PRIVACY IMPACT ASSESSMENT (PIA)

For the

FINANCIAL MANAGEMENT INFORMATION SYSTEMS (FMIS)
ARMY MATERIEL COMMAND (AMC) COMMUNICATIONS ELECTRONICS COMMAND (CECOM LCMC)

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: 3003 (DA05468)
- ☐ **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: A0690-200 DAPE

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: 20120531

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.

(1) 10 U.S.C. 3013, Secretary of the Army;
(2) Army Regulation 600-8-22
(3) 10 U.S.C. Section 3013, Secretary of The Army;
(4) E.O 9397 (SSN), as amended.
(5) DoD Directive 8320.0 Data-Sharing in a Net-enteric Department of Defense
(6) DoD Directive 81001.1 Global Information Grid (GIG) Overarching Policy

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.

Financial Management Information System (FMIS) is a reporting system that collects data from accounting and civilian personnel systems. Customers identified in section 2h drive the reporting process.

Financial Management Information System (FMIS) is an integrated data mining, business intelligence tool that enables Army organizations to rapidly compile operational data from its disparate legacy financial, acquisition, logistics, personnel, payroll and local unique systems. Current legacy systems include: SOMARDS (Standard Operation Maintenance and Research and Development System), MOCAS (Management of Contract Accounting System), DCPDS (Defense Civilian Personnel Data System), DCPS (Defense Civilian Payroll System), and local systems.

FMIS utilizes exclusive E/T/L to deliver consolidated data to customers via the web. The web utilizes HTML and ASP.NET. FMIS operates on a windows platform utilizing Microsoft SQL Server. FMIS output reports include: Analysis Cubes, Crystal Reports, Excel, Graphs, and also offers user input capability. Some of the benefits to using FMIS are: centralized and faster access to data, integrated data, reduced labor cost, provides time to concentrate on mission, increased data visibility resulting in improved data quality, tools to generate flexible and in-depth business reports for better decision making, reduces portfolio cost.

The FMIS system has customers throughout the Communications-Electronics Command (CECOM) and Program Executive Office (PEO) communities.

The type of PII collected is personal, financial, educational, and employment information.

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

Risk: PII Location
Mitigation: PII data is located on servers within government controlled datacenters. These facilities are controlled and restricted to personnel with authorized security clearances and need to know. To ensure controlled access, accessibility utilizes two-factor authentication.

Risk: Customer web access
Mitigation: The website is secured by using SSL. Users authenticate using Army Knowledge Online authentication and therefore conforms to Army policy for creating and changing passwords. Access to reports is limited to customers for official use only.

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. Army Materiel Command (AMC), Communications Electronics Command LCMC (CECOM LCMC), CECOM LCMC Personnel Policy and Planning (CECOM LCMC G1), CECOM LCMC Operations and Planning (CECOM LCMC G3/G5), CECOM LCMC Resource Management (CECOM G8), CECOM LCMC Software Engineering Center (CECOM LCMC SEC), Base Installation Garrison Commands, Civilian Personnel Advisory Centers, Scientists and Technology Demonstration Project, CECOM LCMC SEC Personnel Action Tracker.

☐ **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. Contractors support the office through system administration, and maintenance. The contractors who have access are in support of other government systems and their access is limited according to FOUO and the requirements specified in support of their system.

☐ **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.

The information is collected through DCPDS and legacy financial systems for government civilians within the C4ISR data constraints and organizations within Army Materiel Command.

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.

The information is collected through DCPDS and legacy financial systems for government civilians within the C4ISR data constraints and organizations within Army Materiel Command.

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.

The system does not collect PII data directly from the individual. It is gathered through the sharing of information from other systems that have Privacy Act Statements.