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/CARTS R/M (Store Level)

2. DOD COMPONENT NAME:

Defense Commissary Agency

3. PIA APPROVAL DATE:

06/01/18

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

☒ 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)*

☒ 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.

EBS Increment 3 provides a new point-of-sale (POS) system for the Defense Commissary Agency (DeCA). The POS system must validate shopping privileges via the Defense Manpower Data Center using web services with a query based on the Barcode 39 value from a military ID. Depending on the payment method the customer uses, additional information may be required. For instance, Treasury processing of a personal check requires images of the front and back of the check as well as a customer ID unique to the the individual. The default check ID will be the Barcode 39 value from the ID card. If there is no Barcode 39, the secondary ID choice is the DoD ID number printed on the military ID; the tertiary ID choice is the SSN when there is no Barcode 39 or DoD ID number; in Korean commissaries only, the ration card can be used to identify the customer.

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 and accept their tenders

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. Treasury policy requires a customer ID for electronic check processing though OTCnet.

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 card). If customers do not want to participate in digital coupons or other promotional activities, the customer can elect not participate in "opt in" registration activities.

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; Enterprise Data Warehouse
☒ Other DoD Components	Specify.	Defense Manpower Database Center
☒ Other Federal Agencies	Specify.	U.S. Treasury
☒ State and Local Agencies	Specify.	State 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 new point of sale; contracts for both companies include the appropriate clause 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)*

☒ Individuals

☒ Existing DoD Information Systems

☒ Other Federal Information Systems

☒ Databases

☐ Commercial Systems

DMDC DEERS database, Treasury Local Verification Download (LVD) database for bad checks

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

☐ E-mail

☒ Face-to-Face Contact

☐ Fax

☐ Information Sharing - System to System

☐ Other *(If Other, enter the information in the box below)*

☒ Official Form (*Enter Form Number(s) in the box below)*

☐ Paper

☐ Telephone Interview

☐ Website/E-Form

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.

☒ 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.

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

(3) Retention Instructions.

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.

DoD policy requires authentication of customers to ensure they are entitles to shop at a commissary; this is achieved by validating the customer has commissary privileges associated with their ID card by querying the DMDC database using encrypted web services. Treasury electronic check processing via OTCnet requires a patron identifier as part of the data exchange which supports the bad check list maintained by Treasury. Offline processing of credit card tenders requires the POS to retain credit card information in an encrypted format until the connection is restored.

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 operations determined to be exempt from PRA OMB control number requirements by DeCA GC memo of October 22, 2012.

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)***?** *(Check all that apply)*

☐ Biometrics
☐ Citizenship
☐ Driver's License
☐ Employment Information
☐ Home/Cell Phone
☐ Mailing/Home Address
☐ Military Records
☐ Official Duty Address
☐ Passport Information
☐ Place of Birth
☐ Race/Ethnicity
☐ Records
☐ Work E-mail Address

☐ Birth Date
☐ Disability Information
☐ Education Information
☐ Financial Information
☐ Law Enforcement Information
☐ Marital Status
☐ Mother's Middle/Maiden Name
☐ Official Duty Telephone Phone
☐ Personal E-mail Address
☐ Position/Title
☐ Rank/Grade
☐ Security Information
☐ If Other, enter the information in the box below

☐ Child Information
☒ DoD ID Number
☐ Emergency Contact
☐ Gender/Gender Identification
☐ Legal Status
☐ Medical Information
☐ Name(s)
☐ Other ID Number
☐ Photo
☐ Protected Health Information (PHI)[1]
☐ Religious Preference
☒ Social Security Number (SSN) *(Full or in any form)*

POS reads the Barcode 39 format on the military ID card to support a query against the DMDC DEERS database to determine if the customer has commissary privileges. POS does not store any data from the DMDC query response and the commissary does not share any PII with the local military exchanges. POS provides Treasury's OTCnet with the customer ID (Barcode value or DoD ID number or SSN or Koren Ration card ID if there is no barcode) and the image of the check.

If the SSN is collected, complete the following questions.

(*DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)*

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

☐ Yes ☒ No

If "Yes," provide the signatory and date approval. If “No,” explain why there is no SSN Justification Memo.

SSN is the identifier of last resort which is used only when an ID card cannot provide a Barcode 39 value or a DoD ID number.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 “Reduction of Social Security Number (SSN) Use within DoD”.

Required by Treasury for electronic check processing if that is the only form of federal government identification the customer can provide.

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, “Reduction of Social Security Number (SSN) Use within DoD”.

The cashier hand enters the SSN which is include in the transaction log and in the information sent to Treasury's OTCnet check processing system. Store staff do not have access to the transaction log or the check batch created for Treasury so they cannot print out the customer's SSN.

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

☐ Yes ☒ No

SSN is only used when that is the only federal identifier printed on the military ID card; most military IDs now have a barcode and/or a DoD ID Number which can be used in lieu of a SSN. The POS does not store the SSN at store level but does pass the SSN to HQ for processing by other information systems.

b. What is the PII confidentiality impact level[2]? ☒ Low ☐ Moderate ☐ High

[1] The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2] Guidance on determining the PII confidentiality impact level, see Section 2.5 “Categorization of PII Using NIST SP 800-122.” Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

□ Cipher Locks
□ Combination Locks
□ Key Cards
□ Security Guards
□ Closed Circuit TV (CCTV)
□ Identification Badges
□ Safes
□ If Other, enter the information in the box below

(2) Administrative Controls. *(Check all that apply)*

☒ Backups Secured Off-site
☒ Encryption of Backups
☒ Methods to Ensure Only Authorized Personnel Access to PII
☒ Periodic Security Audits
□ Regular Monitoring of Users' Security Practices
☒ If Other, enter the information in the box below

Only the POS support contractor has role-based access to the transaction log at store level. The POS support contractors sign non-disclosure agreements which cover customer PII.

