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:

Personnel Investigations Processing System (PIPS)

2. DOD COMPONENT NAME:

DoD Business Enterprise

DCSA

3. PIA APPROVAL DATE:

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [x] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

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

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] 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 Personnel Investigations Processing System (PIPS) supports personnel vetting missions and is the case processing system for background investigations conducted by DCSA. This processing includes: ingest of security questionnaire information on subjects of investigation, either electronically via the Electronic Questionnaires for Investigations Processing (e-QIP) or via manual data entry; automated scheduling of National Agency Checks at the Federal Bureau of Investigation (FBI), Department of Defense Central Index of Investigations (DCII), national credit bureaus, etc.; scheduling and transmitting investigation requests to multiple investigative service providers; receiving reports of investigation from other investigative service providers; scheduling investigative inquiries to various sources (e.g., law, education, employment, etc.); closing investigations automatically; transmitting results electronically to customer agencies; and tracking all stages and pieces of each investigation. From the data in PIPS, DCSA produces a large variety of statistics and specific management information reports, used within the agency and its customer agencies to track investigations. Adjudication, security clearance, and credential data is also stored in PIPS.

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 and used for personnel vetting missions, such as the conduct of personnel background investigations; suitability, fitness, and security clearance determinations; physical and logical access determinations; continuous evaluation; etc.

e. Do individuals have the opportunity to object to the collection of their PII? [ ] Yes [x] 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 individuals were notified of the routine use previously at the point of collection via the e-QIP system, and again at the beginning of an in person interview. The investigator provides notice and consent details verbally.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [ ] Yes [x] 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, 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.)*

[X] Privacy Act Statement [ ] Privacy Advisory [ ] Not Applicable

Individuals are not provided with notice specifically about PIPS. The Privacy Act advisement, provided on the SF forms and at the beginning of personal interviews, informs the individual on the uses of the information. While that advisement does not explain the system specifically, it does provide information concerning how their information will be used. In addition, notification specifically about this system is provided through publication of this PIA.

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

[X] Within the DoD Component	Specify.	FTS, e-QIP, OPIS, DMRS, NFW, FWS, Arc-Nlets
[X] Other DoD Components	Specify.	DMDC (JPAS)
[X] Other Federal Agencies	Specify.	External Agency Partners including FBI, State Department, USCIS, FINCEN, etc. who provide records in support of the PV mission; as well as sharing PII as necessary with the Suitability and Security Executive Agents.
[X] State and Local Agencies	Specify.	PII is shared with state and local agencies (such as law enforcement agencies) when we conduct LAWE checks, state BAR checks, etc.
[X] 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.	PII is only shared with contracted entities and their respective personnel who have been properly vetted.
[X] Other *(e.g., commercial providers, colleges).*	Specify.	Credit bureas, education instiitiutions, Employment verifuication services.

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

[X] Individuals
[X] Databases
[X] Existing DoD Information Systems
[X] Commercial Systems
[X] Other Federal Information Systems

PIPS accepts the subject-entered data from e-QIP as well as data that may be manually entered by DCSA personnel/contractors, scopes investigative leads, distributes work to field investigators, provides automated National Agency Checks (NAC) such as fingerprints searches to the FBI, supports review of cases, closes cases, and delivers closed cases, as well as advance products to the agencies. PIPS provides automated capability for agencies to upload adjudications, as well as clearance and credential data into CVS.

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

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

System-to-System Information System: FTS, e-QIP, NFW, FWS, and ARC-Nlets.. OMB numbers for forms are noted in section 1.n below.

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.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier PERSONNEL VETTING RECORDS SY

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. N1-478-08-002 and DAA-0446-2019-0004

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

(3) Retention Instructions.

The records in PIPS 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; 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 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 PIPS for 6 months after case closing; but retained according to the retention schedule in OPIS. Credit reports are temporarily retained in PIPS for 7 days after case closing; but retained according to the retention schedule in OPIS. 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 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.

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.

