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: May 22, 2012

Document Version: Version 1.1

Name of System: Electronic Federal Tax Payment System

SYSTEM GENERAL INFORMATION:

1) System Overview: Describe the purpose of the system.

Operational since October of 1996, EFTPS (Electronic Federal Tax Payment Systems) is an electronic remittance processing system used to accept and process electronic information pertaining to all types of United States Government Federal tax payments. Due to the necessary security controls that must be in place to ensure data integrity and confidentiality of data, this system has been classified as a major application. Corporations, individuals, and Federal Agencies (agencies) remit taxes to the Internal Revenue Service and the United States Treasury through this system which provides mechanisms that:

- allow the efficient exchange of payments from the private sector and agencies to the government;
- enhance accessibility for use of Electronic Funds Transfer (EFT) by business, individual, and agency taxpayers;
- transmit agencies' 941 tax filings to the government;
- and, allow sufficient and flexible information.

Bank of America is the EFTPS Financial Agent (FA) that processes and financially settles the various Federal tax payment types. Bank of America sub-contracts their Information Technology development and operations to First Data.

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. EFTPS information consists of Taxpayer/Employee Identification Number (TIN/EIN); Personal Identification Number; Internet access password; Name; Address; Phone Numbers; Social Security Number; Financial History (including Bank Account Info); and, Tax Forms

b. Is the information about employees or contractors?

No

5) What legal authority authorizes the purchase or development of this system?

The Secretary of the Treasury has authority to designate financial institutions as depositaries and financial agents of the United States to perform essential banking services pursuant to 12 United States Code (U.S.C.) §§ 90 and 265, 31 U.S.C. § 3303, and other authorities. The Secretary of the Treasury has delegated to FMS the authority to select and designate depositaries and financial agents for, among other purposes, providing EFTPS and related services.

EFTPS is a major application of the Financial Management Service and Bank of America is the EFTPS Financial Agent (FA) that processes and financially settles the various Federal tax payment types. Bank of America sub-contracts their Information Technology development and operations to First Data Government Solutions.

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
_x_ Federal agencies
__ State and local agencies
_x_ Third party

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

No information is collected from employees or contractors.

b. What information will be collected from the public?

The following information is collected:

- Taxpayer Identification Number; Personal Identification Number; Internet access password; Name; Address; Phone Numbers; Social Security Number; Financial History (including Bank Account Info); Tax Forms.
- Employee Identification Number; Personal Identification Number; Internet access password; Name; Address; Phone Numbers; Social Security Number; Financial History (including Bank Account Info); Tax Forms.
- Significant audit trails, ranging from firewall logs, router logs, intrusion detection logs and user logon activity
- Google Analytics; network traffic to include date; time; originating Internet Protocol (IP) address; type of browser and operating system used (if provided by the browser); URL of the referring page (if provided by the browser); the object requested; completion status of the request; pages visited on our site

c. What Federal agencies are providing data for use in the system?
The Internal Revenue Service provides data for use in EFTPS.

d. What State and local agencies are providing data for use in the system?
No state or local agencies provide data for use in EFTPS

e. From what other third party sources will data be collected?
Various Bulk & Batch Providers as identified by the IRS provide data to EFTPS.

3) Accuracy, Timeliness, and Reliability

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

Once the taxpayer has supplied required data elements at the Web site, several steps are taken to ensure accuracy, timeliness and completion. Within 24 hours, taxpayer data is sent to IRS Memphis for validation against the masterfile. Banking information is verified by sending a standard electronic non-monetary transaction to the taxpayer's bank. The taxpayer's bank has five days to respond to this transaction. At the end of this period, the taxpayer is sent correspondence that includes all information that the taxpayer submitted at the Web site. The taxpayer has the opportunity to review and update this information. Customer service numbers are provided. If the taxpayer information fails any of the described validations, a letter is sent to the taxpayer explaining the error and the corrective action required.

b. How will data be checked for completeness?

Once the taxpayer has supplied required data elements at the Web site, several steps are taken to ensure accuracy, timeliness and completion. Within 24 hours, taxpayer data is sent to IRS Memphis for validation against the masterfile. Banking information is verified by sending a standard electronic non- monetary transaction to the taxpayer's bank. The taxpayer's bank has five days to respond to this transaction. At the end of this period, the taxpayer is sent correspondence that includes all information that the taxpayer submitted at the Web site. The taxpayer has the opportunity to review and update this information. Customer service numbers are provided. If the taxpayer information fails any of the described validations, a letter is sent to the taxpayer explaining the error and the corrective action required

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

Once the taxpayer has supplied required data elements at the Web site, several steps are taken to ensure accuracy, timeliness and completion Within 24 hours, taxpayer data is sent to IRS Memphis for validation against the master file. Banking information is verified by sending a standard electronic non-monetary transaction to the taxpayer's bank. The taxpayer's bank has five days to respond to this transaction. At the end of this period, the taxpayer is sent correspondence that includes all information that the taxpayer submitted at the Web site.

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

Data elements are described in detail and documented in the *EFTPS Security Plan.*

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 data items are required for business purposes. All data is used to complete required fields for posting information to IRS and funds to FMS.

