CARTS Privacy Impact Assessment

1. *Department of Defense (DoD) Component*: Defense Commissary Agency (DeCA)

2. *Name of Information Technology (IT) System*: Commissary Advanced Resale Transaction System (CARTS)

3. *Budget System Identification Number (SNAP-IT Initiative Number):* 277

4. *System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR)):* 819

5. *IT Investment (OMB Circular A-11) Unique Identifier:* N/A

6. *Privacy Act System of Records Notice Identifier:* Z0035-1

7. *OMB Information Collection Requirement Number and Expiration Date:* N/A

8. *Type of authority to collect information:*

   DOD Directive 1330.17, "Military Commissaries", dated 13 March 1987 and Treasury's Paper Check Conversion/Over The Counter Program.

9. *Provide a brief summary or overview of the IT system (activity/purpose, present life-cycle phase, system owner, system boundaries and interconnections, location of system and components, and system backup):*

CARTS is the point of sale system used in military commissaries. During source selection, DeCA selected IBM as the system integrator. DeCA established the CARTS Program Management Office (PMO) to coordinate the procurement, testing, and deployment of the CARTS system to 268 commissaries around the world starting in October 2006 and completing in May 2008. CARTS interfaces with four systems: DeCA's Enterprise Data Warehouse (EDW); DeCA's Electronic Record Management and Archive System (DERMAS); Treasury's Plastic Card Network program which is managed by Fifth Third Bank; and Treasury's check processing system. The front-end of CARTS is located in the commissaries and the back-end of CARTS is hosted at two server centers located at Ft Lee VA and Sacramento CA.

10. Describe what information in identifiable form will be collected and the nature of the names, SSN, gender, race, other component IT systems, IT systems from agencies outside DOD, etc).

CARTS does not necessarily require all of the following information, but it is possible that CARTS could collect some or all of this information depending on the method of payment. More detail on how CARTS would collect these types of information is provided later in the document. The information in identifiable form could potentially be collected during transactions:

CHECK PROCESSING:

- Full name
- Address
- Driver's license number
- Phone number
- Social security numbers (SSN)
- Electronic Data Interchange – Personal Identifier (EDI-PI)
- Bank account number
- Bank Routing information

CREDIT CARD TRANSACTIONS:

- Credit Card numbers
- Expiration dates

DEBIT CARD PURCHASE:

- Debit card number
- Personal Identification Number (PIN)

AGE-RESTRICTED ITEM PURCHASES:

- Date of Birth

11. Describe how the information will be collected (e.g., via the Web, via paper-based collection, etc).

Check Processing

DeCA and the United States Treasury have agreed to process checks provided by DeCA patrons through Treasury's Electronic Verification and Imaging System (ELVIS). Check processing through ELVIS require the SSN or the EDI-PI; DeCA submits the sponsor's SSN or EDI-PI to comply with Treasury's patron identification requirement. When a patron submits a check for payment, the cashier has two options for collecting the sponsor's SSN or EDI-PI: (1) scanning the barcode on the back of a military identification (ID) card using the built-in or handheld scanner at the cash register; or (2) through visual inspection of the SSN printed on the military ID card (the cashier must key-in the SSN when obtained via inspection of the military ID card). To process a check electronically, Treasury required DeCA to scan both sides of the check and provide ELVIS with an image of each side of the check. Bank account number and routing information are collected from the Magnetic Ink Character Recognition line found at the bottom of most checks. Many DeCA customers have preprinted checks which include full name, address, driver's license number, and phone number. If this information is preprinted on the check, the information will be forwarded to Treasury as part of the scanned image of the check.

In addition to uploading check images to ELVIS for electronic processing, CARTS also downloads data on a daily basis from ELVIS. This data includes the following information for customers who have previously written a bad check at a DeCA commissary: bank account number, bank routing information and SSN or EDI-PI.

