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

SECURITY CLASSIFICATION: Unclassified

SYSTEM LOCATION: Defense Security Service, 27130 Telegraph Road, Quantico, VA 22134-2253.

SYSTEM MANAGER(S): Defense Security Service, (DSS), Data Center Operations, NISS System Manager, 27130 Telegraph Road, Quantico, VA 22134-2253, dss.quantico.dss-hq.list.mla-data-center-ops@mail.mil.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: National Industrial Security Program Operating Manual, (DoD Manual 5220.22-M); Department of Defense Instruction 5220.22, National Industrial Security Program; E.O. 12829, National Industrial Security Program (NISP); and E.O. 9397 (SSN), as amended.

PURPOSE(S) OF THE SYSTEM: NISS is the DSS industrial system information system architecture and will replace the Industrial Security Facilities Database (ISFD) and Electronic Facilities Clearance System (e-FCL) capabilities to develop an on-demand, data-driven environment with automated workflows accessible to industry and government partners. NISS will serve as the only system to evaluate performance related to the Department of Defense's administration and implementation of the NISP as outlined in EO 12829. NISS provides users a perspective on NISP-related facilities and facilities under DSS oversight in the DoD conventional Arms, Ammunition, and Explosives (AA&E) program. NISS stores various types of facility information such as security vulnerability assessment results, advice and assistance information. NISS allows contractors to electronically submit facility information to DSS when applying for a new facility clearance or when reporting changed conditions for an existing FCL. It also allows DSS personnel to review and process new FCL applications and changed conditions, which are referred to as "packages".

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Civilian and contractor personnel of DoD and those federal agencies that receive NISP services from DoD. This includes DSS civilian and contractor personnel performing NISP oversight duties; military, civilian and contractor personnel of DoD and other federal agencies performing facility clearance verification or sponsorship of contractors for facility clearances; and, contractor security personnel performing duties related to administration of industrial security at their company or cleared facility.

CATEGORIES OF RECORDS IN THE SYSTEM: Name; Social Security Number (SSN); date of birth; place of birth; country of citizenship; personal and work telephone numbers; facsimile number; mailing/residence address; personal and work email addresses; security clearance information, and mailing/home address. Name, security clearance, and position titles are recorded for select individuals interviewed by DSS, Industrial Security Specialists during oversight activities.

RECORD SOURCE CATEGORIES: Information is obtained from the individual either in paper form, by telephone, fax, email, or face-to-face contact, and then entered into NISS, or via direct entry electronically into NISS. All information is protected and disposed of according to the classification.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH 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:
The DoD Blanket Routine Uses set forth at the beginning of DSS' compilation of systems of records notice may apply to this system.

a. To Defense Security Service (DSS) personnel for the purpose of being issued an Internal NISS user account; those individuals will have access to Personal Identification Data information. The primary users are authorized DSS personnel performing industrial security oversight duties. These individuals maintain, verify, and update information about their own NISP oversight work and information regarding facilities participating in the NISP. NISS captures name, SSN, date of birth, place of birth, citizenship data, and security clearance information of key management personnel for each cleared facility, and for persons found to be responsible for compromises of classified information. Additionally, DSS collects and records the name and contact information (telephone number, email address, facsimile number, mailing address) of personnel performing security duties for cleared companies. Finally, name, security clearance level, and job titles are recorded for select individuals interviewed by DSS Industrial Security Specialists during oversight activities.

b. To DoD security and contracting personnel, in connection with Facility Clearance (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.

c. To security and contracting personnel for other (non-DoD) Federal Agencies, in connection with Facility Clearance (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.

d. 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.

e. To DSS Insider Threat Identification and Mitigation Program personnel or Federal law enforcement authorities for use in assessing a potential risk or threat to DoD personnel, property,

information and facilities posed by persons within the agency who are, or are believed to be, engaging in activity which may harm U.S. national security interests or U.S. national security through unauthorized disclosure of classified information, data modification, espionage, terrorism, or action that would result in loss or degradation of DoD or other Federal Government resources or capabilities.

f. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government when necessary to accomplish an agency function related to this system of records.