(3) Technical Controls. *(Check all that apply)*

□ Biometrics
□ Encryption of Data at Rest
☒ Firewall
☒ Role-Based Access Controls
□ Virtual Private Network (VPN)
☒ Command Access Card (CAC)
☒ Encryption of Data in Transit
☒ Intrusion Detection System (IDS)
□ Used Only for Privileged (Elevated Roles)
□ If Other, enter the information in the box below
☒ DoD Public Key Infrastructure Certificates
□ External Certificate Authority Certificates
☒ Least Privilege Access
□ User Identification and Password

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

SECTION 3: RELATED COMPLIANCE INFORMATION

a. Is this DoD Information System registered in the DoD IT Portfolio Repository (DITPR) or the DoD Secret Internet Protocol Router Network (SIPRNET) Information Technology (IT) Registry or Risk Management Framework (RMF) tool[3]?

☒ Yes, DITPR	DITPR System Identification Number	12134
□ Yes, SIPRNET	SIPRNET Identification Number	
□ Yes, RMF tool	RMF tool Identification Number	
□ No		

If "No," explain.

b. DoD information systems require assessment and authorization under the DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology".

Indicate the assessment and authorization status:

□ Authorization to Operate (ATO)	Date Granted:	
□ ATO with Conditions	Date Granted:	
□ Denial of Authorization to Operate (DATO)	Date Granted:	
□ Interim Authorization to Test (IATT)	Date Granted:	

(1) If an assessment and authorization is pending, indicate the type and projected date of completion.

RMF ATO pending; projected for completion in Jun 2018.

(2) If an assessment and authorization is not using RMF, indicate the projected transition date.

c. Does this DoD information system have an IT investment Unique Investment Identifier (UII), required by Office of Management and Budget (OMB) Circular A-11?

□ Yes ☒ No

If "Yes," Enter UII If unsure, consult the component IT Budget Point of Contact to obtain the UII

[3] Guidance on Risk Management Framework (RMF) tools (i.g., eMASS, Xacta, and RSA Archer) are found on the Knowledge Service (KS) at https://rmfks.osd.mil.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Completion of the PIA requires coordination by the program manager or designee through the information system security manager and privacy representative at the local level. Mandatory coordinators are: Component CIO, Senior Component Official for Privacy, Component Senior Information Security Officer, and Component Records Officer.

a. Program Manager or Designee Name	Ericka Pearson	(1) Title	EBS Increment 3 Program Manager
(2) Organization	PMO	(3) Work Telephone	Ext 48249
(4) DSN		(5) E-mail address	Ericka.Pearson@DeCA.mil
(6) Date of Review		(7) Signature	PEARSON.ERICKA.J.1039466615 Digitally signed by PEARSON.ERICKA.J.1039466615 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DECA, cn=PEARSON.ERICKA.J.1039466615 Date: 2018.05.15 11:50:18 -04'00'

b. Other Official *(to be used at Component discretion)*		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	

c. Other Official *(to be used at Component discretion)*		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	

d. Component Privacy Officer (CPO)	Camillo DeSantis	(1) Title	DeCA Privacy Officer
(2) Organization	Office of the DeCA Legal Counsel	(3) Work Telephone	Ext 48982
(4) DSN		(5) E-mail address	Camillo.DeSantis@DeCA.mil
(6) Date of Review	May 16, 2018	(7) Signature	DESANTIS.CAMILLO.R.1019281112 Digitally signed by DESANTIS.CAMILLO.R.1019281112 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DECA, cn=DESANTIS.CAMILLO.R.1019281112 Date: 2018.05.16 08:23:54 -04'00'

e. Component Records Officer	Carol Chambliss	(1) Title	DeCA Records Officer
(2) Organization	LEIMG	(3) Work Telephone	Ext 48841
(4) DSN		(5) E-mail address	Carol.Chambliss@DeCA.mil
(6) Date of Review		(7) Signature	
f. Component Senior Information Security Officer or Designee Name		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review:		(7) Signature	
g. Senior Component Official for Privacy (SCOP) or Designee Name	Ralph Tremaglio	(1) Title	DeCA Legal Counsel
(2) Organization	DeCA/GC	(3) Work Telephone	Ext 48116
(4) DSN		(5) E-mail address	Ralph.Tremaglio@DeCA.mil
(6) Date of Review		(7) Signature	
h. Component CIO Reviewing Official Name	Jeffrey Perry	(1) Title	DeCA Chief Information Officer
(2) Organization	DeCA LEIT	(3) Work Telephone	Ext 48757
(4) DSN		(5) E-mail address	Jeffrey.Perry@DeCA.mil
(6) Date of Review		(7) Signature	

Publishing: Only Section 1 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: osd.mc-alex.dod-cio.mbx.pia@mail.mill.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Section 1.