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?**

EFTPS will not derive new data or create previously unavailable data about an individual through aggregation from the information collected.

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 system maintains significant and comprehensive security features that were designed into the WWW interface to ensure that risks posed by Internet threats are effectively countered.

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

The system maintains significant and comprehensive security features that were designed into the WWW interface to ensure that risks posed by Internet threats are effectively countered.

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**

- All users initiate a Secure Socket Layer (SSL) session and identify and authenticate themselves by using a Taxpayer Identification Number (EIN or SSN), PIN, and Internet password before they are given access to data within EFTPS-Online.
- Each individual maintains a unique identifier per the EFTPS security requirements.
- For taxpayer access, subsequent to authentication with TIN, PIN and Password, only data pertaining to their own records is accessible.
- For internal users, there are policies in place, including Unauthorized Access (UNAX), as well as audit trails of who accesses the data retrieve data.

9) **What kind of reports can be produced on individuals? What will be the use of these**

reports? Who will have access to them?

Some application activity logs (audit trails) are maintained that can monitor the activity of taxpayers. These logs are maintained for security purposes and are protected against unauthorized access. Users, Managers, System Administrators and Developers will have access to this information. Special access is provided to users via Resource Access Control Facility (RACF). Other reports generated by EFTPS do not contain information specific to individuals

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?

- Individuals may choose to use or not use EFTPS.
- EFTPS provides privacy notices, accessibility statements and agreement notices that individuals can accept or decline prior to providing and/or submitting information.
- Warning notices are used to inform taxpayers that activity monitoring may occur.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

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

- EFTPS retains data for seven (7) years, seven (7) months. The reports are destroyed as described in the EFTPS Security Plan.
- Google Analytics retains data for a minimum of 90 days to comply with National and Records Administration requirements. Report data will be retained for (7) years, seven (7) months..

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

- Prior to eliminating the data after the (7) year, (7) month retention period, FD validates with FMS that the data may be eliminated. After approval, data is eliminated following one of the destruction methods as defined in the *EFTPS Security Plan,* depending on the medium.
- Google Analytics will be configured to dispose of the data after 180 days of online access. Disposition procedures will be documented in the Google Analytics user guide.

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 system is operated in more than one site, and data is replicated between sites.

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

EFTPS is not using technologies in new ways that FMS has not previously employed.

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.

Yes. EFTPS can be used to identify or locate individuals. Some application activity logs (audit trails) are maintained that can monitor the activity of taxpayers. These logs are maintained for security purposes and are protected against unauthorized access. Also, warning notices are used to inform taxpayers that activity monitoring may occur. The system does not provide the capability to monitor groups

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

Some application activity logs (audit trails) are maintained that can monitor the activity of taxpayers. These logs are maintained for security purposes and are protected against unauthorized access.

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

EFTPS employs an intrusion detection system (monitored 24 hours, 7 days per week, 365 days per year) that prevents unauthorized monitoring. In addition, the *EFTPS Incident Response Plan* outlines how FDGS handles any security threats. Refer to Appendix A - Input/Output file and the *EFTPS Security Plan* for a detailed description of controls in place.

ACCESS TO DATA:

1) Who will have access to the data in the system?
Check all that apply:

__ Contractors
_x_ Users
_x_ Managers
_x_ System Administrators
_x_ System Developers
__ Others (explain)_____

Special access is provided to users via Resource Access Control Facility (RACF). Taxpayers are provided access to their own information via an Internet World Wide Web (WWW) Interface after being properly authenticated by a TIN, PIN and password.

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

- For taxpayer access, subsequent to authentication with TIN, PIN and Password, only data pertaining to their own records is accessible.
- For internal users, there are policies in place, including UNAX, as well as audit trails of who accesses the data.
- Access is not governed by form 5081 for EFTPS-Online processing.

This is documented in the *EFTPS Security Plan*

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

Taxpayers will only have access to their own records once being authenticated with their TIN, PIN and password. For internal users, access control is based on least privilege, which refers

to granting users only the minimum access required to perform their duties as described in the *EFTPS Security Plan.*

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)

EFTPS maintains audit trails of who accesses data. In addition, all employees and contractors are made aware of security, confidentiality and "unauthorized access of taxpayer data" (UNAX) violations through mandatory annual security awareness training. Security, UNAX, and confidentiality information is also distributed to all employees and contractors during training. Each employee and contractor is required to sign a security training and compliance acknowledgment form, which is maintained on file by Human Resources. All employees and contractors are made aware that the penalties for knowingly violating these policies can include dismissal from the company and possibly criminal prosecution that may include fines and imprisonment.

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, Bank of America is involved in the design, development, and maintenance in EFTPS. Approved contractors may be involved with the design, development and maintenance of EFTPS. All contractors go through the same background checks and screening as employees and must obtain EFTPS security clearance prior to having access to EFTPS. Contractors are subject to all security and Privacy Act regulations as employees, including a signed security training and compliance acknowledgement form maintained on file in a Treasury Folder by Compliance. In addition, there is a clause in the agreement (Section 5 G) that addresses privacy act information

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.

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.

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

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