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:

CAS Apps Suite

2. DOD COMPONENT NAME:

Defense Counterintelligence and Security Agency

3. PIA APPROVAL DATE:

12/19/2025

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) Adjudication and Vetting Services (AVS)'s CAS (Consolidated Adjudcation Services) Apps Suite information suite is currently comprised of six disparate web applications, all of which provide the needed functional and operational capabilities that are absent from the Defense Information System for Security (DISS). These capabilities are described below each application. The applications are hosted as intranet web applications (as opposed to public web applications), restricting access only to NIPR users. To gain access to any of the applications, users in NIPR must navigate to the application's URL using the web browser. Currently, users are automatically authenticated as their NIPR Windows identity. Note that as part of the DoD Zero Trust effort, the applications will soon integrate with the Enterprise Identity Credential and Access Management (E-ICAM) solution to offload user management and authentication to the Defense Information Systems Agency (DISA). Users accessing the applications comprise of both federal and contractor personnel. As the applications deal with case tracking and management, much of the PII and possible PHI will be related to case subjects. AVS handle cases from all categories of individuals detailed in DUSDI 02–DoD: "Personnel for whom DoD conducts or adjudicates background investigations for security, suitability, fitness, and credentialing." When a case arrives at AVS, cases are waiting for an adjudicator to provide an eligibility determination.

***** Application: Productivity Tracker *****

Productivity Tracker handles the following responsibilities: (1) tracking and reporting of adjudicator productivity actions and hours; (2) management and reporting of AVS case inventory, assignments, and timeliness; and (3) management and reporting of AVS case adjudication quality reviews and second reviews. The application also consists of the DISS Ingest component, which reads and stores data found in the daily all open cases report from DISS. While the report includes the subject's SSN, first name, and last name, none of that data is stored in the Millington SQL Server database.

***** Application: Case Works *****

Case Works handles the following responsibility: specialized case management, tracking, and reporting for specialized teams at AVS. Currently, there are four distinct instances of Case Works: Case Works Psych Eval supports psychological assessments; Case Works MAVNI supports the Military Accessions Vital to the National Interest (MAVNI) program; Case Works Linguist supports the linguist program; and Case Works Personal Appearance (PA) supports the personal appearance program. Unlike Productivity Tracker, this application stores PII and PHI long-term within the Millington SQL Server database. PII and PHI are manually entered into the application by the adjudicators.

• PII: subject's full name and aliases, SSN, DOB, birth country, citizenship, languages spoken, and address; PHI: psychological information, medical provider's name, title, address, phone numbers, and address

***** Application: Common Letter Wizard (CLW) *****

CLW handles the following responsibility: generation of official AVS correspondence. This is done through a wizard-like process, in which the chosen letter template is filled in based on the adjudicator's responses. At the end of the process, the adjudicator must download the letter – as either a Microsoft Word or PDF file – to their local workstation to access the letter's contents. Currently, there are two distinct instances of CLW: CLW CAS and CLW VRO, one for each organization before the merger into AVS. The two instances have the same functionality, with the only difference being the letter templates available for adjudicators to use. When letters are generated, the application must

temporarily store the letter as a file on the Willards web server's file system. A copy of the letter needs to be saved on the web server to allow for the user to download the letter. Note that after the adjudicator downloads the letter, CLW no longer touches the letter. After 24 hours, the letter will be removed from the file system.
• PII: subject's full name and SSN (Note that more PII/PHI may be entered dependent on the information needed for the chosen letter template)

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 to support security clearance adjudication for AVS mission-related use and subject identification and verification.

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.

Individuals cannot object directly in CAS Apps Suite. Completion of the SF 85/86 or Personnel Vetting Questionnaire (PVQ) is voluntary, but necessary to initiate the eligibility and/or clearance process.

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 cannot consent directly in CAS Apps Suite, however, consent is given through the completion and certification of the SF85/86 or PVQ.

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

PERSONALLY IDENTIFIABLE INFORMATION
DATA YOU ARE ABOUT TO ACCESS COULD POTENTIALLY BE PROTECTED BY THE PRIVACY ACT OF 1974, AS AMENDED, and the Personnel Vetting Records System, DUSDI 02-DoD, System of Records Notice (SORN). 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.	TD (ADJUDICATIONS)
☐ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	
☐ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	
☐ 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.	
☐ 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)*

- [x] Individuals
- [x] Existing DoD Information Systems
- [ ] Other Federal Information Systems
- [ ] Databases
- [ ] Commercial Systems

PII is initially collected from the data subject when they complete their Standard Form (SF 85/86 or PVQ) and individual adjudicators at AVS. Adjudication records and security clearance information is retrieved from the DISS, Defense Central Index of Investigations (DCII), and the improved Investigative Repository.

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

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

Standard Form (SF) 85/86 or PVQ; DISS Excel report/export is read, parsed, and stored into the CAS Apps Suite information system by the automated DISS ingest process.
For the Case Works applications, adjudicators manually enters case subject PII into the applications. The case subjects themselves do not interact with the CAS Apps Suite information system. Information about Personal Appearance milestones entered into CAS Apps Suite, but not the details of events.

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: DUSDI 02-DoD, Personnel Vetting

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

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

(3) Retention Instructions.

DAA-0446-2019-0004 (0001): Destroy closed cases involving potentially actionable issues 25 years after case closing. Destroy all other closed cases 16 years after case closing.
DAA-0446-2019-0004 (0002): Destroy 30 days after closing date of the related investigation.
DAA-0446-2019-0004 (0003): Destroy entire file 3 years after employment or access to agency facilities and equipment terminates.
DAA-0446-2019-0004 (0004): Destroy 3 years after break. If there is no succeeding report, destroy 3 years from the date of the report.

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. 552, 5 U.S.C. 552a, 32 CFR part 310, 32 CFR part 286. 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 CivilService 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.

Indirect Information Collections:
Defense Information System for Security (DISS), 0705-0008, expiration November 2027
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)