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:

Sky Personnel Investigation Processing System (S-PIPS)

2. DOD COMPONENT NAME:

Defense Counterintelligence and Security Agency

3. PIA APPROVAL DATE:

06/04/2026

DCSA

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.

S-PIPS is a comprehensive, integrated system hosted in the AWS GovCloud for managing and processing personnel vetting and background investigations. Developed as a result of the NBIS BIES modernization effort, which replaced eight on-premise distributed applications and one mainframe application, it supports the entire investigation life-cycle, from initial data collection to final case adjudication and delivery, in a secure, near-paperless environment.

System Functionalities

• Case Management and Processing: S-PIPS serves as the central case processing system, managing all stages of a background investigation from initiation to completion. S-PIPS will automate the scheduling of investigative tasks, route cases to service providers, and store all case data including adjudication results, security clearances, and credentialing information.

• Data Collection and Ingestion: S-PIPS gathers subject information through various channels, including electronic questionnaires, fingerprint submissions, and data entered by field investigators. S-PIPS features robust document imaging capabilities to convert paper documents into an electronic format for efficient processing and storage.

• Investigative Checks and Verification: S-PIPS automates a wide array of investigative checks including fingerprint submissions to the FBI, conducts National Agency Checks by exchanging data with federal entities, and queries state criminal databases. S-PIPS also supports continuous evaluation to ensure individuals continue to meet security requirements.

• Integration and Information Exchange: S-PIPS is designed for secure and seamless information exchange with numerous external partners. S-PIPS electronically delivers completed investigation files to customer agencies and provides a secure portal for authorized partners to access information and collaborate on investigations.

• Document and Data Management: S-PIPS provides a centralized electronic repository for all case-related documents and data. S-PIPS includes advanced features for imaging, quality assurance, storage, and retrieval of electronic files, ensuring that field investigators have secure and reliable access to necessary information.

• Reporting and Oversight: S-PIPS includes a management reporting function that generates statistics and reports on investigation timeliness and workload. This provides authorized users with the necessary data for operational planning and oversight.

• User Access and Collaboration: S-PIPS offers a secure, multi-factor authenticated portal for both internal and external users, with access tailored to their specific roles. S-PIPS also provides collaboration tools, such as secure messaging and file sharing, to facilitate effective communication among all stakeholders involved in the investigation process.

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 PII is collected and use to build a comprehensive investigative file which involves data matching and verification with external agencies like the FBI and SSA, processing state criminal history records, and allowing investigators to access and update case information. The collected information is used for continuous evaluation, statistical reporting, and secure communication among users involved in the vetting process. This comprehensive collection and analysis are necessary for DCSA to fulfill the mandate of ensuring the trustworthiness of

individuals in sensitive government and contractor positions.

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.

The Subjects of the investigation (i.e, the persons being investigated) are notified of the authorities and purpose of the investigation, routine uses of the information, and of the voluntary nature of the information collection at the point of collection via the e-QIP/eAPP system and at the beginning of an in-person interview. The investigator provides notice and consent details verbally. Subjects cannot object to further collection of PII by use of S-PIPS during the investigation, which is accomplished in accordance with Federal Investigative Standards, but the Subject can request that the investigation be terminated at any time, in which case, further collection of information will ceased. All collected PII at the time will be destroyed in accordance with HIPAA and NIST Special Publication 800-88 for Media Sanitization to include shredding, purging, degaussing, etc.

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.

Individuals are notified at the point of collection, at the beginning of an in-person interview, and on various consent forms. They are informed that providing information is voluntary but that if they do not consent to the collection of the required information that 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.

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 Statement (PAS) is provided at initiation of investigation (e.g. SF 85, SF 85P, SF85PS, and or SF 86) which is done outside of S-PIPS.

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. Personnel Vetting, Adjudications and Vetting Services, related mission functions

☒ Other DoD Components *(i.e. Army, Navy, Air Force)* — Specify. DMDC, Department of the Army, Department of the Navy, Department of the Air Force

☒ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*

-Animal and Plant Health Inspection Service
-Bureau of Alcohol Tobacco Firearms and Explosives
-Bureau of Engraving and Printing
-Bureau of Indian Affairs
-Bureau of Land Management
-Central Intelligence Agency
-Centers for Disease Control and Prevention
-Centers for Medicare and Medicaid Services
-Congressional Budget Office
-Consumer Financial Protection Bureau
-Customs and Border Protection
-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 Justice
-Department of Labor
-Department of State
-Department of Transportation
-Department of Veterans Affairs
-Department of the Interior

Specify.	-Department of the Treasury -Drug Enforcement Administration -Environmental Protection Agency -Equal Employment Opportunity Commission -Export-Import Bank -Federal Aviation Administration -Federal Bureau of Investigation -Federal Communications Commission -Federal Deposit Insurance Corporation -Federal Election Commission -Federal Emergency Management Agency -Federal Energy Regulatory Commission -Federal Housing Finance Agency -Federal Labor Relations Authority -Federal Maritime Commission -Federal Mediation and Conciliation Service -Federal Mine Safety and Health Review Commission -Federal Reserve System -Federal Retirement Thrift Investment Board -Federal Trade Commission -Financial Crimes Enforcement Network -Fish and Wildlife Service -Food and Drug Administration -Food and Nutrition Service -Food Safety and Inspection Service -General Services Administration -Government Accountability Office -Government Publishing Office -Immigration and Customs Enforcement -Institute of Museum and Library Services -Internal Revenue Service -Library of Congress -Millennium Challenge Corporation -National Aeronautics and Space Administration -National Archives and Records Administration -National Endowment for the Arts -National Endowment for the Humanities -National Institutes of Health -National Labor Relations Board -National Park Service -National Science Foundation -National Security Agency -Nuclear Regulatory Commission -Office of Management and Budget -Office of Personnel Management -Office of the Comptroller of the Currency -Peace Corps -Rural Development -Secret Service -Securities and Exchange Commission -Small Business Administration -Smithsonian Institution -Social Security Administration -Substance Abuse and Mental Health Services Administration -Transportation Security Administration -U.S. Agency for International Development -U.S. Forest Service -U.S. Geological Survey

