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:

NBIS - Defense Information System for Security Version 2 (NBIS- DISS2)

2. DOD COMPONENT NAME:

Defense Counterintelligence and Security Agency

3. PIA APPROVAL DATE:

05/05/2026

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- ☐ From members of the general public
- ☐ From Federal employees
- ☒ from both members of the general public and Federal employees
- ☐ Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one.)*

- ☐ New DoD Information System
- ☐ New Electronic Collection
- ☒ 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.

The Defense Counterintelligence and Security Agency (DCSA) is a federal security agency of the United States Department of War (DoW) and provides secure services and solutions to support DoW's mission. The DCSA maintains the Defense Information System for Security (DISS2) program to specifically address the security clearance and Suitability/Fitness determination requirements outlined in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) as well as to support Homeland Security Presidential Directive-12 (HSPD-12) compliance across DoW. DISS2 is a secure, end-to-end Information Technology system that reduces the DoW personnel security clearance, Suitability/Fitness, and HSPD-12 process cycle times by electronically collecting, reviewing, and sharing relevant data among appropriate government agencies.

DISS2 is an Enterprise capability that includes the Joint Verification System (JVS), the Case Adjudication Tracking System (CATS), Service Desk, and Appeals. Together, these systems manage the adjudication process for security clearances and HSPD-12 and Suitability/Fitness determinations for all DoW employees, military personnel, civilians, and contractors. JVS provides DoW Security Managers and Officers with current clearance information and the ability to update personnel security information and security history.

CATS performs electronic and human adjudication functions, automating the record-keeping of granting security clearance and eligibility, and generates customized reports on activities in CATS, such as user performance reviews or the amount of time a case spends in each phase.

Additional personal information captured in NBIS-DISS2 is explained in more detail in Section 2: PII Risk Review.

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)*

The intended use of the PII collected by NBIS-DISS2 is for Security Clearance and Verification. The SSN is the identifier that links all aspects of a security clearance investigation together; linked to other Federal agencies that continue to use the SSN as a primary identifier.

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

While individuals cannot object to the collection of their PII by NBIS DISS2 directly, the cleared individuals on whom the PII will be collected have given permission for information to be collected from them by voluntarily filling out the SF 85 and/or SF 86 Questionnaire for National Security Positions. Both the SF85 and SF86 state "The information you provide on this form, and information collected during an investigation, may be disclosed without your consent by an agency maintaining the information in a system of records as permitted by the Privacy Act [5 U.S.C. 552a(b)], and by routine uses, a list of which are published by the agency in the Federal Register." The SF85, SF85P, and SF86 list as a Routine Use, disclosure "to Executive Branch Agency insider threat, Counterintelligence, and Counterterrorism officials to

fulfill their responsibilities under applicable Federal law and policy, including but not limited to E.O. 12333, 13587 and the National Insider Threat Policy and Minimum Standards given consent for data to be collected by voluntarily submitting the SF 85, SF 85P, or SF 86."

f. 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.

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

While individuals cannot consent to the specific use of their PII by NBIS DISS2 directly, the individuals on whom the PII will be collected have given voluntary responses to information requested by official questionnaires (for example: SF 85, SF 85P, or SF 86). The Electronic Questionnaires for Investigation Processing (eQIP) or eAPP (National Background Investigation Services - Electronic Application) is the initial point of PII collection, then PII is transmitted to NBIS-DISS2.

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.)*

☐ Privacy Act Statement ☒ Privacy Advisory ☐ Not Applicable

A Privacy Act Statements is provided to the individual at initiation of personnel vetting processes (SF 85, SF 85P, SF 86, information collections, and interviews). Users of DISS receive the following Advisory:

Personally Identifiable Information
DATA YOU ARE ABOUT TO ACCESS COULD POTENTIALLY BE PROTECTED BY THE PRIVACY ACT OF 1974. You must:
Have completed the necessary training with regards to Security Awareness and safe-guarding Personally Identifiable Information.
Ensure that data is not posted, stored or available in any way for uncontrolled access on any media.
Ensure that data is protected at all times as required by the Privacy Act of 1974 (5 USC 552a(I)(3)) as amended and other applicable DoD regulatory and statutory authority; data will not be shared with offshore contractors; data from the application, or any information derived from the application, shall not be published, disclosed, released, revealed, shown, sold, rented, leased or loaned to anyone outside of the performance of official duties without prior DCSA approval.
Delete or destroy data from downloaded reports upon completion of the requirement for their use on individual projects.
Ensure data will not be used for marketing purposes.
Ensure distribution of data from a DCSA application is restricted to those with a need-to-know. In no case shall data be shared with persons or entities that do not provide documented proof of a need-to-know.
Be aware that criminal penalties under section 1106(a) of the Social Security Act (42 USC 1306(a)), including possible imprisonment, may apply with respect to any disclosure of information in the application(s) that is inconsistent with the terms of application access. The user further acknowledges that criminal penalties under the Privacy Act (5 USC 552a(I)(3)) may apply if it is determined that the user has knowingly and willfully obtained access to the application(s) under false pretenses.