Credit Card Purchase

A credit card purchase requires a credit card number and card expiration date. During a credit card purchase, either the customer or the cashier swipes the credit card through a device which reads the magnetic strip on the credit card. Swiping the card allows CARTS to extract the required information from the magnetic strip on the credit card. If swiping the credit card does not work, the cashier can enter the credit card number and expiration date using the touch-screen keyboard. CARTS does not collect name, SSN or EDI-PI for credit card purchases. Without an associated name, SSN, or EDI-PI, there is no method within CARTS to link the collection credit card number and expiration with a specific individual.

Debit Card Purchase

A debit card purchase requires a debit card number and an associated PIN. During a debit card purchase, either the customer or the cashier swipes the debit card through a device which reads the magnetic strip on the debit card. Swiping the card allows CARTS to extract the debit card number. If swiping the debit card does not work, the cashier can enter the debit card number using the touch-screen keyboard. The customer must enter the P IN on the keyboard which is part of the card swiping device. When the PIN is entered, the device automatically encrypts the PIN so that CARTS never has access to a customer's unencrypted PIN. CARTS does not retain the customer's PIN because this is forbidden by the plastic card industry regulations. CARTS does not collect a name, SSN, or EDI-PI for a debit card purchase. Without an associated name or SSN, there is no method within CARTS to link the collected debit card number and encrypted PIN with a specific individual.

Age Restricted Purchase

Date of birth is printed on a military ID card. The cashier enters the customer's date of birth into CARTS when a customer buys an age-restricted item such as tobacco. Date of birth would only be personally identifiable information if included with a purchase made by check, which required a SSN or EDI-PI for electronic processing. Without an associated SSN or EDI-PI, there is no method within CARTS to link the collected date of birth with a specific individual.

12. Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a Component program, etc.)

For customers paying by check, SSN, EDI-PI, and bank account information is included with data passed to ELVIS. A Treasury Privacy Act notice is posted at each CARTS cash register informing a customer of the requirement to collect a unique patron ID for electronic processing of a check. The customer's SSN or EDI-PI may be obtained by scanning a barcode on the customer's military ID card or keyed in by the cashier after obtaining the SSN through visual inspection if the customer's military ID card. The customer's full name, address, and telephone number will be captured during the imaging process if they are printed on the check, but there is no CARTS requirement for this information.

The United States Treasury has a contract with Fifth Third Bank to process credit, debit, and EBT card transactions for the United States government. To process a credit card payment, Fifth Third Bank requires that CARTS supply the credit card number and card expiration date in the request for payment authorization. To process a debit card payment, Fifth Third Bank requires that CARTS supply the debit card number and an encrypted PIN value in the request for payment authorization.

Date of birth is collected to verify that a customer is old enough to purchase an age-restricted item such as tobacco.

13. Describe how the information in identifiable form will be used (e.g., to verify existing data, etc.).

If a customer pays by check, the cashier enters the sponsor's SSN or EDI-PI, scans the payment check for upload to ELVIS, and CARTS verifies that the customer's SSN or EDI-PI is not included in the bad check data, the cashier will receive immediate notification that the customer's check is unacceptable. The customer will be required to provide an alternate form of payment. The sponsor will not be able to pay by bank check until the debt is paid off. Once the debt is paid, the sponsor will also be prevented from writing checks for a period of days consistent with the current DeCA policy.

CARTS uploads check images and check data to ELVIS. ELVIS can process the customer's check as a debit transaction or using the Check 21 image process. The image of the customer's check potentially includes the customer's full name, address, and telephone number, but this information is simply passed on the ELVIS and is not stored in a database by CARTS.

14. Describe whether the system derives or creates new data about individuals through aggregation.

CARTS does not derive or create new data about individuals through aggregation.

15. Describe with whom the information in identifiable form will be shared, both within the Component and outside the Component (e.g., other DoD Components, Federal agencies, etc.).

For payments made by check, DeCA creates image and data files to send to ELVIS, along with the sponsor's SSN or EDI-PI. The image is a .tif file and contains a picture both sides of the customer's check. The data file comes from the Magnetic Ink Character Recognition (MICR) at the bottom of the check and contains the customer's bank account number, routing number, plus the SSN or EDI-PI.

Credit and debit card payment authorization requests are passed to Fifth Third Bank, Treasury's agent for processing credit and debit card payments.

