PRIVACY IMPACT ASSESSMENT (PIA)

For the

Enterprise Content Management Services
Army Publishing Directorate

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: 1681 (DA76873)
- ☐ **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 A0025-1 CIO G6

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. 3013, Secretary of the Army; Department of Defense Directive 8500.1, Information Assurance (IA) Army Regulation 25-2; DoD Instruction 8500.2, Information Assurance Implementation; AR 25-1, Army Knowledge Management and Information Technology; 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 Purpose of Enterprise Content Management Services (ECMS) is to perform knowledge management in order to facilitate electronic communications and business processes among DoD personnel and other authorized guest users. This system servers as an Army controlled repository for information needed by DoD personnel necessary for performance of duties and other DoD related functions. ECMS serves as a host for numerous Army applications and provides protection for those applications through role-based access. Access is controlled based on individual needs for specific types of information to perform official duties. Statistical data with all personal identifiers removed, may be used by management for system efficiency, workload calculation or reporting purposes.

ECMS is a centralized, authoritative library of electronic forms and publications (over 2,400), that is web-accessible, secure, accessed through Army Knowledge Online and available for use by anyone in the Department of Army (DA). These forms are open standards XML and can serve as a "universal user interface" to any IT system. ECMS has a means of routing these forms to other members of the DA, tracking their progress, and viewing their status. To supplement ad hoc routing, the form is sometimes configured for "self routing" at key steps. A more sophisticated form of routing, when needed to meet the requirements or constraints of the underlying process, is available as a full routing capability. The service has a way to bundle word documents, excel documents, portable document format (PDFs) and other documents with a form, as attachments, to create a complete "package". These "bundles" of forms and documents can also be created with routable "folders". Also, a digital signature tool enabling online, authoritative approval of forms, and other documents, which adhere and allows the enforcement of integrity, confidentiality and non-repudiation that Department of Defense (DoD) Public Key Infrastructure (PKI) offers.

ECMS supports an offline processing capability that allows most work to be completed in an environment with intermittent connectivity. ECMS provides a reporting capability that enables the presentation of information on forms, users or processes is a top down and bottom up tool for all users. ECMS is also a seamless and convenient way of connecting to authoritative data sources and systems, this is the ramifications needed to have data move across efficiently and securely across the Global Information Grid (GiG). Inherently in ECMS is a means of efficiently searching through forms, way of declaring forms as records, compliant with DoD 5015.2, with a mechanism for automatically categorizing forms and associated documents using a system "trained" by experts and a convenient way to access documents or capabilities in local, legacy systems. It also provides a logic workflow to allow any organization to build an intelligent workflow process.
PII collected include personal, financial, employment, medical, and military.

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

ECMS utilizes the Army Knowledge Online Lightweight Directory Access Protocol Data Store (LDAP) & Integrated Total Army Personnel Database (iTAPDB) which tracks personal identifiable information of military members (system users). System users may upload documents that contain PII from various Army Programs and support functions depending on the subject matter. The source of this information is directly from system users, their individual record objects, and other Army activities and personnel database systems.

Internal and external risks are associated with the protection of PII; however, risks are minimized to an acceptable level. Safeguards are employed to detect and minimize unauthorized disclosure, modification and/or destruction of data.

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.

Department of Defense/Department of the Army
Army Deputy Chief of Staff for Personnel
Army G1
Army Reserve Command
National Guard Bureau
Department of the Army Inspectors General
Army Staff Principals in the chain of command and Supervisors and their designated human resources and administrative personal responsible for processing personnel actions
Army MEDCOM
Office of the Provost Marshall General
Army IMCOM

☐ **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.

Dynamic Technology Systems.
The contractor is required to follow Department of Defence (DoD) policy and standards regarding the safe and secure procurement, storage and maintenance of personal identifiable information.

☐ **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.

The majority of the PII will be collected from other authorized systems (such as AKO LDAP & ITAPDB) and documents. Soldiers will have the opportunity to object to the PII collected directly from themselves.

(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.

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

Because of the services provided by the attached systems (eMEB, ePEB, etc.), users are required to provide PII. It is used as the primary information link to users and any of their attached cases within the ECMS enclave. Users can, through the submission of their PII, directly administrator previously submitted cases and only their cases, within the ECMS enclave.

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.

DD FORM 2005, FEB 1976

YOU ARE ACCESSING A U.S. GOVERNMENT (USG) INFORMATION SYSTEM (IS) THAT IS PROVIDED FOR USG-AUTHORIZED USE ONLY.
By using this IS (which includes any device attached to this IS), you consent to the following conditions:

The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
At any time, the USG may inspect and seize data stored on this IS.
Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
This IS includes security measures (e.g., authentication and access