PRIVACY IMPACT ASSESSMENT (PIA)

For the

Correspondence and Tasks Management System (CATMS)
WHS

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	15960
☒	**Yes, SIPRNET**	Enter SIPRNET Identification Number	16845
☐	**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 007-000001906

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 DWHS E06

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.

10 U.S.C. 113, Secretary of Defense;
DoD Directive 5105.53, Director of Administration and Management (DA&M);
DoD Directive 5110.4, Washington Headquarters Services (WHS); and
E.O. 9397(SSN), as amended.

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 Correspondence and Tasks Management System (CATMS) is comprised of the core Tasks Management Tracker tool (TMT) and the Correspondence Management Division module (CMD). The CMD module supports the Secretary of Defense for the control and tracking of actions taken and responses from the Secretary to the President, White House staff, other Cabinet officials, Congress, state and local officials, corporate officials, members of the Department of Defense and the public. This includes full life-cycle management from receipt, control of metadata and image, tasking the OSD Components, Joint Staff, Services and other DoD agencies for action and records management. TMT is used by component Offices of the Secretary of Defense to process and manage the staffing and coordination of actions (which include but are not limited to personnel and staffing) to, from, and within components in the conduct of official daily business. PII collected includes but is not limited to name, SSN, home address, e-mail address and other information provided needed to address the individual's issue or concern. The minimum amount of PII data is collected to facilitate processing of the correspondence and ensure efficient operation of the Offices of the Secretary of Defense while complying with other requirements such as Freedom of Information Act and records retention.

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

It is possible that a user may inadvertently or intentionally disclose PII to an unauthorized user. Users are required to take annual IA training as referenced in DoDI 8500.2. Role-based security is in place to allow only appropriate users associated with the staff action access to the data. Users not associated with the staff action containing the correspondence can not access the data. Risks regarding the collection, use and sharing of PII in the system have been minimized through system design and implementation of various administrative, technical, and physical security controls. Specifically, these risks are addressed by protecting the data collection resource with strong SSL encryption, programmatically restricting the system from releasing PII data through its interfaces, mutual authentication using Kerberos and timestamps, under the routine use guidelines authorized in the Privacy Act SORN, through periodic information assurance certification of personnel with access to the PII, and through access control restricted by CAC to internal network personnel whose job functions require access to PII.

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. Personnel responsible for processing correspondence containing PII.

☒ **Other DoD Components.**

Specify. All DoD Components that have equity in a specific action containing PII.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify.

☐ **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.

Submission of correspondence is completely voluntary and the members of the public writing DoD officials determine what, if any, PII they provide. Since the correspondence is sent, the individual inherently agrees any information collected may be linked to them for tracking of the action requested. This PII is only available to those individuals with a bona-fide need to know in the performance of their duties (and consistent with proper training).

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

DoD employees (military and civilian) cannot object to the inclusion of their PII in the document management portion of this system. They are provided an opportunity to object to collection when the information is initially requested/collected.

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.

Constituent correspondence is not solicited and reflects information unique to each constituent need. Constituents may not know that their letters and e-mail are being entered and tracked in CATMS. Members of the public consent to specific uses of their PII by submitting the PII as part of correspondence addressed to congressional and DoD officials and may withhold consent by not including PII.

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

DoD employees (military, civilian, and contractor) cannot provide consent since they do not submit the personnel-related packages directly but are the subjects of these packages.

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.	Because constituent mail is submitted at the initiation of the constituent about issues that the constituent raises, there is no effective way for OSD to provide adequate notice (i.e., there is no solicitation). With respect to staff packages for personnel matters for DoD military personnel, civilian employees, and contractors, the packages are not submitted by the individual but submitted by the appropriate office. Any applicable forms completed by the individual has an appropriate Privacy Act Statement.

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.