

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:

Managed AI Platform Services (MAPS) IL5 (formerly MINYA-PREPROD-IL5)

2. DOD COMPONENT NAME:

Defense Counterintelligence and Security Agency

3. PIA APPROVAL DATE:

07/01/2026

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 Managed Artificial Intelligence Platform Services (MAPS) system is a IL5 production system designed to host and develop intelligent automation to reduce cost, improve timeliness, and enhance the quality of key DCSA mission areas, especially within areas where processes are repeatable and rely heavily on human labor. MAPS maintains automated solutions such as custom applications and web portals, robotic process automation, and artificial intelligence (AI) and machine learning (ML) workloads. MAPS is not an original point of collection for any data that is analyzed through intelligent automation, rather an analytics platform that enables citizen development and analytics as a service capabilities for the enterprise. All data inputs will be received from internal DCSA mission systems and external data systems that support enterprise operations.

The information scope for the MAPS system includes all mission areas with the primary focus being personnel vetting data elements maintained within NBIS data systems, such as DISS and MIRADOR. This system will process multiple elements of the clearance adjudication, re-adjudication, and continuous vetting process such as SF-86, Results of Investigation (ROI), and Subject Enrollment Data. The system will filter data based on business rules, provide the ability to perform link node analysis, conduct entity resolution, facilitate data science-based investigations, and run AI and ML algorithms to produce curated data products to augment mission operations.

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 for verification, data matching, and administrative use, as needed by the intelligent automation use case. Based on PII, the information can later be retrieved to correctly reconstruct an investigative history of an entity (i.e., person or secure facility).

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.

Direct objection to the collection of PII is not provided through MAPS because MAPS is not the original point of collection. Objection is waived when the subject completes and submits the SF's.

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.

Direct consent is not provided through MAPS because MAPS is not the original point of collection. Consent, where applicable,

is afforded when a subject completes the SFs

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 do not have access to the MAPS system. However, subjects and sources are provided a Privacy Act Statement when completing investigative forms and/or upon interview.

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 Security
Industrial Security
Counterintelligence & Insider Threat
Department of Defense Insider Threat Management and
Analysis Center - System of Systems (DITMAC-DSoS)

☐ 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.

Booz Allen Hamilton:

Specific FAR privacy clauses are not directly identified, however the following language is contained within:

Article XIV, Section B: Protecting Controlled Unclassified Information in Non-federal Information Systems (page 22): This clause mandates the protection of "covered defense information," which includes PII, and requires adherence to NIST standards.

- "The Performer shall Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies--"

Article XIV, Section B: Protecting Controlled Unclassified Information in Non-federal Information Systems (page 22): This clause mandates the protection of "covered defense information," which includes PII, and requires adherence to NIST standards.

- "The Performer shall provide adequate security to safeguard covered defense information that resides on or is transiting through the performer's internal information system or network, as outlined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Non-federal Information Systems.""

Article XIV, Section N: Privacy Act of 1974 (page 28): This section explicitly requires compliance with the Privacy Act.

- Privacy Act of 1974: "The Performer shall Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies-The systems of records; and The design, development, or operation work that the Performer is to perform;"

- "The Performer shall include the Privacy Act notification contained within this agreement in every sub-agreement when the work statement in the proposed sub-agreement requires the design, development, or operation of a system of records on individuals that is subject to the Act;"

☐ 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

- National Background Investigations System (NBIS) - Investigation Management
- [OPIS] The Office of Personal Management (OPM)
- Personnel Investigations Processing System (PIPS)
- National Industrial Security System (NISS)
- National Industrial Security Program (NISP) Contract Classification System (NCCS)
- 847/FRMS (FOCI Risk management system)
- Director of National Intelligence (DNI) - CES Continuous Evaluation Service
- Defense Information System for Security (DISS)
- Dashboard Management Reporting System (DMRS)
- Integrated Security Data Services (ISDS)
- Mirador (FBI)

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)

MAPS will retrieve data from internal and external sources using application programming interface (API) connections, S3 bucket connections, and manual file transfers.

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

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcl.d.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-0446-2016-0001
DAA-0446-2017-0001
DAA-0446-2019-0001
DAA-0446-2019-0004
DAA-0446-2020-0001

DAA-0446-2021-0009

DAA-0446-2022-0013

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

(3) Retention Instructions.

