



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Commissary Advanced Retail Transaction System (CARTS)

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
- 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.

5 U.S.C. 301, Departmental regulations; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. §2481, Defense Commissary and Exchange Systems; Existence and Purpose; 10 U.S.C. §2484, Commissary Stores: Merchandise That May Be Sold; Uniform Surcharges and Pricing; 10 U.S.C. §2485, Commissary Stores: Operation; Department of Defense Directive 5105.55, Defense Commissary Agency (DeCA); Department of Defense Instruction 1330.17, Armed Services Commissary Operations; Department of Defense 7000.14-R, Department of Defense Financial Management Regulations (FMRs), Volume 4, Chapter 3, Receivables; Volume 6A, Reporting Policy and Procedures, Volume 11A, Reimbursable Operations, Policy and Procedures, Volume 11B, Reimbursable Operations, Policy and Procedures – Working Capital Funds.

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 DeCA point-of-sale system (CARTS) processes grocery transactions through the tender phase which allows customers to pay for the groceries they wish to purchase. To obtain digital coupon discounts during checkout, some customers register for the DeCA Rewards Card loyalty program. During registration, the customer is asked to provide personal information (name, mailing address, e-mail address, a 10 digit alternate ID, service affiliation, rank, status (active duty, retired, etc.), distance to the commissary, size of the household and income range of the household.

During tendering, some customers elect to pay by personal check which DeCA processes through a Treasury system called OTCnet. OTCnet requires double-sided check images, the account number, routing number, and a customer identifier. The account number and routing number are extracted from the MICR line at the bottom of the check. Starting in October 2013, CARTS will use the 18-24 character barcode value on military identification cards as the customer identifier for all transactions. If there is no barcode on the military ID, the cashier will use the EDI-PI or the social security number if it is printed on the customer's ID card.

Some customers elect to pay for purchases using a credit/debit/electronic benefits card. When this type of tender is used, the customer swipes their card and POS provides account information to Vantiv, Treasury's provider of electronic funds transfer (EFT) processing. This interaction is typically a synchronous real-time exchange with the POS requesting approval and Vantiv responding with either an approval or a disapproval. In rare instances, the request for approval and the subsequent approval/disapproval become asynchronous due to networking delays.

If a customer uses the Internet to purchase a DeCA gift card, the customer is re-directed from commissaries.com to the web site of DeCA's gift card provider (SVM). The ordering process allows payment by credit card or check. If payment is by credit card, the customer will have to provide the a card number, the card type (Visa, MasterCard, American Express, etc.), the expiration date, and the security code from the back of the card. If payment is by check, the customer must mail the check to SVM. Online ordering requires the customer to provide billing address information, shipping address information, an e-mail address, telephone number. The customer must also create a username and password to facilitate tracking of the fulfillment process.

DeCA offers curbside pickup at three locations via Click2Go ordering page. The users must authenticate their commissary shopping privilege by providing the last four numbers of their social security number, their name and date of birth. DeCA does not save this information but it is used to query the DEERS database to confirm the customer has been authorized for the commissary benefit. After confirmation of the commissary benefit, the customer is re-directed from the commissaries.com web page to the Click2Go order web page maintained by MyWebGrocer, DeCA's commercial provider for Click2Go ordering. During the ordering process, the customer establishes a username and password, and provides an e-mail address and phone number. The username and password allow the customer to retrieve their shopping cart to modify or cancel their order. The e-mail address and phone number allow the commissary staff to interact with the customer if product substitutions are allowed.

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

Several of the shopping related functions (the Rewards Card, Internet gift card sales, Click2Go curbside pick-up, and payment by check) that collect privacy information are purely voluntary and the customers are not required to participate if they have concerns regarding the protection of their personal data. To allay customer concerns related to personal information, DeCA has implemented strict controls to protect customer data. Access to records is limited to the custodian of the records or by persons responsible for servicing the records in the performance of their official duties. Records are stored in locked cabinets or rooms and controlled by personnel screening. Computer terminals are located in supervised areas. Access to computerized data is controlled by password or other user authentication code systems. All electronic data is transmitted using approved, secured methods to ensure the data is protected while in transit, such as encryption and through the use of Secure FTP using Secure Sockets Layer. Credit/debit card numbers are masked. Name, social

Security Number, or DoD ID number is not collected for credit card purchases. PINs are automatically encrypted when entered by a patron at the point of sale using a touch-screen keyboard. Credit card information is also subject to the Data Security Standards (DSS) promulgated by the Payment Card Industry (PCI) Security Council. When the data collection occurs on the website of one of DeCA's service providers, DeCA has contractually bound the service providers to adhere to DeCA's security policies for protection of personal information.

