PRIVACY IMPACT ASSESSMENT (PIA)

For the

DeCA Electronic Records Management Archiving System (DERMAS)
Defense Commissary Agency

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: 817
- ☐ **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 0556

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

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. 01/2011

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.

5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C Chapter 147, Commissaries and Exchanges and Other Morale, Welfare and Recreation Activities; 32 C.F.R. Part 383a, Defense Commissary Agency (DeCA); 44 U.S.C. Chapters 29, 31 and 33, Records Management; 36 C.F.R. Sub-chapter B, Records Management; DoD Directive 5015.2, DoD Records Management Program; Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons, dated November 22, 1943, as amended by Executive Order 13478, Amendments To Executive Order 9397 Relating to Agency Use of Social Security Numbers, dated November 18, 2008.

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 Defense Commissary Agency (DeCA) is implementing a new system of records to facilitate the filing, maintenance, storage, preservation, retrieval and disposition of records containing Personally Identifiable Information (PII)and documenting the organization, functions, policies, decisions, procedures, and essential transactions required for the management and business functions required for the administration of a 24/7, worldwide organization, and to protect the legal and financial rights of the U.S. Government and of persons directly affected by DeCA's activities including current, retired and former DeCA employees; current and past DeCA contractors; DeCA patrons; DeCA Business Partners personnel, including contractors, manufacturers, vendors brokers and distributors doing business with DeCA; military service personnel; personnel of the military service exchange services (Army Air Force Exchange Service (AAFES)/Navy Exchange Service Command (NEXCOM)/Marine Corps Exchange (MCX)/ Coast Guard Exchange System (CGES) personnel; and other individuals who communicate with or receive communications from DeCA. PII collected: Name, SSN, residence address, home telephone numbers, mobile (cell) phone number(s), home or personal e-mail addresses.

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

Data with Personally Identifiable Information (PII): Although the data contained in the system is sensitive in nature, the privacy risks associated with the PII data are minimal due to the measures taken to meet Information Assurance requirements for this type of data, and the handling of the data by personnel trained in the privacy regulations governing the safeguarding of this data and who are charged with the responsibility of protecting it. In addition, electronic records are maintained in a password-protected network and accessible only to DeCA personnel, management, and administrative support personnel on a need-to-know basis to perform their duties. Access to the network where records are maintained requires a valid Common Access Card (CAC). Electronic files and databases are password protected with access restricted to authorized users. Private identifiable information is protected in accordance with the requirements of the Computer Security Act of 1987 (P.L. 100-235). Employees and contractors are required to comply with the Handbook for Safeguarding Sensitive Personally Identifiable Information and the Privacy Program Manual, which details security and privacy controls for the appropriate handling of sensitive personal 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. The following DeCA departments have access to records containing PII: Human Resources Department, Equal Employment Opportunity Department, Records Management-Payroll Section and General Counsel.

DERMAS receives PII information from two sources: automated pdf document feeds from the TAS system or documents scanned by authorized users.

☒ **Other DoD Components.**

Specify. Personnel of the Defense Finance and Accounting Service (DFAS), Columbus, OH and Defense Logistics Agency providing support to DeCA activities.

☒ **Other Federal Agencies.**

Specify. Office of Workers Compensation Program, Department of Labor, Office of Personnel Management

☐ **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.

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

Data containing Personally Identifiable Information (PII): While individuals have the opportunity to object to the collection of PII at the time it is originally collected, this system entails no original collection of PII from individuals, but instead is a compilation of information from existing hard copy documents and electronic databases, there is no opportunity to 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.

Data with Personally Identifiable Information (PII): Individuals have the opportunity to object to the collection of PII at the time it is originally collected. This system entails no original collection of PII from individuals, but instead is a compilation of information from existing hard copy documents and electronic databases, there is no opportunity to object.

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.

Human Resource Data: When the information is collected from the employee, various forms are completed. Each form has the appropriate Privacy Act Notice on it. The notice below is an example for the Thrift Savings Plan (TSP) forms.

PRIVACY ACT NOTICE: We are authorized to request the information you provide on this form under 5 U.S.C., Chapter 84, Federal Employees Retirement System. We will use this information to identify your TSP account and to process this form. In addition, this information may be shared with other federal agencies for statistical, auditing, or archiving purposes. We may share the information with law enforcement agencies investigating a violation of civil or criminal law, or agencies implementing a statute, rule or order. It may be shared with congressional offices, private sector audit firms, spouses, former spouses, and beneficiaries, and their attorneys. We may disclose relevant portions of the information to appropriate parties engaged in litigation and for other routine uses as specified in the Federal Register. You are not required by law to provide this information, but if you do not, we will not be able to process your request.

All Other Data:
Information acquired from system-to-system interfaces/data transfer is not collected from individuals. Notification of Privacy Act information is the responsibility of the source system(s).

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 concern