Defense Security Service (DSS)

Privacy Act of 1974; System of Records

AGENCY: Defense Security Service (DSS)

ACTION: Notice of a NEW System of Records.

SUMMARY: The Defense Security Service (DSS) is establishing the National Industrial Security System (NISS), a new system of records to replace the Industrial Security Facilities Database (ISFD) and Electronic Facility Clearance System (e-FCL).

DATES: This action will be effective without further notice on August 1, 2017 unless comments are received that would result in a contrary determination.

ADDRESSES: You may submit comments to Defense Security Service by contacting the DSS Privacy Act Officer, Defense Security Service, 27130 Telegraph Road, Quantico, VA, 22134; phone: 571-305-6740; email: stephanie.j.courtney.civ@mail.mil.

FOR FURTHER INFORMATION CONTACT: Email the Defense Security Service Industrial Security Field Operations (IO) Program Management Office (PgMO) team, Defense Security Service, 27130 Telegraph Road, Quantico, VA, 22134; email: dss.NISS@mail.mil.

SUPPLEMENTARY INFORMATION: As one of five Government Security Agencies directed to implement the National Industrial Security Program (NISP) per Executive Order 12829, Defense Security Service provides industrial security oversight and training to the Department of Defense (DoD) and thirty-one additional federal agencies. Administering the NISP to cleared contractors eligible to receive, handle, and protect classified information for DoD and the 31 agencies makes Defense Security Service responsible for an industrial base that includes over 12,000 cleared facilities, 40,000 classified information systems, and over 900,000 cleared industry personnel performing on multi-billion dollar annual investments by the United States Government. This capability bridges the foundational technology gap with the DSS risk-based approach to oversee protection of national security information with regards to development of our nation's most critical warfighter programs.

SYSTEM NAME AND NUMBER: National Industrial Security System (NISS) – V10-01

SECURITY CLASSIFICATION: Unclassified

SYSTEM LOCATION: Defense Security Service, 27130 Telegraph Road, Quantico, VA, 22134

SYSTEM MANAGER(S): Defense Security Service Data Center Operations, NISS System Manager, 27130 Telegraph Road, Quantico, VA, 22134, dss.quantico.dss-hq.list.mla-data-center-ops@mail.mil.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: DoD Instruction 5220.22, March 18, 2011; Executive Order 12829, National Industrial Security Program (NISP), January 6, 1993; and
Executive Order 9397.

PURPOSE(S) OF THE SYSTEM: NISS will be the official DSS electronic repository of industrial security facility clearance information and associated oversight activity. In addition to being a repository, it will streamline day-to-day business operations by automating several manual business processes.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals covered by NISS are government and industry personnel within the NISP. This includes DSS operational and support personnel; Government personnel performing facility clearance verification or sponsorship of contractors for facility clearances; and Industry personnel performing facility clearance verification, sponsorship of contractors for facility clearances, and oversight of security responsibilities executed by facility security staff.

CATEGORIES OF RECORDS IN THE SYSTEM: The following records are used for initiating and monitoring personnel security clearances and to evaluate cleared contractors compliance with the NISP and National Industrial Security Program Operating Manual (NISPOM, DoD 5220.22): The database will include name, Social Security Number (SSN), citizenship, place of birth, date of birth, security clearance, and mailing/home address. The following records are maintained to contact cleared contractors in order to execute the oversight mission of DSS: cellular telephone number, work telephone number, facsimile number and email address. In addition, NISS collects name, Social Security Number, date of birth, place of birth, and security clearance information of individuals who are the culpable party of a security violation. This Personal Identification Data (PID) is used to create an incident report in the Joint Personnel Adjudication System (JPAS), as necessary. Finally, name, security clearance, and job titles are recorded for select individuals interviewed by DSS Industrial Security Specialists during oversight activities.