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. DeCA's Enterprise Data Warehouse will receive transaction logs containing the customer identifier obtained by scanning the military ID card. EDW will use the identifier to obtain customer demographic data.

Other DoD Components.

Specify. DFAS will have access to the customer identifier when a check is dishonored by a financial institution. DFAS will use the customer identifier to request payment on the dishonored check.

Other Federal Agencies.

Specify. Treasury's OTCnet system will receive the Customer identifier, bank routing number, and account number for any customer payments made by personal check. Treasury's electronic funds transfer agent, Vantiv, receives account information obtained when the customer swipes their card through the pinpad.

State and Local Agencies.

Specify.

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

Specify. The POS support contractors sign a non-disclosure agreement which requires them not to divulge any PII they have access to while supporting DeCA's point-of-sale operations.

Other (e.g., commercial providers, colleges).

Specify. Data collected for Internet gift card sales, Rewards Card digital coupons, and Click2Go curbside pickup originate on the websites of DeCA's commercial service providers. These service providers have signed non-disclosure agreements which requires them not to divulge any PII they have access to while supporting DeCA's point-of-sale operations.

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.

If the customer objects to collection of PII for voluntary activities such as Rewards Card registration, Internet sales of gift cards, tendering by check, curbside pick-up of groceries, etc., the customer can choose not to

participate in that activity.

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

Scanning of the barcode on the military ID card is mandatory because this is the method DeCA plans to use to establish that the customer is authorized for the commissary benefit.

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.

Most of the personal data collection is voluntary and customers can elect not to participate if they desire. There is no requirement for customers to pay for groceries with a personal check, use the Rewards Card program to redeem digital coupons, order gift cards via the Internet, or order groceries via the Internet for curbside pick-up.

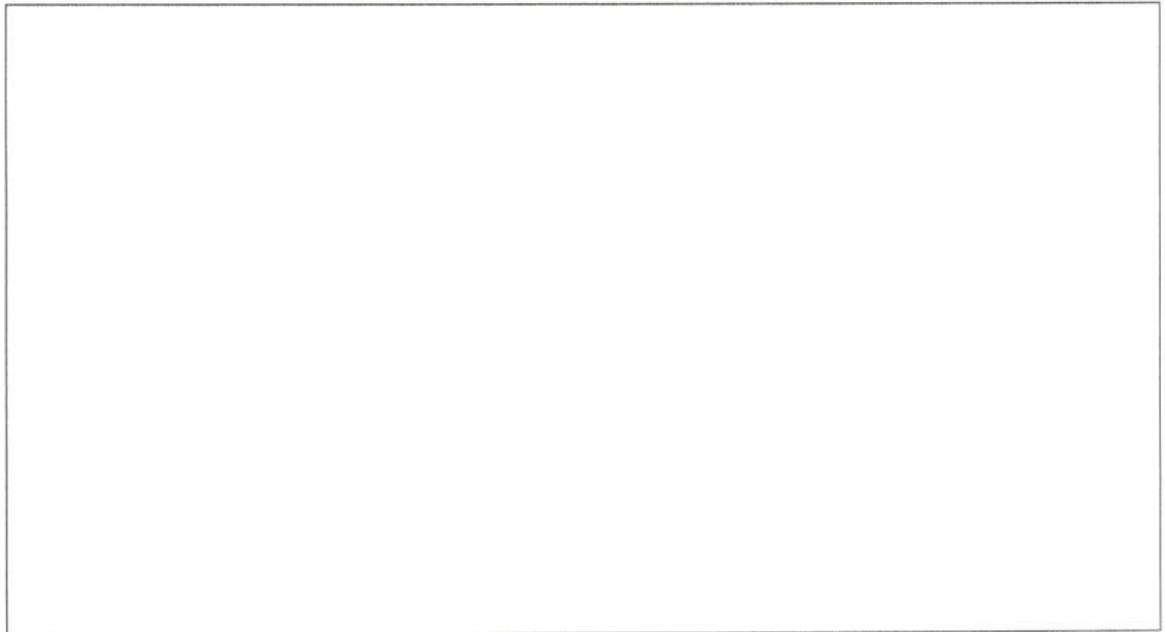
(2) If "No," state the reason why individuals cannot give or withhold their consent.

Collection of the military barcode for all transactions is consistent with DeCA's mission of offering the commissary benefit only to authorized patrons. The barcode value from the military ID card allows DeCA to verify the customer is authorized for the commissary benefit. The demographic data obtained using the barcode value will help DeCA provide better service to our customers by tailoring the stock assortment of our stores to their needs based upon age grouping and gender.

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. DeCA provides Privacy Advisories at the checkout lane that explain the reasons for collecting any privacy information related to tendering. On the websites that solicit personal information for DeCA programs, the mandatory information is highlighted and the customer can elect to opt out.



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.