CARTS conveys all transaction data to EDW. The transaction data includes the SSN or EDI-PI collected for check payment, the date of birth collected for age-restricted purchases, the masked credit/debit card number, and credit card expiration date. EDW does not receive the customer's encrypted PIN.

16. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding who the individual is to grant consent.

Since the customer chooses the payment method, the customer always has the option to choose a payment method that required no personally identifiable information, such as cash payment. Individual customers provide consent for DeCA to collect identifiable information when they: (1) elect to use a bank check for payment; (2) present a credit card or debit card for payment; or (3) provide their date of birth when purchasing age-restricted items.

17. Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of delivery (e.g., written, electronic, etc), regarding the determination to collect the information in identifiable form.

A Treasury notice is posted on every cash register informing customers that Privacy Act information is collected to support processing of the check by Treasury's ELVIS system.

The customer voluntarily keys in the PIN to support a debit card payment transaction.

18. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.

When CARTS passes transaction data to the DeCA EDW, CARTS uses encrypted data transmissions to ensure the data is protected while in transit. These secure transactions are achieved through the use Secure FTP, which protects the information exchange using Secure Sockets Layer (SSL). SSL is the protocol used in many web-based transactions to provide security (encryption) to data being exchanged electronically.

CARTS exchanges customer check images and data (including SSN) with ELVIS using secure data transfers encrypted using SSL as specified in the Treasury interface guide for ELVIS. The bad check data downloaded daily from ELVIS is also protected in transit using SSL.

Within CARTS, data is stored in relational databases (Microsoft SQL Server) which features role-based security access. This access control ensures that only those authorized individuals with a need-to-know can access personally related information.

19. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, "DoD Privacy Program," November11, 2004. If so, and a System Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when publication of the Notice will occur.

A CARTS System of Records Notice (SORN) was submitted to the DoD Privacy Office and was published in the Federal Register.

20. Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures.

Check Payment – Payment by check is a voluntary option provided to each customer. A Treasury notice is posted on every cash register informing the customer that Privacy Act information is collected to support processing of the check by ELVIS.

A customer must follow Treasury procedures for clearing their SSN or EDI-PI from the Treasury bad check database, the source of the CARTS bad check database. CARTS uses the Treasury list to determine whether customers are allowed to pay with a check. If a customer's SSN or EDI-PI is on the Treasury list of persons denied check cashing privileges, the customer must pay for purchases using another type of tender (cash, credit card, or debit card). If a breach of security occurred, an intruder would be able to determine that a specific SSN or EDI-PI was associated with a check number that had been returned for insufficient funds. Although this disclosure might prove personally embarrassing, there is a low risk that access to a customer SSN or EDI-PI in the CARTS bad check database would result in possible identity theft unless additional information was obtained from other sources. DeCA's information technology security staff analyzed the CARTS security controls and determined that there is a low risk of malicious, inadvertent, or intentional unauthorized access to a customer's SSN or EDI-PI because of the technical security controls implemented by CARTS.

Credit and Debit Card Payment – Credit and debit card information does not include a name, EDI-PI, or SSN, so there is no method in CARTS to link an individual with the credit or debit card payment authorization request. The CARTS PMO included this information for information purposes only; it is not personally identifiable information without a name, SSN, or EDI-PI.

Age-restricted Item Purchase – Unless an age-restricted item purchase is made in conjunction with a check payment, these is no method within CARTS to link it to an individual. When purchase of an age-restricted item is made in conjunction with payment by bank check, the CARTS transaction data correlates a SSN or EDI-PI with the birth date of the individual. DeCA's information technology security staff analyzed the CARTS security controls and determined that there is a low risk of malicious, inadvertent, or intentional unauthorized access to the correlated data (the two types of personally identifiable information) because of the technical security controls implemented by CARTS.

21. State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form.

CARTS does not process government classified information. However, CARTS does process administrative and financially sensitive data. The CARTS Privacy Impact Assessment (PIA) is published in full on the DeCA public Web site. In addition, the CARTS SORN has been published in the Federal Register.