Financial Management Service

Privacy Impact Assessment

The Financial Management Service (FMS) Mission is to provide central payment services to Federal Program Agencies, operate the federal government's collections and deposit systems, provide government-wide accounting and reporting services, and manage the collection of delinquent debt owed to the government.

FMS Privacy Impact Assessments (PIA) http://www.fms.treas.gov/pia.html

Document Date: September 15, 2011

Document Version: 2.1

Name of System: Electronic Check Processing (ECP) System

SYSTEM GENERAL INFORMATION:

1) System Overview: Describe the purpose of the system.
The purpose of ECP is to provide Federal agencies with a centralized check-clearing, report inquiry and retrieval mechanism, as well as an imaging archive solution.
2) Under which Privacy Act Systems of Records Notice (SORN) does the system operate? Provide number and name.
Treasury/FMS.017 – "Revenue Collections Records"
3) If the system is being modified, will the SORN require amendment or revision?
__yes, explain.
_X_no

4) Does this system contain any personal information about individuals?
_X_yes
__no

a. Is the information about members of the public?
Yes
b. Is the information about employees or contractors?
No

5) What legal authority authorizes the purchase or development of this system?
FMS generally has the authority to appoint agents (*e.g.*, commercial financial institutions or federal reserve banks) to provide financial services to the government and perform all such reasonable duties that may be required of them to support those services. *See, e.g.*, 12 U.S.C. § 90, 391. In this instance, the financial agent was selected through a Financial Agent Selection Process ("FASP") that was conducted during 2008. The FASP resulted in the selection of Citibank, N.A. ("Citibank") to be FMS' financial agent for the operation, maintenance and development of the Electronic Check Processing System ("ECP"), replacing the Federal Reserve Bank of Cleveland which had acted as fiscal agent for those purposes since 2005. The selection was memorialized in a Financial Agent Agreement ("FAA") between Citibank and FMS dated September 30, 2008

DATA in the SYSTEM:

1) Identify the category of individuals in the system
Check all that apply:
__ Employees
__ Contractors
__ Taxpayers
__X Others (describe)

_____

- Agency Users – The Federal agency users have the ability to access the cash flows that they own within the ECP system. They are restricted to their own agency cash flows by viewshields and reporting functionality defined for the agency.
- Financial Agent Lockbox Banks Users – These users have the ability to access any of the cash flows that they process within the ECP System. Specific functions, capabilities, and access levels are maintained at the individual employee level as defined within the system.
- Administrative Users – These users have the ability to create and modify application objects such as organizations, users, and cash flows in order to grant access and/or to obtain additional views and functionality not provided to the average user. These users reside within the appropriate functional areas of the Central Business Application Function (CBAF) at Citibank.

2) Identify the sources of information in the system

Check all that apply:

__ Employee
__X Public
__ Federal agencies
__ State and local agencies
__ Third party

a. What information will be collected from employees or contractors?

N/A

b. What information will be collected from the public?

The archive contains images of both the financial instrument and remittance document(s) for a payment, as well as related financial data and user define data fields that have been determined by the Federal agency as necessary for its records. Banking information will consist of bank account number, bank routing number, and check number. Additional information collected from the user could include Social Security Number or Alien Number.

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

Agencies participating in the FMS' General Lockbox Network are providing this Data.

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

None

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

None

3) Accuracy, Timeliness, and Reliability

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

ECP provides all the transactional data as well as the remittance data back to the agency in the form of reports and selected queries. Accuracy and completeness are verified and reconciled several ways. The lockbox bank balances each file before sending it to ECP. The agency receives an Accounts Receivable file from the lockbox bank, and ECP deposit report with a line by line item count, and then can confirm within Cashlink II that these deposit reporting number match. Below is a list of selected queries and reports offered to agencies in ECP:
- Item History on status of payments in settlement process, including returns;

- Selected images of financial instruments and remittance documents;
- Balancing information on items settled for an entire cash flow as well as for those settled exclusively by the Federal Reserve Bank-Cleveland;
- Up to 24 User Defined Data fields;
- Statistical information, including total items processed, return information, information regarding truncation vs. conversion;
- Deposit Ticket and Debit Voucher Numbers (Cashlink II activity);
- Comma Separated Value report providing financial and remittance documents

b. How will data be checked for completeness?

The agency and the bank are involved in verifying that the data collected or configured in the system is accurate and complete in the Agency Cash flow Profile

c. What steps or procedures are taken to ensure the data is current?

Yes, the data is current. An Agency Cash flow Profile (ACP) is created for each individual agency's cash flow. All cash flow data is captured in this document. The ACP specifies which agency unique fields need to be captured. These fields are then associated with each check transaction. The financial data is not verified within ECP, but rather through FED-ACH when the debits are submitted for settlement.

d. In what document(s) are the data elements described in detail?

Yes, the data elements are described in detail and documented. The Agency Cash flow Profile document, which is located at Citibank in a secure locked file.

ATTRIBUTES OF THE DATA:

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

All of the data collected by the system as previously detailed in this document is relevant and deemed necessary for the purpose of converting paper checks into electronic transactions.