-U.S. Marshals Service
-U.S. Mint

☒ State and Local Agencies

Specify. PII is shared with state and local agencies (such as law enforcement agencies) when we conduct law criminal history record information and state license (e.g., bar membership).

☒ 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. IBM
• 52.224-3, Privacy training
• The Contractor shall maintain administrative, technical, and physical safeguards and controls required for the security level and services being provided IAW the Department of Defense Cloud Computing Security Requirements Guide (DoD CC SRG). The architecture and all related application components shall comply with the security standards and controls specified in DoDI 8500.01, Cybersecurity, DoDI 8510.01, Risk Management Framework for DoD Systems, and NIST SP 800-53, Revision 5 (Rev. 5), Security and Privacy Controls for Information Systems and Organizations. The Contractor shall utilize all security controls available at time of order issuance and pursue modernization to the maximum extent possible.
• The Contractor shall comply with (1) Security Agreement (DD Form 441/DD Form 441-1), including the National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M and any revisions and (2) 32 CFR, Part 117. Provisions of the Privacy Act apply to all records and reports maintained by the contractors.
• Appendix B References - NIST SP 800-53, Revision 5

☒ Other *(e.g., commercial providers, colleges).*

Specify. Credit bureaus, education institutions, employment verification services.

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

The data stored within DCSA Sky-PIPS will include information received from and sent to both internal and external systems.

Data will be pulled from DCSA systems including but are not limited to NBIS-Mirador, NBIS-DCII - Defense Central Index of Investigations, NBIS-DISS - Defense Information Security System Version 2, INBIS-M - Investigation Management. There is a potential for other DCSA Personnel Vetting systems to be temporary sources of information for data migration/validation purposes such as NBIS-DMS - Data Management System.

The data will be pulled from external Systems (agencies) including but not limited to CJIS (FBI), Scattered Castles (DNI).

Data will be pushed or sent via e-delivery to Systems within DCSA and external agencies (See agency list in section 1h)

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 85PS, SF 86, 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-DOD

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, DAA-446-2019-0007, DAA-0446-2019-0004-0002, DAA-0446-2024-0002

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

(3) Retention Instructions.

The S-PIPS records are subject to the retention schedules referenced above. Depending on the type of information and the action taken on that information, various retention periods apply. Standard investigations with no issues are retained for 16 years from the closing of the investigation; while those with issues are retained for 25 years from the closing of the investigation. Files obtained from other agencies in the course of an investigation are retained consistent with the agreement between the agency and DCSA. Additionally, information in S-PIPS is retained for certain business need purposes, for a temporary time. Case processing data is temporarily retained for 2 years or less, depending on the business need. FBI criminal history record information is temporarily retained in S-PIPS for 6 months after case closing. Credit reports are temporarily retained in S-PIPS for 7 days after case closing. If there is a credit report received on the individual, it is retained for 7 days after the case has closed. If information received includes FBI case files on the individual it is stored in S-PIPS, and retained for 6 months after the case has closed. Individual data, investigation and item events during the processing of the case are retained. SSN is necessary as they are used as primary keys to request individual information from federal agencies and bureaus including the following commercial entities: Credit Bureaus, Court and Law information, Periodical information from wire services, license information from license bureaus.

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.

Please see below:

* 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
* 5 U.S.C. 9101, Access to Criminal History Records for National Security and Other Purposes
* Atomic Energy Act of 1954, 60 Stat. 755
* DoD Instruction (DoDI) 1400.25, Volume 731, DoD Civilian Personnel Management System: Suitability and Fitness Adjudication for Civilian Employees

* DoD Manual 5200.02, Procedures for the DoD Personnel Security Program (PSP)
* DoDI 5200.46, DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC)
* Executive Order (E.O.) 10865, as amended, Safeguarding Classified Information Within Industry
* E.O. 12333, as amended, United States Intelligence Activities
* E.O. 12829, as amended, National Industrial Security Program
* E.O. 12968, as amended, Access to Classified Information
* 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. 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. 13549, as amended, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities
* 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
* E.O. 9397 (SSN), as amended
* Federal Information Processing Standard (FIPS) 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors
* Homeland Security Presidential Directive (HSPD) 12: Policy for a Common Identification Standard for Federal Employees and Contractors
* 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)

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.

Form Number	Form Name	OMB Number	Expiration Date
SF-85	Questionnaire for Non-Sensitive Positions	3206-0261	12/31/2027
SF-85P	Questionnaire for Public Trust Positions	3206-0258	04/30/2027
SF85PS	Supplemental Questionnaire for Selected Positions	3206-0258	04/30/2027
SF-86	Questionnaire for National Security Positions	3206-0005	11/30/2026
SF-87	Fingerprint Chart	3206-0150	04/30/2027
PVQ	Personnel Vetting Questionnaire	3206-0279	11/30/2026