PRIVACY IMPACT ASSESSMENT (PIA)

For the

Personnel Security Branch (PSB) Case Management (CM)
Mission Assurance Division (MAD) - Defense Health Agency (DHA)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☐	**New DoD Information System**	☒	**New Electronic Collection**
☐	**Existing DoD Information System**	☐	**Existing Electronic Collection**
☐	**Significantly Modified DoD Information System**		

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☐	**Yes, DITPR**	Enter DITPR System Identification Number	
☐	**Yes, SIPRNET**	Enter SIPRNET Identification Number	
☒	**No**		

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☐ **Yes** ☒ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

☒ **Yes** ☐ **No**

If "Yes," enter Privacy Act SORN Identifier Working with DHA PCLO to draft a new SORN.

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an 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**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

50 U.S.C. 3161, Procedures; E.O. 10450, Security requirements for Government employment; E.O. 12968, Access to Classified Information; E.O. 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust; Homeland Security Presidential Directive (HSPD)-12, Policy for a Common Identification Standard for Federal Employees and Contractors; DoDD 1000.25, DoD Personnel Identity Protection (PIP) Program; DoDI 1000.13, Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals; DoD 5200.2-R, Personnel Security Program; DoD Manual 5200.01, Volume 1, DoD Information Security Program: Overview, Classification, and Declassification; and E.O. 9397,(SSN) as amended.

NOTE: The references above are a non-exhaustive list which may provide legal authority to run the PSB CM application as described in the draft PIA. However, the system will not be in line with the requirements of the Privacy Act until an applicable SORN is established.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The PSB Case Management is a Web-based application. Its purpose is to assist members of the MAD PSB (known as Users) in tracking government investigations (Military, Civilian, Contractor, Consultants and Public Health) during the Common Access Card (CAC) and Security Clearance process. This application will facilitate the PSB reporting capabilities and will allow for a fully functional, searchable, sortable PSB Case Management . It is being built and secured by Defense Information Systems Agency (DISA) Application Security Technical Implementation Guides (STIGS). The PSB Case Management will be CAC-enforced and users are restricted using Role-Based Access Controls.

Information collected includes Personally Identifiable Information (PII), such as name, Social Security Number, date and place of birth, security clearance level, and work history. The information utilized for the PSB CM is garnered from two already existing OMB-approved Federal forms: Standard Form (SF) 86 (Questionnaire for National Security Positions) used to apply for Security Clearances and DHA Form 33 (Request for DoD Common Access Card Trusted Associate Sponsorship System Registration) used for obtaining a CAC card.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Privacy risks include data leakage, such as the unauthorized release of PII/PHI data to include identity theft, sharing of PII with those who have no need to know, unsolicited marketing, and compromise of sensitive information.

These risks have been mitigated through physical, technical, and administrative controls, such as adhering to all DoD and standard encryption practices and DISA STIGs.

The application is CAC-enforced. Users must be approved and have the need-to-know.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. Defense Health Agency, Mission Assurance Division, Personnel Security Branch

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. Authorized users within DHA MAD Personnel Security Branch

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

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

PSB CM is not the initial point of collection. The information utilized for the PSB CM is garnered from two already existing OMB-approved Federal forms: SF 86 used to apply for Security Clearances trust and DHA Form 33 used for obtaining a CAC. Individuals would need to object to those forms if they did not want to disclose PII.

j. 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.

PSB CM is not the initial point of collection. Consent would have to have to be given when they complete one or both of the previously mentioned forms.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐	**Privacy Act Statement**	☐	**Privacy Advisory**
☐	**Other**	☒	**None**

Describe each applicable format.

PSB CM is not the initial point of collection of PII.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.