RECORD SOURCE CATEGORIES: The record sources are the individuals themselves, which is collected via Paper Form, Telephone Interview, Email, Face-to-Face Contact, Fax, Website, and the NISS.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

a) DSS: Authorized DSS personnel may be issued an Internal NISS user account; those individuals will have access to Personal Identification Data (PID) information. The primary users are the members of the security oversight team, many of whom are located across the country in DSS Field Offices. These individuals maintain information of those facilities participating in the NISP. The DoD Security Service Centers located in Fort Meade, MD and Quantico, VA has access to information for facility verification purposes. NISS captures name, SSN; date of birth, place of birth, citizenship data, and security clearance information of Key Management Personnel at each facility and culpable persons of a security violation. Additionally, DSS collects and records the name and contact information (telephone number, email address, facsimile number, mailing address) of company individuals who support the security program. Finally, name, security clearance level, and job titles are recorded for

select individuals interviewed by DSS Industrial Security Specialists during oversight activities.

b) DoD: Information provided to Facility Clearance Verifier external users at a given DoD agency will include core facility clearance information and facility contact information, including classified mailing addresses as applicable. For Facility Clearance (FCL) Verification Requests for all external users, Facility Security Officer (FSO) name and telephone number will be available for any valid company searched. Special requests for additional information may be made, and these requests will be coordinated and adjudicated in accordance with Agency standard procedures.

c) Other Federal Agencies: Information provided to Facility Clearance Verifier external users at a given external federal agency will include core facility clearance information and facility contact information, including classified mailing addresses as applicable. For FCL Verification Requests for all external users, FSO name and telephone number will be available for any valid company searched. Special requests for additional information may be made, and these requests will be coordinated and adjudicated in accordance with Agency standard procedures.

d) Industry: Information provided to Security Staff External users at a given facility will include detailed facility clearance information and correspondence with DSS. Only External Industry users who have a valid requirement for access to the facility's information (e.g., the Industry user is a key member of the security team for a given facility) will be granted access to that facility's detailed information. For general FCL information requests for all Facility Clearance Verifier users, core facility information and FSO name and telephone number will be available for any valid company searched.

In addition to those DSS closures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be DSS closed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows: The 'Blanket Routine Uses' published at the beginning of DSS' compilation of systems of records notices apply to this system.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Retention and purging of electronic and hard copy files will be in conformance with guidelines identified in schedule NC1-446-81-2 Item 2, "Industrial Security Facility Case Files."

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Retention and purging of electronic and hard copy files will be in conformance with guidelines identified in schedule NC1-446-81-2 Item 2, "Industrial Security Facility Case Files."

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Retention and purging of electronic and hard copy files will be in conformance with guidelines identified in schedule NC1-446-81-2 Item 2, "Industrial Security Facility Case Files."

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Printed paper records are contained and stored in regulation safes/filing cabinets which are located in a Sensitive Compartmented Information Facility (SCIF) with limited access. The database is also maintained in the SCIF which is password protected and entry provided on a need-to-know basis only. DSS will enforce procedures, standards, and guidelines on privacy and confidentiality of records 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 includes name, SSN, date of birth, place of birth, and citizenship data of specific Key Management Personnel (KMP) and individuals deemed culpable for security violations. Name and contact information (telephone numbers, email address, facsimile number, mailing address) are collected for company individuals who support the security program. Name, security clearance level, and job titles are recorded for select individuals interviewed by DSS Industrial Security Specialists during oversight activities. 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 two factor authentication utilizing their Common Access Card (CAC) or similar credentials such as Public Key Infrastructure (PKI), only after their request for an account has been properly vetted. 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 Enterprise Mission Assurance Support Service (eMASS). We perform a system assessment of each control during the Approval to Operate (ATO) accreditation process.

RECORD ACCESS PROCEDURES: Individuals seeking access to information about themselves contained in this system of records should address written inquiries to the Privacy Act Officer, DSS, 27130 Telegraph Road, Quantico, VA All Privacy Act requests must contain the following: full name, street address, city, state and zip code, Email and telephone number, social security number, date of birth, city of birth, state of birth, country of birth, Subject's birth name (if different). In addition, a perjury statement must be provided:

Individuals seeking access to information about themselves contained in this system of records should address written inquires to the Privacy Act Officer at 27130 Telegraph Road, Quantico, VA 22134

CONTESTING RECORD PROCEDURES: DSS' rules for accessing records, contesting contents, and appealing initial agency determinations are contained in DSS Regulation 01-13; 32 CFR part 321; or may be obtained from the Defense Security Service, Office of FOI and PA, 27130 Telegraph Road, Quantico, VA 22134.

NOTIFICATION PROCEDURES: Inquiries from individuals should be addressed to the assigned DSS Industrial Security Representative for the facility that is responsible for maintenance of the record.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: [Citation(s) to the last full *Federal Register* notice that includes all comments that is required to be in a SORN, as well as any subsequent notices of revision].