PRIVACY IMPACT ASSESSMENT (PIA)

For the

Army Food Management Information System (AFMIS)

Army Materiel Command (AMC) - Communications Electronic Lifecycle Management Command (CECOM)

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: 238 (DA00202)
- ☐ **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 007-21-01-03-02-0147-00

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 G/6

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);
DoD Instruction 8500.2, Information Assurance Implementation;
AR 25-1, Army Knowledge Management and Information Technology;
Army Regulation 25-2, Information Assurance;
and E.O. 9397, as amended (SSN).

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 Army Food Management Information System (AFMIS) is an automated system supporting the management of Army Food Service Operations, to include 60 Army/Reserve installations, and 411 dining facilities - worldwide. AFMIS is currently a web base application with clients to support automated head count and is past Milestone IV. Software Change Package (SCP) 14 migrated AFMIS to a web environment that eliminated near end-of-life back office computers in dining facilities and installation servers; and brought Army worldwide subsistence execution into a single reporting system. AFMIS also includes Scan and Go head count and Headquarters Reporting (Decision Support System). AFMIS interfaces with Subsistence Total Ordering Receipting Electronic System (STORES) for catalogs, orders, and receipts; AFMIS interfaces with operation data store (ODS) to send obligation and accrual and adjustment transactions to DFAS. Contractor support to AFMIS encompasses software engineering to include coding, training of installation functional personnel and system administrators, deployment of technical upgrades and customer support to users worldwide. AFMIS includes online help for all processes and functional training which is available for all users of AFMIS. AFMIS provides software upgrades and customer support to 475 point-of-sale stations at 60 installations.

The type of PII collected includes personal, employment and military information.

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

Every system has the potential for information to become compromised and accessible by individuals without an official need-to-know, whether through conventional hacking techniques, lost media, or intentionally by an insider. The system has implemented the latest cyber security safeguards to reduce an outside attack and lower the risk of lost electronic media. Every individual who has access to the system, with regards to using the entered data, has undergone a security background review and privacy and security training.

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. All Army components and major commands which includes Active Duty, Army Accessions Command, Army Criminal Investigation Command, Army Deputy Chief of Staff for Personnel, Army Intelligence and Security Command, Army Medical Department, Army Research Institute, Army Reserve Command, Army Training and Doctrine Command, Assistant Secretary of the Army (Financial Management & Comptroller), Department of the Army Inspectors General, Provost Marshal General, Army Staff Principals in the chain of command, and Supervisors and their designated human resources and administrative personnel responsible for processing personnel actions.

☒ **Other DoD Components.**

Specify. Defense Criminal Investigative Service, Defense Finance and Accounting Service, Defense Manpower Data Center, Defense Security Service, National

Guard Bureau, Office of the DoD Inspector General, Office of the Secretary of Defense, Office of the Secretary of Defense Personnel and Readiness, and U. S. Military Entrance Processing Command, Department of the Navy, Marine Corps, Coast Guard, Department of the Air Force.

☒ **Other Federal Agencies.**

Specify. Office of Personnel Management; Department of Veterans Affairs, Department of Homeland Security, Department of Health and Human Services, Federal law enforcement and confinement/correctional agencies, Department of the Treasury, and the Social Security Administration.

☐ **State and Local Agencies.**

Specify.

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

Specify. The system is maintain by contractor personnel from Dynamic Resource Corporation. These personnel are required to receive annual training concerning protecting PII. The following is extracted from the contract:
5.1.4 The contractor shall not divulge any information regarding files, data, processing activities/functions, user ID's, passwords, or other knowledge that may be gained, to anyone who is not authorized to have access to such information. Contractor personnel shall abide by all Government rules, procedures, and standard of conduct. Contractors requiring access to Government Automated Information Systems (AIS) shall have background investigations and security awareness training completed, after task order award but prior to AIS access. When the period of performance is complete or and contractor personnel leave work on this project they will have 5 days to terminate all their network user account and to return all access cards and base identification badges.

☐ **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.

Yes, If individual refuse to provide their government ID which contain their PII they are objecting to the collection of their PII. When individuals receive their government ID cards (CAC, government facility ID, and military ID) they are given Privacy Act statements that explains the collection and use of their PII. If individuals object to having their government ID cards scanned they are not allowed access to military dining facilities.

(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.

No, individuals do not have the opportunity to consent to the specific uses of their PII. If and when individuals provide their government ID cards for scanning in order to be given access to military dining facilities they are not given the opportunity to consent to the specific uses of their PII. If they refuse to allow their government ID to be scanned they are not allowed access to the military dining facility.

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.

When individuals receive their government ID cards (CAC, government facility ID, and military ID) they are given Privacy Act statements that explains the collection and use of their PII.