g. To designated officers and employees of Federal, State, local, territorial or tribal, international, or foreign agencies maintaining civil, criminal, enforcement, or other pertinent information, such as current licenses, if necessary, to obtain information relevant and necessary to a DoD Component decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

h. To contractors whose employees require suitability determinations, security clearances, and/or access to classified national security information, for the purpose of ensuring that the employer is appropriately informed about information that relates to and/or may impact a particular employee or employee applicant's suitability or eligibility to be granted a security clearance and/or access to classified national security information.

i. To a former DoD employee for the purpose of responding to an official inquiry by a Federal, State, local, territorial or tribal entity or professional licensing authority, in accordance with applicable DoD regulations; or for the purpose of facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the DoD requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

j. To foreign or international law enforcement, security, or investigatory authorities to comply with requirements imposed by, or to claim rights conferred in, international agreements and arrangements, including those regulating the stationing and status in foreign countries of DoD military and civilian personnel.

k. To the Merit Systems Protection Board and the Office of the Special Counsel for the purpose of litigation, including administrative proceedings, appeals, special studies of the civil service and other merit systems; review of Office of Personnel Management or component rules and regulations; investigation of alleged or possible prohibited personnel practices, including administrative proceedings involving any individual subject of a DoD investigation.

l. To appropriate Federal, State, local, territorial, tribal, foreign, or international agencies for the purpose of counterintelligence activities authorized by U.S. law or Executive Order, or for the purpose of executing or enforcing laws designed to protect the national security or homeland security of the United States, including those relating to the sharing of records or information concerning terrorism, homeland security, or law enforcement.

m. To any person, organization or governmental entity (e.g., local governments, first responders, American Red Cross, etc.), in order to notify them of or respond to a serious and imminent terrorist or homeland security threat or natural or manmade disaster as is necessary and relevant for the purpose of guarding against or responding to such threat or disaster.

n. To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of an investigation or case arising from the matters of which they complained and/or of which they were a victim.

o. To such recipients and under such circumstances and procedures as are mandated by Federal statue or treaty.

p. To the news media and the public unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

q. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information indicates a violation or potential or violation of law, whether criminal, civil, or regulatory in nature.

r. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

s. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

t. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

u. To appropriate agencies, entities, and persons when (1) DoD suspects or has confirmed that there has been a breach of the system of records; (2) DoD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

v. To another Federal agency or Federal entity, when DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and

operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

w. If a system of records maintained by a DoD Component to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether Federal, State, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

x. A record from a system of records maintained by a Component may be disclosed as a routine use to a Federal, State, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a Component decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

y. A record from a system of records maintained by a Component may be disclosed to a Federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

z. Disclosure from a system of records maintained by a Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

aa. A record from a system of records maintained by a Component may be disclosed to foreign law enforcement, security, investigatory, or administrative authorities to comply with requirements imposed by, or to claim rights conferred in, international agreements and arrangements, including those regulating the stationing and status in foreign countries of Department of Defense military and civilian personnel.

bb. Any information normally contained in Internal Revenue Service Form W-2 which is maintained in a record from a system of records maintained by a Component may be disclosed to State and local taxing authorities with which the Secretary of the Treasury has entered into agreements under 5 U.S.C., sections 5516, 5517, 5520, and only to those State and local taxing authorities for which an employee or military member is or was subject to tax regardless of whether tax is or was withheld. This routine use is in accordance with Treasury Fiscal Requirements Manual Bulletin No. 76-07.

cc. A record from a system of records subject to the Privacy Act and maintained by a Component may be disclosed to the Office of Personnel Management (OPM) concerning information on pay and leave, benefits, retirement reductions, and any other information

necessary for the OPM to carry out its legally authorized government-wide personnel management functions and studies.
dd. A record from a system of records maintained by a Component may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the Department of Defense, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

ee. Information as to current military addresses and assignments may be provided to military banking facilities who provide banking services overseas and who are reimbursed by the Government for certain checking and loan losses. For personnel separated, discharged, or retired from the Armed Forces, information as to last known residential or home of record address may be provided to the military banking facility upon certification by a banking facility officer that the facility has a returned or dishonored check negotiated by the individual or the individual has defaulted on a loan and that if restitution is not made by the individual, the U.S. Government will be liable for the losses the facility may incur.

