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 Background Investigation Services - Investigation Management

2. DOD COMPONENT NAME:

Defense Counterintelligence and Security Agency

3. PIA APPROVAL DATE:

03/15/2026

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.

Investigation Management (IM) capability is the central NBIS functional platform. PII is collected in support of mission related use for federal background investigation related to personnel vetting. These investigation results are used to determine eligibility, suitability, fitness, access, etc. of individuals for employment purposes. There are three major activities associated with a background investigation: initiation, investigation, and adjudication. IM provides all of the capabilities required to conduct and manage the information aspects of an investigation. IM provides the completed case file to an external adjudication agency for final determination. The IM system will provide automated scoping of a case, automated assignment of items based on dynamic parameters, electronic reminders to information providers (e.g., [E-]Voucher respondent), and workflow support for investigators.

Individuals are informed at the point of collection in eApplication (eAPP) and again at the beginning of an in person interview, that providing information is voluntary. They are advised that if they do not consent to the collection of the required information, it may affect the completion of their background investigation. They do not have the ability, once they have agreed to the background investigation, to consent to some uses of their information and decline to consent to other uses. The exception to this is the SF86 Medical Release authorization, which is valid for 1 year from the date signed but can be revoked at any time by writing to the individual's health care provider/entity, except to the extent that action has already been taken based on the authorization.

IM is an automated system that houses the Security/Suitability Investigations Index (SII) and is used for the automated entry, scheduling, case control and closing of background investigations. SII is the repository of personnel investigations conducted by DCSA (including predecessors) and other authorized agencies. The purpose of the NBIS Investigation Management (IM) system is to facilitate the secure processing of personnel security questionnaires submitted through eApp . IM directly collects the eApp data. The types of personal information collected within the system include, but are not limited to: full name, date of birth, place of birth, Social Security Number (SSN), contact information, citizenship, marital status, family information, education history, employment history, financial information, criminal history, foreign contacts, drug use history, and mental health history. Security Officers from Agencies and Industry utilize IM to review this information. Authorizers then use IM to securely release the eApp to the investigative process or continuous vetting process.

The type of personal information collected includes but is not limited to: name, address, phone number, aliases used, email, Social Security Number, Date of Birth, Place of Birth, citizenship, and personal identifiers. Also collected is detailed information on spouse, cohabitant(s), and immediate family members, such as dates and places of birth and addresses. All PII information are stored in AWS GovCloud.

Note: IM releases SF applications to eQIP Direct and eQIP Direct sends it to the FBI for their specific investigations. Not all Agencies use DCSA to do the investigation. For instance Intel, State Dept, FBI, DHS and others perform their own investigations we help with the collection of data from the Subject/Applicant and forward it to them.

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)*

PII is collected in support of mission related use for federal background investigations for personnel vetting purposes. These investigation results are used to determine eligibility, suitability, fitness, access, etc. of individuals for employment purposes. The PII collected includes financial, commercial, public, and law enforcement records to determine if individuals pose a security risk. PII is also used as identification/ verification to confirm information provided in response to conducted checks relates to the individual.

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.

IM does not collect with the individuals directly. The subject is asked to provide PII by the Facility Security Office (FSO) to provide for the IM system. The system does not present individuals the opportunity to object to the collection of their PII and/or consent to the specific uses of their PII. Individuals voluntarily complete the SF85, SF85P, SF85P-S, SF86, or Personnel Vetting Questionnaire (PVQ) in eAPP, and are advised of and are asked to acknowledge the specific uses for their PII.

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.

The system does not present individuals the opportunity to consent to the specific uses of their PII, as IM does not collect directly from the subject/individual. Individuals voluntarily complete the SF85, SF85P, SF85P-S, SF86, or Personnel Vetting Questionnaire (PVQ) in eAPP, and are advised of and are asked to acknowledge the specific uses for their PII.

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

Subjects have no access to the system, subjects are not entering information directly into NBIS IM, however agency users are presented with the following advisory:

The USG routinely intercepts and monitors communications on this Information System (IS) for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants.
Such communications and work product are private and confidential.

