



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Enterprise Data Warehouse (EDW)
Defense Commissary Agency (DeCA)

### **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
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

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
- 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

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.

**Human Resources Data:**

1. Privacy Act SORN: DoD requested that all component personnel systems attach to OPM's system notice - OPM-GOVT-1.

2. Authority for DoD electronic collection: Authority to create the Defense Civilian Personnel Data System (DCPDS), which includes the reporting tool (database), was directed by Program Budget Decision 711, "Corporate Information Management Initiatives", December 5, 1994.

**All Other Data:**

DoD Directive 1330.17, Military Commissaries, and Executive Order 9397 (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.

**Human Resources Data:**

The Human Resources (HR) data mart is an Oracle database that provides a single point of reference for all DeCA civilian personnel information. Information contained in DeCA's HR data mart is not accessible by the public and contains no personal information on any persons other than DeCA federal civilian employees. The data in DeCA's HR data mart is accessed by authorized HR users: (1) to track the processing of personnel actions in the Defense Civilian Personnel Data System (DCPDS); (2) to meet Agency, OPM and DoD reporting requirements; and (3) to provide information to DeCA managers and HR professionals to assist in making business decisions. All personnel information provided from the DeCA HR data mart complies with the Privacy Act of 1974. Personal data is only provided to individuals with a need-to-know.

DCPDS does not provide ad hoc query and reporting capabilities, so the Civilian Personnel Management Service (CPMS) gave the Components and Military Services the authority to develop their own query/reporting tool. DeCA's civilian personnel are serviced by the Defense Logistics Agency (DLA), Army and Air Force, therefore DeCA's personnel records are not stored in a single DCPDS database server. CPMS granted DeCA access to pull data from the DCPDS Customer Service Unit (CSU) database which only contains current information on active civilian employees. DeCA's HR data mart consists of current and historical civilian personnel data from: DLA's DCPDS database for current DeCA CONUS civilian employees; CPMS's DCPDS Corporate Management Information System (CMIS) database for current DeCA OCONUS civilian employees; and data from three legacy personnel systems (Legacy DCPDS, DMDC and DBMS). The data pulled from DCPDS on current employees is archived in DeCA's HR data mart monthly for historical purposes.

The types of personal information contained in the HR data mart are: social security number, name, home address, date of birth, gender, race/ethnicity, citizenship, security clearance, disability information, pay plan/schedule, grade/band, education information, etc. Social security numbers (SSN) are used internally in the data mart to join employee information tables and are available to the HR users to perform the required duties of their position. Information provided to DeCA managers and to other DoD organizations to meet reporting requirements does not include SSN. They generally contain statistical data with counts by location, race/ethnicity, disability, type of personnel transactions processed, pay plan/schedule - occupational series - grade/band, etc. Internal reports for DeCA managers may contain personal information such as name, pay plan/schedule, occupational series, grade, and location/organization.

**All Other Data:**

The Enterprise Data Warehouse (EDW) is a central data repository that provides a single, logical view of product, sales, and other selected business data across DeCA, allowing end users to make informed business decisions. Currently the EDW receives data files from DeCA business systems, or retrieves data directly from the underlying data storage of the source system. These files contain both business transaction data and program edit/control codes. The EDW translates the business transaction information into a data warehouse format using business rules defined by functional experts. The transformed data is maintained in a Teradata database in a format that provides quick access to required raw data, summary data, and reports. DeCA hosts the EDW environment on a set of clustered servers at DeCA Headquarters in Fort Lee, Virginia.

The information collected during the point-of-sale utilizing the Commissary Advanced Resale Transaction System (CARTS), an existing DoD / DeCA IT system, is electronically transmitted to the EDW for system-to-system data sharing. All data received is compressed and archived in a file staging area. Only a limited portion of this data is loaded into the warehouse. The following information is available to authorized users of the data warehouse.

**Check Information:**

- Social Security Number (SSN)
- Bank account number
- Bank routing information

- Check number

Credit Card Information:

- Credit card number (only received in a masked format from the source (XXXXXX000000XXXX, where X represents an actual digit from the card number)

Debit Card Information:

- Debit card number (only received in a masked format from the source (XXXXXX000000XXXX, where X represents an actual digit from the card number)

The EDW does not collect, nor store PIN or PIN blocks associated with credit and debit card transactions.

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

Human Resources Data: Although the data contained in the HR data mart is sensitive in nature, the privacy risks associated with the PII data contained in the HR data mart are minimal due to the measures taken to meet Information Assurance requirements for this type of data, and the handling of the data by HR professionals trained in the privacy regulations governing the safeguarding of this data and who are charged with the responsibility of protecting it.

All Other Data:

The transactional point-of-sale data containing SSN information does not include any other personally identifiable information such as name or address. Without additional identifiable information, there is no method within the EDW to link the SSN to other personally identifiable information.

Transactional point-of-sale data containing credit and debit card information does not include a name or SSN, so there is no method in EDW to link an individual with the credit or debit card number. Furthermore, debit and credit card numbers are received in a masked format, and as a result could not be used for fraudulent purposes.

**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.

**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.

**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.

**Human Resources Data:**

Records on Federal employees are electronically maintained at the designated Agency that currently employs the individual. Records reflecting Federal service and documenting work experience and education while employed are maintained. Such records contain information about past and present positions held; grades, salaries, duty station locations, and notice of all personnel actions. Participation in Federal benefits programs are maintained as well. In order to maintain these records, employees would not be given the opportunity to consent or withhold their consent to these records. This permission is authorized by the Office of Personnel Management, Federal Register Document 06-5459.

**All Other Data:**

There is no opportunity for an individual to object to the EDW collection of identifiable information because the information is not collected from individuals but from CARTS, an existing DoD / DeCA IT system. The PII data is provided to the EDW via a system-to-system interface. Individuals may object to the collection of PII at the time of point-of-sale prior to the data being collected by CARTS and provided to the EDW.

**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.

**Human Resources Data:**

Records on Federal employees are electronically maintained at the designated Agency that currently employs the individual. Records reflecting Federal service and documenting work experience and education while employed are maintained. Such records contain information about past and present positions held;

grades, salaries, duty station locations, and notice of all personnel actions. Participation in Federal benefits programs are maintained as well. In order to maintain these records, employees would not be given the opportunity to consent or withhold their consent to the collection or use of these records. The PII data in the HR data mart is used by HR users. The Office of Personnel Management, Federal Register Document 06-5459 authorizes HR to collect and use the information in the performance of their official duties.

All Other Data:

There is no opportunity for an individual to object to the EDW use of identifiable information because the information is not collected from an individual. CARTS, an existing DoD / DeCA IT system, provides PII data to the EDW through a system-to-system interface. Individuals may object to the use of PII at the time of point-of-sale prior to the data being collected by CARTS and provided to the EDW.

**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 Resources 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 of the notice 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 provide it, we will not be able to process your request.

All Other Data:

The EDW does not provide any information regarding PII to individuals because the EDW does not collect data from individuals. The information is acquired from a system-to-system data transfer between CARTS, an existing DoD / DeCA IT system, and the EDW. Notification of Privacy Act information is the responsibility of the source system, CARTS.

**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.**