ff. A record from a system of records maintained by a Component may be disclosed as a routine use to the General Services Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

gg. A record from a system of records maintained by a Component may be disclosed as a routine use to the Merit Systems Protection Board, including the Office of the Special Counsel, for the purpose of litigation, including administrative proceedings, appeals, special studies of the civil service and other merit systems, review of Office of Personnel Management or Component rules and regulations, investigation of alleged or possible prohibited personnel practices, including administrative proceedings involving any individual subject of a DoD investigation, and such other functions, promulgated in 5 U.S.C. 1205 and 1206 or as may be authorized by law.

hh. A record from a system of records maintained by a Component may be disclosed as a routine use outside the Department of Defense (DoD) or the U.S. Government for the purpose of counterintelligence activities authorized by U.S. law or Executive Order or for the purpose of enforcing laws that protect the national security of the United States.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Electronic storage media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Information is generally retrieved by SSN. However, access to certain functions may require a combination of SSN, name, date of birth, and/or state and/or country of birth.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Disposition pending until the National Archives and Records Administration has approved the retention and disposition schedule, treat as permanent.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Administrative: backups secured off-site, encryption of backups, methods to ensure only authorized personnel

access to PII, periodic security audits, and regular monitoring of users' security practices. Physical: cipher locks, closed circuit TV, key cards, and security guards. Technical safeguards: Common Access Card, DoD public key infrastructure certificates, encryption of data at rest, encryption of data in transit, firewall, intrusion detection system, and role-based access control, used only for privileged (elevated roles).

RECORD ACCESS PROCEDURES: Individuals seeking access to information about themselves contained in this system of records should address written requests to the Defense Security Service, ATTN: Office of Freedom of Information and Privacy Act, 27130 Telegraph Road, Quantico, VA 22134-2253. For verification purposes, individuals should provide full name, current address, and sufficient details to permit locating pertinent records, and signature. Signed, written requests should contain the individual's full name, telephone number, street address, email address, and name and number of this system of records notice.

In addition, the requester must provide a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

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 Freedom of Information and Privacy Act , 27130 Telegraph Road, Quantico, VA 22134-2253.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to Defense Security Service, ATTN: Office of Freedom of Information and Privacy Act, 27130 Telegraph Road, Quantico, VA 22134-2253. Signed, written requests should contain the individual's full name, telephone number, street address, email address, and name and number of this system of records notice.

In addition, the requester must provide a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

EXEMPTIONS PROMULGATED FOR THE SYSTEM: The Department of Defense is exempting records maintained in DSS V10-01 from subsections (c)(3), (d)(1), and (d)(2),of the Privacy Act pursuant to 5 U.S.C. 552a(k)(5). Exempt records received from other systems of records in the course of industrial security oversight activities may, in turn, become part of the case records in this system. When records are exempt from disclosure in systems of records for record sources accessed by this system, DSS hereby claims the same exemptions for any copies of such records received by and stored in this system.

(b) Promises of confidentiality. (1) Only the identity of sources that have been given an express promise of confidentiality may be protected from disclosure under paragraphs (d)(3)(i), (ii), and (iii) and (d)(4) of this section. However, the identity of sources who were given implied promises of confidentiality in inquiries conducted before September 27, 1975, also may be protected from disclosure. (2) Ensure promises of confidentiality are not automatically given but are used sparingly. Establish appropriate procedures and identify full categories of individuals who may make such promises. Promises of confidentiality shall be made only when they are essential to obtain the information sought (see 5 CFR part 736).

(iii) Subsection (d)(1). Disclosure of records in the system could reveal the identity of confidential sources and result in an unwarranted invasion of the privacy of others. Disclosure may also reveal information relating to actual or potential criminal investigations. Disclosure of classified national security information would cause damage to the national security of the United States. Disclosure could also interfere with a civil or administrative action or investigation; reveal the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations; and reveal the confidentiality and integrity of Federal testing materials and evaluation materials used for military promotions when furnished by a confidential source.

(xi) Subsection (k)(1)(2)(3)and (5). Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5).

HISTORY: N/A