Department of the Treasury
Financial Management Service (FMS)
Privacy Impact Assessment (PIA)

Name of Project: **Stored Value Card**
Project's Unique ID: **SVC**

A. SYSTEM APPLICATION/GENERAL INFORMATION:

1) **Does this system contain any information about individuals?**

YES

a. **Is this information identifiable to the individual[1]?** (*If there is NO information collected, maintained, or used that is identifiable to the individual in the system, the remainder of the Privacy Impact Assessment does not have to be completed*).

Yes – Name, address, social security number, telephone number, e-mail address, date of birth for all SVC cardholders. For SVC cardholders who use the self-service kiosks, SVC also collects banking data (routing number, account number, account type).

b. **Is the information about individual members of the public?** (*If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security C&A documentation*).

Yes. Information is about active duty military personnel and military government contractor personnel.

c. **Is the information about employees?** (*If yes and there is no information about members of the public, the PIA is required for the FMS IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation*).

See A.1.b. above.

2) **What is the purpose of the system/application?**

SVC uses smart card technology with "electronic purses" to eliminate coin, currency, scrip, vouchers, money orders, and other labor intensive payment mechanisms in closed government locations such as military bases.

This program is aimed at eliminating the float loss associated with the more than $2 billion in coin and currency in circulation on military bases and other closed government locations around the world. SVC also eliminates the cost of securing, transporting, and accounting for cash held outside of Treasury. In addition, SVC eliminates the manually intensive backend operations necessary to support scrip, vouchers, meal tickets, money orders, traveler's checks, and other paper payment mechanisms used in closed government environments.

3) What legal authority authorizes the purchase or development of this system/application?

5 U.S.C. 301; 31 U.S.C. 321; 31 U.S.C. chapter 33; 31 U.S.C. 3720

B. DATA in the SYSTEM:

1) What categories of individuals are covered in the system?

Army, Air Force, and Marine Corps basic trainees; deployed military personnel at selected overseas bases and troop transfer stations; and civilians (contractors, including commercial/retail salespeople) at selected overseas bases and troop transfer stations

2) What are the sources of the information in the system?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

EagleCash information is provided by the individual.

EZpay (SVCs for basic trainees) information is provided by the Defense Finance and Accounting Service (DFAS) or the local base Finance Office in the case of the Marine Corps basic training sites.

b. What Federal agencies are providing data for use in the system?

DFAS and United States Army Finance Command

c. **What State and local agencies are providing data for use in the system?**

None

d. **From what other third party sources will data be collected?**

None

e. **What information will be collected from the employee and the public?**

Name, address, social security number, telephone number, e-mail address, and date of birth will be collected for all cardholders. For cardholders accessing self-service kiosks, banking data (routing number, account number, and account type) will also be collected.

3) Accuracy, Timeliness, and Reliability

a. **How will data collected from sources other than FMS records be verified for accuracy?**

Information provided by DFAS for all EZpay program participants (basic military trainees) will be verified by the appropriate service branch.

Information provided by EagleCash participants will be verified against military pay records and/or military ID card (i.e. CAC).

b. **How will data be checked for completeness?**

Information provided by DFAS for all EZpay program participants (basic military trainees) will be verified as complete by the appropriate service branch.

Information for EagleCash participants will be checked for completeness against military pay records and/or military ID cards (i.e., CAC).

c. **Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).**

For EZpay, the local finance office will send an updated file if information about the cardholder needs to be updated; the same holds true for EagleCash finance officers and cardholders. In addition, EagleCash self-service kiosk users are instructed upon kiosk enrollment to re-enroll at the finance office if their banking data changes. Lastly if a self-service kiosk user's banking data is determined to be out of date, the cardholder's card will be locked out of ACH transactions with a message referring the cardholder to the finance office; and the local finance office is instructed separately to locate the cardholder and obtain up-to-date account information.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

Yes, data elements are described in the standard operating procedures, enrollment form, security plan, and contingency plan.

C. <u>ATTRIBUTES OF THE DATA:</u>

1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

Yes, this information is maintained electronically in an SQL server database.

3) Will the new data be placed in the individual's record?

Residual information is exchanged with DFAS to allow them to return any outstanding residual value post-expiration to a basic trainee. This information is sent via FedACH. Information about a cardholder owed SVC debt is exchanged with DFAS in order to allow them to collect the debt from the pay of military personnel who owe the debt.

4) Can the system make determinations about employees/public that would not be possible without the new data?

N/A

5) How will the new data be verified for relevance and accuracy?

