PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

EBS Increment 3 (Above Store-Level)

2. DOD COMPONENT NAME:

Defense Commissary Agency

3. PIA APPROVAL DATE:

04/16/18

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [x] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [x] New DoD Information System
- [ ] New Electronic Collection
- [ ] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

The DeCA EBS Increment 3 solution 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, customers must register for the new DeCA loyalty program. During registration for the new loyalty program, the customer is asked to provide personal information (name, mailing address, e-mail address for digital receipts/promotions, 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). This information resides in the EBS Customer Relationship Management (CRM) module. This information is not shared with other Defense retailers such as the military exchanges operated for the Services (AAFES, NEX, etc.)

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. CARTS also uses 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 customer ID is the EDI-PI, the social security number (if it is printed on the customer's ID card), or the ration card number used in Korean commissaries. This information is processed in the DeCA Server Centers to create check batches which are conveyed to OTCNet via secure web services.

Some customers elect to pay for purchases using a credit/debit/electronic benefits card. When this type of tender is used, the customer swipes/inserts their card and account information is sent to Connected Payments which conveys this information to WorldPay (Treasury's provider of electronic funds transfer (EFT) processing) or AAFES (for the Military STAR card). This interaction is typically a synchronous real-time exchange with the POS requesting approval and WorldPay/AAFES responding through Connected Payments 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 SVM with the 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 also 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 curb-side pickup at multiple locations via a Click2Go ordering page. DeCA authenticates Click2Go user commissary shopping privilege. This information (the last four digits of their social security number, their name and date of birth) resides in the CRM module of the solution and 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 directed to the eCommerce ordering application to initiate Click2Go orders. During the CRM registration 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 and to allow digital receipt delivery if the customer opts in for this feature.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

Mission related use to authenticate customers, accept their tenders, and facilitate online ordering.

e. Do individuals have the opportunity to object to the collection of their PII? ☐ Yes ☒ No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

DoD policy requires DeCA to validate shopping privileges.

f. 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.

Customers can choose to use tenders which do not require PII (e.g. use cash instead of a personal check or credit/debit cards). Customers can elect not to participate in the customer loyalty program.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

☒ Privacy Act Statement ☐ Privacy Advisory ☐ Not Applicable

Collection of Social Security Number/Military ID Card Bar Code Value/DoD ID Number
Authority: 10 U.S.C. 2481, 2485(g) and (h); DoD Instruction 1330.17; E.O. 9397
Principle Purposes: To positively identify authorized patrons of the Defense Commissary Agency; to enable patrons to tender payment for groceries and household goods by means of check; to enable the Defense Commissary Agency to identify writers of previously dishonored checks; and to obtain general aggregated demographic data concerning authorized patrons, including Military Service affiliation and status, from the Defense Enrollment Eligibility Reporting System (DEERS).
Routine Uses: Disclosures are permitted under 5 U.S.C. 552a(h), Privacy Act of 1974, as amended. In addition, information may be disclosed to the United States Treasury for electronic check processing and electronic funds transfers related to check charges, and for any Department of Defense Commissary Agency "Blanket Routine Use" as published in the Federal Register.
Disclosure: Voluntary; however, failure to furnish the information requested may result in inability to shop in the commissary and/or refusal to accept a check from the patron and require payment by other means.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒	Within the DoD Component	Specify.	HQ components of EBS Increment 3; DeCA Enterprise Data Warehouse
☒	Other DoD Components	Specify.	Defense Manpower Database Center (DMDC)
☒	Other Federal Agencies	Specify.	U.S. Treasury
☒	State and Local Agencies	Specify.	State/Territory WIC agencies
☒	Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	NCR and IBM are support contractors for the point of sale; contracts for both companies include the appropriate clauses citing the need to protect Privacy information
☐	Other *(e.g., commercial providers, colleges).*	Specify.	

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

- [x] Individuals
- [x] Databases
- [x] Existing DoD Information Systems
- [ ] Commercial Systems
- [x] Other Federal Information Systems

DMDC DEERS database, Treasury Local Verification Download (LVD) database for bad checks, initial upload of legacy Inmar customer database for DeCA customers and any subsequent Loyalty program updates provided by patron.

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

- [ ] E-mail
- [x] Official Form (*Enter Form Number(s) in the box below)*
- [x] Face-to-Face Contact
- [ ] Paper
- [ ] Fax
- [ ] Telephone Interview
- [x] Information Sharing - System to System
- [x] Website/E-Form
- [ ] Other *(If Other, enter the information in the box below)*

DD Form 2 or Common Access Card (CAC)

k. 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 must be consistent.

- [x] Yes
- [ ] No

If "Yes," enter SORN System Identifier Z0035-01

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. N1-506-07-5 and DAA-

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

For Financial Transaction Records destroy 6 years after final payment or cancellation. For Customer Survey Files,destroy after 3 years.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must 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.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☒ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

Information collected as part of DeCA retail operation determined to be exempt from PRA OMB control number requirements by DeCA GC memo of October 22, 2012.