The Bureau of the Fiscal Service

Privacy Impact Assessment

The mission of the Bureau of the Fiscal Service is to promote the financial integrity and operational efficiency of the federal government through exceptional accounting, financing, collections, payments, and shared services.

This Privacy Impact Assessment is a Public document and will be made available to the general public via the Fiscal Service Privacy Impact Assessment (PIA) webpage (shown below).

Fiscal Service - Privacy Impact Assessments (PIA):
http://www.fiscal.treasury.gov/fsreports/rpt/fspia/fs_pia.htm

Name of System: Electronic Check Processing (ECP) System

Document Version: 3.0

Document Date: May 23, 2017

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 image archiving solution.

2) **Under which Privacy Act System 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?**

   The legal authorities applicable to this system are:

   5 U.S.C 301 Departmental Regulations
   31 U.S.C 321 General Authority of the Secretary
   31 U.S/C Chapter 33 Depositing, keeping, and paying money
   31 U.S.C 3720 Collection of Payments

DATA in the SYSTEM:

1) **Identify the category of individuals in the system**
   Check all that apply:
   __ Employees
   __ Contractors
   X Taxpayers

__ **Others (describe)**

2) **Identify the sources of information in the system**
Check all that apply:
__ **Employee**
X **Public**
__ **Federal agencies**
__ **State and local agencies**
X **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 images of both the financial instrument and remittance document(s) for a payment, related financial data and user defined data fields that have been determined by the Federal agency as necessary for its records.

c. **What Federal agencies are providing data for use in the system?**
Agencies participating in the Fiscal Service's 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?**
- US Bank (Financial Agent)
- Bank of America (Financial Agent)
- JP Morgan (Financial Agent)
- PNC Bank (Financial Agent)
- Sallie Mae/Navient (Student Loan Service Provider)
- Nelnet (Student Loan Service Provider)
- PHEAA (Student Loan Service Provider)
- Great Lakes (Student Loan Service Provider)
- ACS/Maximus (Student Loan Service Provider)

3) **Accuracy, Timeliness, and Reliability**

a. **How will data collected from sources other than Fiscal Service records, be verified for accuracy?**
ECP is a pass through system, which relies on the Financial Agents (FA) to send complete and accurate transaction data files. Before the data files provided by FA's are uploaded into ECP, they are systematically checked to ensure that they meet the vendor interface specifications for that file type (each file type has its own specification). The data from the files matching all vendor interface specifications is loaded into ECP. If there is an error, the entire file is rejected by the system and an email is sent to the applicable FA containing the reason for the rejection so they can correct the issue and resends the file.

b. **How will data be checked for completeness?**
ECP is a pass through system, which relies on the FA to send complete and accurate transaction data files. Before the data files provided by FA's are uploaded into ECP they are systematically checked to ensure that they meet the vendor interface specifications for that file type (each file type has its own specification). The data from the files matching all vendor interface specifications is loaded into ECP. If there is an error, the entire file is rejected by the system and an email is sent to the applicable FA containing the reason for the rejection so they can correct the issue and resend the file. 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.

c. **What steps or procedures are taken to ensure 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.

d. **In what document(s) are the data elements described in detail?**
The data elements are described in detail and documented in the Agency Cash flow Profile (ACP).

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 check 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?**
Not applicable.

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

5) **How will the new data be verified for relevance and accuracy?**
Not applicable.

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 various cash flows is consolidated within the ECP system. The users at each agency has 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

(link) and access to reports through the reporting process. Roles for page-level access within the application 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 principle of both "separation of duties" and "least privilege". ECP follows NIST and Treasury-Fiscal Service 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)**
ECP 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?**
None.

10) **What opportunities do individuals have to decline to provide information (i.e., in such cases 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?**
ECP does not have the ability to give individuals consent to decline information provided to agencies. The ECP application is not for personal use and it is not accessible to the general public.

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. The system will retain up to 2 years of data online, with an additional 5 years of data in archive. The entire retention period being a total of 7 years. 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 Revenue Collections Management 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?**
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 support system 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 Fiscal Service 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?**
   Not applicable.

6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**
   Yes, this system provides a real-time monitor to report audit events and application exceptions involving the 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 modification made to the 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 to identify any security violations (invalid logins) and that report is retrieved and reviewed on a daily basis by the Information 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.

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 contracts for the Federal Agency and the lockbox banks. All privileges granting access to the users are processed by the Information Security Staff.

3) **Will users have access to all data on the system or will the users' 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 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 View 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?**
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?**
X yes
__ no

If yes,

a. Explain the interface.

Each of the following entities have a secured file transfer instance specifically created for sharing data with ECP.

- Financial Agents – Financial and remittance information
- Department of Education Return Files Servicers – Financial and remittance information
- Debit Gateway – Check images and financial information
- Collection Information Repository – Financial and remittance information

b. Identify the roles responsible for protecting the privacy rights of the public and employees affected by the interface.
The ECP System Owner and ISSO are responsible for assuring proper use of the data.

7) **Will other agencies share data or have access to the data in this system?**
X yes
__ no

If yes,

a. Check all that apply:
X Federal
__ State
__ Local
Other (explain) _____

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

ECP allows agency users to update remittance information for their own Viewshields (only their own remittances).

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

The ECP System Owner and ISSO are responsible for assuring proper use of the data.