Form Number	Form Name	OMB Number	Expiration Date
SF-85	Questionnaire for Non-Sensitive Positions	3206-0261	09/30/2021
SF-85P	Questionnaire for Public Trust Positions	3206-0258	12/31/2020
SF86	Questionnaire for National Security Positions	3206-0005	02/28/2023
SF-87	Fingerprint Chart	3206-0150	12/31/2020

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)***?** *(Check all that apply)*

[X] Biometrics	[X] Birth Date	[X] Child Information
[X] Citizenship	[X] Disability Information	[X] DoD ID Number
[X] Driver's License	[X] Education Information	[X] Emergency Contact
[X] Employment Information	[X] Financial Information	[X] Gender/Gender Identification
[X] Home/Cell Phone	[X] Law Enforcement Information	[X] Legal Status
[X] Mailing/Home Address	[X] Marital Status	[X] Medical Information
[X] Military Records	[X] Mother's Middle/Maiden Name	[X] Name(s)
[X] Official Duty Address	[X] Official Duty Telephone Phone	[ ] Other ID Number
[X] Passport Information	[X] Personal E-mail Address	[ ] Photo
[X] Place of Birth	[X] Position/Title	[X] Protected Health Information (PHI)[1]
[X] Race/Ethnicity	[X] Rank/Grade	[ ] Religious Preference
[X] Records	[X] Security Information	[X] Social Security Number (SSN) *(Full or in any form)*
[X] Work E-mail Address	[X] If Other, enter the information in the box below	

Aliases used, Personal Conduct, other information requested on applicable forms and during the investigative process from investigation sources.

If the SSN is collected, complete the following questions.

(*DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)*

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

[ ] Yes [X] No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

PIA itself provides justification.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

Security Clearance Investigation or Verification: The initiation, conduct,adjudication, verification, quality assurance, and billing fund control of background investigations and security clearances requires the use of the SSN. The SSN is the single identifier that links all of the aspects of these investigations together. This use case is also linked to other Federal agencies that continue to use the SSN as a primary identifier.

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

[ ] Yes [ ] No

b. What is the PII confidentiality impact level[2]? [ ] Low [ ] Moderate [X] High

[1]The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2]Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

- [ ] Cipher Locks
- [ ] Combination Locks
- [ ] Key Cards
- [ ] Security Guards
- [ ] Closed Circuit TV (CCTV)
- [ ] Identification Badges
- [ ] Safes
- [ ] If Other, enter the information in the box below

(2) Administrative Controls. *(Check all that apply)*

- [x] Backups Secured Off-site
- [x] Encryption of Backups
- [x] Methods to Ensure Only Authorized Personnel Access to PII
- [x] Periodic Security Audits
- [x] Regular Monitoring of Users' Security Practices
- [ ] If Other, enter the information in the box below

(3) Technical Controls. *(Check all that apply)*

- [x] Biometrics
- [x] Encryption of Data at Rest
- [x] Firewall
- [x] Role-Based Access Controls
- [x] Virtual Private Network (VPN)
- [x] Common Access Card (CAC)
- [x] Encryption of Data in Transit
- [x] Intrusion Detection System (IDS)
- [x] Used Only for Privileged (Elevated Roles)
- [x] If Other, enter the information in the box below
- [x] DoD Public Key Infrastructure Certificates
- [x] External Certificate Authority Certificates
- [x] Least Privilege Access
- [x] User Identification and Password

Biometrics will be implemented in the new computer room.

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

Privacy Risk: There is a risk that the information obtained in the course of the investigation will be inaccurate, resulting in an adverse decision for the individual being investigated.
Mitigation: This risk is mitigated by incorporating reviews by a team of case analysts who confirm that the information pertains to the individual being investigated and corroborate the information using various sources.

Privacy Risk: There is a risk that information obtained from commercial sources and electronic records searches will be misinterpreted or that relevant information may be overlooked, resulting in an adverse decision for the individual being investigated.

Mitigation: This risk is mitigated by training investigators regarding how to interpret the information they obtain in the course of the investigation and by having processes in place to validate the information.

Privacy Risk: There is a risk that authorized users may inappropriately access and disclose the information in PIPS for an unauthorized purpose.
Mitigation: This risk is mitigated by assigning specific cases and roles. They can then only see the cases assigned to them, based upon their authorization and privilege. In addition, there are also built in audit logs to monitor disclosures and determine who had access during this time. These logs are checked regularly to ensure that the system was is accessed appropriately.

Privacy Risk: There is a risk of loss or compromise of sensitive information collected through the background investigation process.

Mitigation: This risk is mitigated through the use of multiple layers of physical and IT protection used to safeguard the data. In addition, physical security on the premises ensures that only authorized individuals have access to the building and layered firewalls and data encryption methods ensure it can only be access by authorized individuals on the network.

Privacy Risk: There is a risk that information may be kept longer than is necessary to meet the business need for which it was collected.
Mitigation: This risk is mitigated by DCSA staff following the established retention schedule and documented guidance from NARA, which

clearly defines retention requirements by record type and agency. The risk is also lessened by using the ROID application, a backend application consisting of scheduled batch jobs that purge and minimize investigation data in accordance with internal business need retentions as well as NARA-approved retention schedules.