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

☒ Within the DoD Component	Specify.	Authorized DCSA personnel who have a need-to-know (for example: CAS, VRO, DITMAC, PCLF, and OCCA).
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Defense Office of Hearings and Appeals (DOHA); Office of the Secretary of Defense (OSD); Under Secretary of Defense for Intelligence (USD(I)); Under Secretary of Defense for Acquisition, Technology and Logistics (AT&L); Washington Headquarters Services (WHS); Defense Security Services (DSS); Joint Chiefs of Staff (JCS); U.S. Army; U.S. Air Force; U.S. Navy; U.S. Marine Corps; and Guard/Reserve Components.
☒ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	Accessions - Air Force Recruiting Information Support System (AFRISS), Accessions - Army Recruiting Information Support System (ARISS), Accessions - Marine Core Recruiting Information Support System (MCRISS), Accessions - Navy Recruiting Information Support System (NRISS), Army Analytical Group (AAG) DB Extract, Army Human Resource Command (HRC) (Formerly LiveScan), Army Human Resource Command (HRC) (Formerly LiveScan), Contractor Verification System (CVS) - DISS Result Files, CVS - SII Bridge Files, Defense Central Index of Investigations (DCII), Data Delivery Service (DDS), DISS Subject Interface (DSI), DISS Subject Application Program Interface (API), Electronic Questionnaires for Investigations Processing (eQIP), Integrated Personnel Pay System - Army (IPPS-A), JAVELIN, Military Personnel

Data System (MilPDS), Mirador (CE Submission)(CE Enrollment), Mirador [Continuous Evaluation (CE) Status], Mirador (Defer to CE), Mirador Subject Summary, Mirador CE Subject Trigger, DISS Rapback Interface, National Background Investigative Services (NBIS) Flat File, NBIS Trigger, National Industrial Security System (NISS), Naval Information Warfare Center (NIWC), National Security Agency (NSA), NBIS Determination Propagator, DISS Organization NBIS Trigger, DISS-PDT, PIPS - Daily Case File (DCF), PIPS - Investigation, Scattered Castles (SC), and Total Army Personnel Database (TAPDB)

☐ State and Local Agencies

Specify.

☒ 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. Contractors with an active Facility Clearance and employees who are eligible to have a security clearance and/or access to classified national security information following National Industrial Security Program Operating Manual (NISPOM) regulations.

☐ 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)*

☒ Individuals
☒ Databases
☒ Existing DoD Information Systems
☒ Commercial Systems
☒ Other Federal Information Systems

NBIS-DISS2 accepts the subject-entered data from e-QIP or eAPP as well as data that may be manually entered in SF-85 (Questionnaire for Non-Sensitive Positions), SF-85P (Questionnaire for Public Trust Positions), SF-86 (Questionnaire for the National Security Positions), or self-reported information. Information sources include Defense Enrollment Eligibility Reporting System (DEERS), Defense Civilian Personnel Data System, Electronic Military Personnel Record System, continuous evaluation records, DoW and federal adjudicative facilities/organizations, Defense Counterintelligence Security Agency (DCSA) Investigative Service Providers (ISP), DoW intelligence (NSA, NRO, NGA, and DIA), security managers, security officers, or other officials requesting and/or sponsoring the security eligibility, suitability determination, and visitation of facilities. Additional information may be obtained from sources such as personnel security investigations, DCSA investigative criminal or civil investigations, subject's personal financial records, military service records, travel records, medical records, and unsolicited sources.

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

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

SF 85, SF 85P, SF 86, and eQIP/eAPP.

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 ☐ No

If "Yes," enter SORN System Identifier Personnel Vetting Records System, DUS

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-0446-2019-0004 and DAA-0446-2021-0009

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

(3) Retention Instructions.

Records are destroyed no later than 16 years after termination of affiliation with the DoW. Investigative files and the computerized data bases which show the scheduling or completion of an investigation are retained for 16 years from the date of closing or the date of the most recent investigative activity, whichever is later, except for investigations involving potentially actionable issue(s) which will be maintained for 25 years from the date of closing or the date of the most recent investigative activity.

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.

5 U.S.C. 9101, Access to Criminal History Records for National Security and Other Purposes; 10 U.S.C. 137, Under Secretary of Defense for Intelligence; E.O. 12968, Access to Classified Information; E.O. 12333 United States Intelligence Activities; E.O. 12829, National Industrial Security Program; E.O. 10450, Security Requirements for Government Employment; E.O. 10865, Safeguarding Classified Information Within Industry; E.O. 13467 Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees and Eligibility for Access to Classified National Security Information; E.O. 12968, as amended, Access to Classified Information; E.O. 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust; E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information; DoDI 1400.25, Volume 731, DoD Civilian Personnel Management System: Suitability and Fitness Adjudication for Civilian Employees; DoDD 5205.16, DoD Insider Threat Program; DoDD 1145.02E, USMEPCOM; DoD 5200.2-R, DoD Personnel Security Program; DoD Manual 5105.21, Volume 1, SCI Administrative Security Manual: Administration of Information and Information Systems Security; DoDI 1304.26, Qualification Standards for Enlistment, Appointment, and Induction; DoDI 5200.02, DoD PSP; DoDD 5220.6, Defense Industrial Personnel Security Clearance Review Program; DoDI 5220.22, NISP; DoDI 5200.46, DoW Investigative and Adjudicative Guidance for Issuing the CAC; HSPD-12, Policy for Common Identification Standard for Federal Employees and Contractors; 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.

0705-0008 . OMB EXPIRATION DATE: 11/30/2027. The 60-Day Notice for 0705-0008, "Defense Information System for Security," published in the Federal Register on 9/23/2024. The Docket ID is DoD-2024-OS-0056.