The data are produced from an automated application which processes all residuals for EZpay in a like manner. Data is verified manually and by sending notice about the debt to the affected cardholder.

6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

   SVC servers are on a standalone LAN segment which is separate from the Federal Reserve network, the FMS network, and the internet. It has no connectivity to any other network. In addition, there are physical and logical controls which prevent any unauthorized access to the server area and the servers/databases.

7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain**.

   The SVC servers are on a standalone LAN segment which is separate from the Federal Reserve network, the FMS network, and the Internet. It has no connectivity to any other network. In addition, there are physical and logical controls which prevent any unauthorized access to the server area and the servers/databases.

8) **How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

   Information is retrieved by social security number or SVC card number at the direction of an operator working at an SVC workstation at the FRB.. Information may also be retrieved by name. Information can be displayed using Crystal Reports or by viewing through a module of the SVC back office system only to users with authority to view such information.

9) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

   Reports produced include: Card Issuance (initial issuance or subsequent reloading of funds), Transaction History, and Kiosk Activity. These reports are used primarily for internal use to reconcile a day's processing work or to assist with the research of an outstanding issue with a particular card. Reports are sent to SVC program managers, DFAS, and selected program-participating merchants. However, the data shared with these recipients varies (i.e., merchants only receive information about their own activity not about individuals' issuance activity). In addition, the back office system is only accessible to a limited number of authorized users from SVC – FRB employees or contractors as well as an FMS SVC program manager.

10) **What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.**

Individuals are free to decline providing banking data for EagleCash card issuance; however, declining to provide this information will require that the user forego self-service kiosk enrollment as the information is required to process any kiosk ACH-based transactions (i.e. self-service card load from bank account or self-service card unload to bank account). Further, individuals are not required to enroll in the EagleCash program. Upon enrollment for the EagleCash program, individuals sign an enrollment form (DD Form 2887) consenting to the use of their information for the EagleCash program.

D. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

N/A

2) **What are the retention periods of data in this system?**

Data are retained indefinitely.

3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

N/A

4) **Is the system using technologies in ways that the FMS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

No.

5) **How does the use of this technology affect public/employee privacy?**

N/A

6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

An individual cardholder's transaction history allows for a system operator to review the location and dates/times of purchases over the lifecycle of that particular smartcard. The merchant location, date, and time are recorded in each transaction record and are stored in the central database for that particular smartcard program. However, this data is not real-time; it is based on a time lag inherent in the system (which is offline with batch processing) so there is no opportunity for real-time monitoring or tracking of individual cardholders.

7) **What kinds of information are collected as a function of the monitoring of individuals?**

No data are collected specifically for the purpose of tracking or monitoring individuals. The ability to track or monitor individual purchase patterns (after the fact) is ancillary and may be used on an ad hoc basis by military law enforcement only where there is suspected fraudulent or unauthorized use of the card.

8) **What controls will be used to prevent unauthorized monitoring?**

Access to SVC is limited to individuals authorized specifically for the purpose of completing tasks and work related to SVC transaction processing, settlement, or reconciliation (or support thereof). See E. below.

9) **Under which Privacy Act systems of records notice does the system operate? Provide number and name.**

Treasury/FMS.017 - Collections Records-Treasury/Financial Management Service

10) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

No

E. ACCESS TO DATA:

1) **Who will have access to the data in the system?** (*E.g., contractors, users, managers, system administrators, developers, other*)

The following categories of individuals have access to the back office system:

FRB SVC employees and FRB contractors

2) **How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**

   Access is assigned based on the principle of least privileged; rights are assigned at the active directory (server/network infrastructure), database, and application/function levels with the smallest possible set of rights provided to each individual.

3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**

   User access is restricted as noted above. Individual cardholders have no access to the system other than to the balance on their card.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials.)**

   Each SVC user with access to the backend system is required to sign a Rules of Behavior document explaining the responsibilities inherent on all users of the system. This document also includes language specifically noting the appropriate disciplinary action for failure to comply with the Rules of Behavior. In addition, all users are to undergo Security Awareness Training.

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?**

   Yes. All contractor contracts contain a non-disclosure agreement.

6) **Do other systems share data or have access to the data in the system? If yes, explain.**

   No.

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

It is the responsibility of both FMS (SVC system owner/SVC ISSO) and the FRB (SVC operations). The systems operations take place at the FRB in an offline environment.

8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)?

No.

9) How will the data be used by the other agency?

N/A

10) Who is responsible for assuring proper use of the data?

The SVC system owner