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

No

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

No

4) **Can the system make determinations about employees or members of the public that would not be possible without the new data?**

No

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

N/A

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

The data received from the lockbox banks for the various cash flows is consolidated within the ECP System. The users at each Agency have restricted access to only view the data from their cash flow(s). The users are also set up and configured with certain permissions based on the type of role assigned. ECP uses Discretionary Access Control, which is based upon allowable functions as defined by roles, permissions, and policies. Roles are a set of permissions that are assigned to a user when his/her account is created or modified. In ECP, roles are used to provide the appropriate page

level access (links), and access to reports through the Actuate reporting process. Roles for page-level access within the application roles are not static. The application has the ability to create new roles with a different set of permissions if business needs arise, or remove permissions if necessary. The roles currently defined have been created in compliance with the principles of both "separation of duties" and "least privilege". ECP follows NIST and Treasury-FMS security policies, standards, and procedures for access control. On an annual basis, all users of the system must be recertified.

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

Processes are not consolidated

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

Data can be retrieved based on a person's check account number, name, agency account number, or other agency specific identifiers.

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

This level of reporting is not available in ECP.

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)? How can individuals grant consent?**

A checkwriter has the right to not have their check converted electronically. A procedure is in place such that individuals may OPT OUT by simply contacting Citibank and providing the necessary information so that the ECP System will be configured and set up to not convert those checks.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) **What are the retention periods of data in this system? How long will the reports produced be kept?**

Currently, all images are available in ECP. As ECP grows, the system will retain up to 2 years of data online, with an additional 5 years of data in archive. ECP also has the ability to retain data for an agency that may require a longer retention of data due to court order, litigation, or statute.

2) **What are the procedures for disposition of the data at the end of the retention period? Where are the disposition procedures documented?**

After the retention period, the Assistant Commissioner for Federal Finance must send a memo to the Chief Counsel through the Assistant Commissioner for Management, with a description of the data to be destroyed, along with a proposed method of disposition. Specific procedures are outlined in the TWAI Data Retention and Disposition guidelines dated August 25, 2006.

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

The ECP production environment has a primary and back-up site in the TWAI. The primary operations site is at the Federal Reserve's Consolidation Center 3 (CC3) in Dallas, TX**,** and the back-up site is at the Federal Reserve's Consolidation Center 1 (CC1) at the Operations Center in East Rutherford, New Jersey.

In the event of a primary site failure, ECP production will be relocated to the back-up site. Data replication of the application and the database ensures the consistent use of the system and data. In the face of such an event or interruption, the IT infrastructure and related business support systems would be activated at the alternate recovery site to provide a consistent processing platform and infrastructure for ECP.
Data recovery exercises are conducted on a regular basis to ensure that the system recovery process is functioning properly.

4) **Is the system using technologies in ways that FMS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**
   No
5) **How does the use of this technology affect employee or public privacy?**
   N/A
6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

This system provides a real-time monitor to report audit events and application exceptions involved in files being processed.

7) **What kind of information is collected as a function of the monitoring of individuals?**

The system captures auditable records within a table stored in the database and provides a trace of user actions performed within the application. ECP shall log all activities associated with modifications, entry and exits. Some auditable records will include "before change values" and change value relating to any modifications made to records. Unauthorized attempts at logging in to ECP are also captured.

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

Separation of duties is enforced within the application by providing appropriate roles for the end user. Unauthorized attempts to log in to ECP are monitored. The ECP application has a standard report in Actuate to identify any security violations (invalid logins) and that report is retrieved and reviewed on a daily basis by CitibankInformation Security Staff.

ACCESS TO DATA:

1) **Who will have access to the data in the system?**
   Check all that apply:
   __ Contractors
   _X_ Users
   __ Managers
   _X_ System Administrators
   __ System Developers
   _X_ Others (explain)_____

Users of the system have access to the data. The users include: Federal Agency users; General Lockbox Network lockbox banks; and Administrators at Citibank.

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

Privileges are authorized by ECP management for administrative users and by designated security contacts for the Federal Agency and the lockbox banks. All privileges granting access to the users are processed by the Information Security Staff at Citibank.

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

Roles are a set of permissions that are assigned to a user when his/her account is created or modified. In ECP, roles are used to provide the appropriate page level

access (links), and access to reports through the Actuate reporting process. The roles currently defined have been created in compliance with the principles of both "separation of duties" and "least privilege". Access is further controlled by the use of Views and Viewshields, which limits the users to only access cash flows that they are associated with.

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)

New users are required to read and sign the ECP Rules of Behavior before gaining initial access to ECP, and annually thereafter.

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

Yes, a software vendor (RDM) is involved in the design, development, and testing of the ECP system. Non-disclosure statements, in addition to a confidentiality clause, are included in the program agreement.

6) Do other systems share data or have access to the data in the system?

__yes
_X_no

If yes,

a. Explain the interface.

b. Identify the role responsible for protecting the privacy rights of the public and employees affected by the interface.

It is the responsibility of both the FMS and Citibank. It is a dual role since the operations take place at Citibank and the information resides within the TWAI, which is a Treasury network.

7) Will other agencies share data or have access to the data in this system?

__yes
_X_no

If yes,

a. Check all that apply:

__Federal
__State
__ Local
__Other (explain) _____

b. Explain how the data will be used by the other agencies.

No agency has access to any ECP data except the Federal Prison Agency on whose behalf the General Lockbox is processing items.

c. Identify the role responsible for assuring proper use of the data.

The ECP System Owner is the person responsible for assuring proper use of the data.