PRIVACY IMPACT ASSESSMENT (PIA)

For the

PACAF Enterprise Information Management - Decision Support Integration (EIM-DSI) System
US Air Force

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 1977

☐ **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 OPM/GOVT-1

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.

Executive Order 9397, 10 United States Code 8013 and functional user requirements:
(1) CPTS – 15 CPTS/FMF,
(2) MPF – 15 MSS/DPM and
(3) EMS – HQ PACAF/CCQ.

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.

- Activity/Purpose:
-- CPTS – Web application to manage appointments for Inprocessing, and Retirements/Separations appointments, supporting 15 CPTS business processes.
-- MPF – Web application to manage appointments for MPF Customer Service support (DEERS updates, ID/CAC card issuance, etc.), supporting 15 MSS MPF Customer Service.
-- EMS – SharePoint custom task list to semi-automate processing and staffing of military officer performance reports, enlisted performance reports and military decoration documentation.
- Present Lifecycle Phase: Production/Sustainment
- System Owner: PACAF CSF/A6I
- System Boundaries and interconnections: EIM-DSI System boundary includes all EIM-DSI regional web and database servers, including the servers on which CPTS, MPF and EMS are hosted. The EIM-DSI system does not interconnect with any other system. The EIM-DSI system does connect to and obtain network core services from the Hickam Base Area Network (HBAN), administered by 15CS and 561 NOS Det 1.
- Location of system and components: Hickam AFB, HI building 1102.
- System Backup: Addressed in SSAA Appendix L, Contingency Plan, published in EITDR and available upon request. All EIM-DSI data is stored on the Hickam SAN. SAN and related backup/recovery services are included in the HBAN core services received/provided by 15CS NCC and 561 NOS Det 1 (PACAF NOSC).

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

Risks: Collection risk is borne by application users which is voluntary (CPTS/MPF). EMS does not collect additional PII data, but does process it via files uploaded to the related SharePoint web page/site. PII data in uploaded files is obtained from performance report "shell" files by the external non-interfacing existing military personnel system (MILPDS) system measures.

Safeguards:
(1) CPTS - .mil w/CAC access, (2) MPF - .mil w/CAC, (3) EMS – PACAF AOR .mil accounts w/CAC. Application-level permissions are limited by role for users/facility staff/full admin. Only users with sufficient roles/ permissions are authorized to execute specific application features/transactions. Administrative/ business processes include using application features to limit access to your own data only. This prevents the end user from having access to someone else's PII. For instance, end users of MPF can only tell that a particular appt slot is taken or not (MPF staff and administrators can see the appt details for all appts for all users). System admin/ database admin permissions are role/group-based and limited to those with validated responsibilities/need to know. Only authorized administrators have access to the databases themselves. We continue to work with the functional application owner to limit online data available in the active database and backup data to 90 days of appointments. This would limit the amount of PII stored in the database in the event of a data breach. Full IA control information is posted in EITDR. For EMS, only the member's chain of command, orderly room and base military personnel flight staff have access to the member's personnel records and EMS sites/files. EMS site permissions are limited to that member's chain of command.

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. USAF - Data is for internal PACAF use only and is not shared outside PACAF.

☐ **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. PACAF ETS II support contractors who perform system administration are required to protect all system information IAW public law.

☐ **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.

PII in CPTS, MPF and EMS is already collected through different sources (MILPDS, smart card, individual PACAF directorate employee OPR/EPR databases, feedback databases, or training databases), so PII collection/use should not ever be objectionable. Use of the web application constitutes consent to the data collection and specific uses of the PII, per Privacy/Security Notice link on homepage. Individual grants consent to collection/use (and security monitoring etc.) via entering the PII data at all. Instructions are posted on the application homepage (Privacy Advisory and Privacy Act Statement) explaining who the user should contact if they decline to disclose any PII data, and/or to make arrangements for scheduling the appointment using alternative means.

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

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.

PII in CPTS, MPF and EMS is already collected through different sources (MILPDS, smart card, individual PACAF directorate employee OPR/EPR databases, feedback databases, or training databases), so PII collection/use should not ever be objectionable. Use of the web application constitutes consent to the data collection and specific uses of the PII, per Privacy/Security Notice link on homepage. Individual grants consent to collection/use (and security monitoring etc.) via entering the PII data at all. Instructions are posted on the application homepage (Privacy Advisory and Privacy Act Statement) explaining who the user should contact if they decline to disclose any PII data, and/or to make arrangements for scheduling the appointment using alternative means.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

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.

Per applicable Air Force Instructions.

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.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]