DAA-0446-2017-0001-0001 Destroy when no longer needed
 DAA-0446-2017-0001-0003 Destroy when no longer needed
 DAA-0446-2019-0001-0001 Destroy when superseded in accordance with DAA-0446-2017-0001-0009
 DAA-0446-2019-0001-0002 Destroy 6 years(s) after contract closeout
 DAA-0446-2019-0001-0003 Destroy when superseded or 6 years after contract closeout
 DAA-0446-2022-0013-0001 Other: Facility profiles of terminated facilities that do not have associated FOCI mitigation agreements will be deleted from NISS 10 years after facility termination. Facility profiles of terminated facilities that have associated FOCI mitigation agreements will be deleted from NISS 15 years after facility termination.
 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 closed cases involving potentially actionable issues after 25 years. Destroy all other closed cases after 16 years.
 DAA-0446-2019-0004-0004 Destroy entire file 3 years after employment or access to agency facilities and equipment terminates.
 DAA-0446-2019-0004-0005 "Place in inactive file on receipt of succeeding report. Break inactive file annually. Destroy 3 years after break. If there is no succeeding report, destroy 3 years from the date of the report."
 DAA-0446-2021-0009-0001 "Cut off after closing date or the date of the most recent investigative activity. Destroy 16 years from the date of closing or the date of the most recent investigative activity, whichever is later."
 DAA-0446-2021-0009-0002 "Cut off after closing date or date of the most recent investigative activity. Destroy after 25 years from the date of closing or the date of the most recent investigative activity, whichever is later."
 DAA-0446-2016-0001-0001 "Cutoff is after investigative closing or date of the most recent investigative or operational activity. Destroy after 25 years from the date of closing or the date of the most recent investigative or operational activity, whichever is later."
 DAA-0446-2020-0001-0001 Destroy 15 year(s) after the date of the last action
 DAA-0446-2020-0001-0002 Destroy 25 year(s) after the date of the last action
 DAA-0446-2020-0001-0003 Destroy 15 year(s) after last action

5 U.S.C. 301, Departmental Regulations; E.O. 10450, Security Requirements for Government Employment; DoD Directive 5200.2, DoD Personnel Security Program (32 CFR part 156); and E.O. 9397, as amended (SSN)

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 statute 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. 301, Departmental Regulations; E.O. 10450, Security Requirements for Government Employment; DoD Directive 5200.2, DoD Personnel Security Program (32 CFR part 156); and E.O. 9397, as amended (SSN)

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.

This system does not directly collect data from members of the public. Instead, the data is retrieved from the sources of PII as described in section 1.i (above).

OMB 0704-0567 - National Industrial Security Program (NISP/NCCS: Contract Classification System) - exp 8/31/2028
 OMB 0705-0002 - SF-87: Fingerprint Chart - exp April 2027 (DCSA) - exp 04/30/2027
 OMB 0705-0003 - Federal Background Investigation and Personnel Vetting Investigative Request Forms (INV 40-44) - exp 10/31/2027
 OMB 0705-0004 - Investigative Interview Survey (newly identified) - exp 10/30/2028
 OMB 0705-0005 - FOCI Outside Director/Proxy Holder Nomination Questionnaires - exp 04/30/2029
 OMB 0705-0006 - National Industrial Security System (NISS) - exp 05/31/2028
 OMB 0705-0007 - Personnel Security Investigation (PSI) Projections - exp 11/30/2027
 OMB 0705-0008 - Defense Information System for Security (DISS) - exp 11/30/2027
 OMB 0705-0009 - Personnel Security System Access Request Form (DD Form 2962) - exp 05/31/2028
 OMB 1110-0046 - FD-258: Standard Fingerprint Form (FBI) (FBI Managed) - exp 09/30/2026
 OMB 3095-0058 - SF-714: Financial Disclosure Oath (ODNI) - exp 04/30/2028
 OMB 3206-0005 - SF-86: Questionnaire for National Security Positions - exp 11/30/2026
 OMB 3206-0182 - Optional Form (OF) 306 Declaration for Federal Employment form (Replaces SF-171) - exp 08/30/2026
 OMB 3206-0258 - SF-85P: Questionnaire for Public Trust Positions - exp 04/30/2027
 OMB 3206-0258 - SF-85P-S: Supplemental Questionnaire for Selected Positions - exp 04/30/2027
 OMB 3206-0261 - SF-85: Questionnaire for Non-sensitive Positions - exp 12/31/2027