult the Component Privacy Office for this date.

**e. Does this DoD information system or electronic collection have an 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**

**Enter OMB Control Number**

**Enter Expiration Date**

☒ **No**

**f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.**

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

DoD Instruction 5220.22, March 18, 2011
Executive Order 12829, National Industrial Security Program,January 6, 1993
Executive Order 9397

**g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.**

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

NISS will be the official DSS 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 DSS oversight in the DoD conventional Arms, Ammunition, and Explosives (AA&E) program. All industrial security personnel will use NISS to track industrial security facility clearances and actions in connection with any NISP or AA&E facility. For Key Management Personell (KMP) and for Culpable individuals involved in Security violations, NISS collects First, Middle, Last Name, SSN, Date of Birth, Place of Birth (City, State, Country), Citizenship Data, and Personnel Security Clearance information.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

DSS will enforce procedures, standards, and guidelines on privacy and confidentiality of PII collected and maintained by DSS and identify and afford security protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information collected and maintained by NISS.

The collection of PII poses an amount of risk based purely on the collection in electronic form. The amount of PII collected and maintained within the DSS NISS system is limited to SSN,Date of Birth, Place of Birth, Citizenship data of KMP, Facility Security Officer (FSO) and Communications Security COMSEC, Custodian and Alternate name and telephone number as well as the name and telephone number of the designated person for facility clearance requests. The privacy risk would include identification of individuals and its potential to subject an individual to identity theft. This risk is reduced by implementing strong security measures to protect PII information. In addition, all users are required to log into NISS utilizing their Common Access Card (CAC). Current or future security measures will not pose any risk to individual privacy information unless a decision is made to remove or reduce the existing security features. NISS utilizes role-based access which only grants users access to PII data to personnel with an official need to know in the performance of their official duties. The primary system consists of servers located within the DSS 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 DSS Data Center West, which has similar physical and virtual access control measures in place and is located in Monterey, CA.

In addition, NISS utilizes Role Based Access Controls. Risk Management Framework (RMF) Security Controls are applied at High/High/Moderate classification. The security controls and associated control assessment methods/procedures for NISS are provided by DISA eMASS. We perform a system assessment of each control during the ATO accreditation process. The PII and backup site are covered in the eMASS controls.

**h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)?** Indicate all that apply.

☒ **Within the DoD Component.**

Specify. Authorized DSS 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. NISS captures Name, SSN, Date of Birth, Place of Birth, Citizenship data of KMP, FSO and telephone number, as well as the name and telephone number of the designated person for facility clearance requests.

☒ **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.

☒ **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.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

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. Do individuals have the opportunity to object to the collection of their PII?**

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Participation in the NISP is voluntary. 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 Authorities, Purpose, Routine Use(s) and Disclosure for specific uses of their PII within the system. If an user doesn't consent to the Privacy Act Statement their account request will not be approved.

(2) If "No," state the reason why individuals cannot object.

j. **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.

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.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. **What information is provided to an individual when asked to provide PII data?** Indicate all that apply.

☒ **Privacy Act Statement** ☐ **Privacy Advisory**

☐ **Other** ☐ **None**

Describe each applicable format.

Notice: This is an Official U.S. Government internet system for authorized use only. Do not Discuss, Enter, Transfer, Process, or Transmit Classified/Sensitive National Security information of greater sensitivity than that for which this system is authorized. Use of this system constitutes consent to security testing and monitoring. All individuals are advised that system administrators may provide evidence of possible criminal activity identified during such monitoring to appropriate law enforcement officials. Unauthorized attempts to upload, download or change information is strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1987, the National Information Infrastructure Protection Act of 1996, and United States Code Title 18, Section 1030. Under the Privacy Act of 1974, individuals with access to NISS must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United State Code, Section 552a, Public Law 93-579, DoDD 5400.11, DoDD 5400.11-R and the applicable service directives. Information contained herein is exempt from mandatory disclosure under the FOIA. Exemption(s) 6 and 7c apply.

**NOTE:**

**Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.**

**A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.**