PERSONALLY IDENTIFIABLE INFORMATION
DATA YOU ARE ABOUT TO ACCESS COULD POTENTIALLY BE PROTECTED BY THE PRIVACY ACT OF 1974, AS AMENDED. You must:
• Have completed the necessary training with regards to Security Awareness, Cyber Awareness, and safeguarding 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 Federal or Departmental 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.	Personal Vetting, BI, AVS, Privacy, PEO, NBIS
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	U.S. Navy, U.S. Marine Corps, U.S. Army, U.S. Air Force, and U.S. Space Force, DMDC, NSA, DIA, DISA, DFAS, Fourth Estate Agencies
☒ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	Environmental Protection Agency, Department of Agriculture, Department of Commerce, Department of Education, Department of Energy, Department of Health and Human Services, Department of Homeland Security, Department of Housing and Urban Development, Department of the Interior, Department of Justice, Department of Labor, Department of State, Department of Transportation, Department of the Treasury, Department of Veterans Affairs, Central Intelligence Agency, Federal Bureau of Investigation, National Security Agency, Immigration and Customs Enforcement, Customs and Border Protection, Transportation Security Administration, Federal Emergency Management Agency, Secret Service, Drug Enforcement Administration, Bureau of Alcohol Tobacco Firearms and Explosives, U.S. Marshals Service, Federal Aviation Administration, Internal Revenue Service, Bureau of Engraving and Printing, U.S. Mint, Financial Crimes Enforcement Network, Office of the Comptroller of the Currency, Social Security Administration, Centers for Disease Control and Prevention, Food and Drug Administration, National Institutes of Health, Centers for Medicare and Medicaid Services, Substance Abuse and Mental Health Services Administration, U.S. Geological Survey, National Park Service, Fish and Wildlife Service, Bureau of Land Management, Bureau of Indian Affairs, U.S. Forest Service, Rural Development, Food and Nutrition Service, Animal and Plant Health Inspection Service, Food Safety and Inspection Service, Federal Trade Commission, Securities and Exchange Commission, Federal Communications Commission, Federal Energy Regulatory Commission, Nuclear Regulatory Commission, Equal Employment Opportunity Commission, National Labor Relations Board, Federal Election Commission, Consumer Financial Protection Bureau, Small Business Administration, General Services Administration, Office of Personnel Management, Government Accountability Office, Congressional Budget Office, Library of Congress, Government Publishing Office, Smithsonian Institution, National Archives and Records Administration, Office of Management and Budget, U.S. Agency for International Development, Peace Corps, Federal Deposit Insurance Corporation, Federal Reserve System, Export-Import Bank, Millennium Challenge Corporation, National Science Foundation, National Aeronautics and Space Administration, Environmental Protection Agency, National Endowment for the Arts, National Endowment for the Humanities, Institute of Museum and Library Services, DISA
☐ 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.	There are no FAR clauses in the contract. NBIS-IM is a System of Record; POA&M is in the eMASS. Contract mod is required for related Peraton contract.

☐ 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

IM receives data from other DoD information System and from FSO but not from other Federal Information Systems.
IM receives from eApp, Defense Information System for Security (DISS), National Industrial Security System (NISS NI2), pushes to eQIP Direct/PIPS, Mirador, Secure File Gateway (SFG).

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)*

eAPP for system-to-system information sharing, and security officials/FSOs for subject profile creation.
Forms: SF85, SF85P, SF85P-S, SF86, or Personnel Vetting Questionnaire (PVQ)

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 DUSDI-02, Personnel Vetting Records

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-446-2019-0004, DAA-446-2019-0007

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

(3) Retention Instructions.

DAA-446-2019-0004: Investigative Case Files - Master file of each investigation. Cutoff when case closes. Destroy closed cases involving potentially actionable issues 25 years after case closing. Destroy all other closed cases 16 years after case closing.
DAA-446-2019-0007: Continuous Evaluation Program Records - Destroy or delete records involving potentially actionable issues 25 years after the end of affiliation. Destroy or delete all other records 16 years after the end of affiliation.

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.

10 U.S.C. 137, Under Secretary of Defense for Intelligence; 10 U.S.C. 504, Persons Not Qualified; 10 U.S.C. 505, Regular components: Qualifications, term, grade; Atomic Energy Act of 1954, 60 Stat. 755; Public Law 108-458, The Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 401 note); Public Law 114-92, Section 1086, National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2016, Reform and Improvement of Personnel Security, Insider Threat Detection and Prevention, and Physical Security (10 U.S.C. 1564 note); Public Law 114-328, Section 951 (NDAA for FY2017), Enhanced Security Programs for Department Defense Personnel and Innovation Initiatives (10 U.S.C. 1564 note); Public Law 115-91, Section 925, (NDAA for FY2018) Background and Security Investigations for Department of Defense Personnel (10 U.S.C. 1564 note); 5 U.S.C. 9101, Access to Criminal History Records for National Security and Other Purposes; Executive Order (E.O.) 13549, as amended, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities; E.O. 12333, as amended, United States Intelligence Activities; E.O. 12829, as amended, National Industrial Security Program; E.O. 10865, as amended, Safeguarding Classified Information Within Industry; E.O. 13467, as amended, 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. 13470, Further Amendments to Executive Order 12333; E.O. 13488, as amended, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust; E.O. 13526, Classified National Security Information; E.O. 13741, Amending Executive Order 13467, To Establish the Roles and Responsibilities of the National Background Investigations Bureau and Related Matters; E.O. 13764, Amending the Civil Service Rules; DoD Manual 5200.02, Procedures for the DoD Personnel Security Program (PSP); DoD Instruction (DoDI) 1400.25, Volume 731, DoD Civilian Personnel Management System: Suitability and Fitness Adjudication for Civilian Employees; DoDI 5200.46, DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC); Homeland Security Presidential Directive (HSPD) 12: Policy for a Common Identification Standard for Federal Employees and Contractors; Federal Information Processing Standard (FIPS) 201-2, Personal Identity Verification (PIV) of 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.

IM does not collect from the individuals directly. Individuals voluntarily complete the SF85, SF85P, SF85P-S, SF86, or PVQ, in eAPP, and IM is used to carry out the personnel vetting process.

Indirect Information Collections / Data Sources:
Defense Information System for Security (DISS), 0705-0008, EXP:11/2027
National Industrial Security System (NISS NI2), 0705-0006, EXP: 5/2028
Personnel Vetting Questionnaire (PVQ), 3206-0279, expiration November 2026 (OPM)
SF-85: Questionnaire for Non-sensitive Positions, 3206-0261, expiration December 2027 (OPM)
SF-85P: Questionnaire for Public Trust Positions, 3206-0258, expiration April 2027 (OPM)
SF-85P-S: Supplemental Questionnaire for Selected Positions, 3206-0258, expiration April 2027 (OPM)
SF-86: Questionnaire for National Security Positions, 3206-0005, expiration November 2026 (OPM)