



Financial Management Service

Pay.gov

Privacy Impact Assessment

2.0

July 1, 2011

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: 07/01/2011

Name of System/Application:

Pay.gov

System Overview:

The Financial Management Service of the U.S. Treasury designed and developed Pay.gov to support their enterprise-wide commitment to processing electronic collections using Internet technologies. Pay.gov satisfies agency and consumer requests for electronic payment alternatives by providing the ability to complete forms, make payments, and submit queries twenty-four hours a day from any computer with Internet access.

Launched in October 2000, Pay.gov is a secure government-wide collection portal. Pay.gov provides a suite of services and interface options through which Pay.gov processes collections in an efficient, timely, secure manner for Federal agency programs.

Pay.gov services include:

- Collections Service, which processes Automated Clearing House (ACH) direct debit and plastic card payments.
- Billing Service, which receives invoice data from agency systems, formats the data for viewing, and notifies agency customers via email of payment due.
- Forms Service, which enables agency customers to submit completed forms to agencies, electronically, with or without payment.
- Reporting Service, which provides agencies with online or as an electronic file all payment and form data submitted by their customers, including the settlement status for all ACH payment transactions.

Pay.gov helps Federal agencies meet the directives outlined in the Government Paperwork Elimination Act (GPEA), primarily by reducing the number of paper transactions and utilizing electronic transaction processing over the Internet.

System of Records Notice (SORN):

FMS .017—Collections Records

SYSTEM APPLICATION/GENERAL INFORMATION:

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

a. Is the information about individual members of the public?

YES

b. Is the information about employees or contractors?

NO

DATA in the SYSTEM:

1) Categories of individuals covered in the system

Check all that apply:

Employees

Contractors

Taxpayers

Note - not individual taxpayers

Others (Individuals and Businesses paying for goods, services, fees, or taxes to the Federal Government).

2) Identify the sources of information in the system

Check all that apply:

Employee

Public

Federal agencies

State and local agencies

Third party sources

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

In order to populate bills, Pay.gov obtains billing information from Federal agencies that choose to use the Internet Cancellations service.

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

None

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

None

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

Profile information for the employee user accounts is stored but it is not their private information but profile information related to their employment.

e. What information will be collected from the public?

Pay.gov obtains forms information and edited bill information from end-users.

Pay.gov obtains collection information from end- users. Pay.gov obtains authentication information from end-users, including user profile information from our customers.

3) Accuracy, Timeliness, and Reliability

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

Form and billing information provided by end- users is subject to error checking to ensure that the information is accurate. This error checking primarily occurs on the end user's browser to ensure the validity of the information, according to rules set out the by agency responsible for the bill or form. Billing information provided by agencies is checked for accuracy by the agency. Payment information provided by Treasury agents is checked for accuracy by the agents. Collection information provided by end- users is subject to browser-based and server-side validation checking to ensure that the information is accurate. These edits include eliminating the possibility of zero-dollar transactions and the scheduling of

collection dates in the past. In addition, financial account information is subject to edits to ensure that, for Automated Clearing House debits, that the routing number is valid and that the account structure is reasonable and for credit card collections, that the card is valid. Additional proofing and balancing is performed.

The system validates the data entered against the Allowable ASCII Characters (White List) defined in the Pay.gov Glossary document, either against version 1 or version 2, depending on the data type.

Additionally, all search queries against the database use prepared statements to prevent Sql Injection attacks.

b. How will data be checked for completeness?

In addition to the steps required for accuracy, Pay.gov ensures that required fields to perform a function are entered to ensure completeness of the transaction.

c. What steps or procedures are taken to ensure the data is current and not out-of-date?

Validation occurs for payments to ensure that scheduling of collection dates are not in the past. In addition, financial account information is subject to edits to ensure that the routing number is valid and that the account structure is reasonable and for credit card collections, that the card is valid.

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

Pay.gov has developed a “Data Elements” document that is updated with every release of Pay.gov. This document includes the parameters of each data element such as length, valid values, default values, etc.

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?

Form and bill information is set out by the agency; Pay.gov simply facilitates agency programs in this regard. Collection information includes only that which is necessary for collection networks to process collections.

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?

NO

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

N/A

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

N/A

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?

Pay.gov maintains comprehensive security features that were designed into the interfaces to ensure that risks posed by Internet threats are effectively controlled. Secure Coding Standards

are followed to prevent web security vulnerabilities and sensitive data is properly stored encrypted within the database. Pay.gov also provides an encryption option for the custom collections fields provided to the cashflows.

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

Pay.gov maintains comprehensive security features that are designed into all of the Pay.gov processes and interfaces.

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.)

Personal Identifiers are not used for authentication /authorization to data. Access is through the Pay.gov web interface with unique identifiers, through TCS with certificated based authentication, or through Pay.gov system-to-system interfaces.

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

Pay.gov requirements concerning Personal identifiable information is to mask the information when presented in reports unless an exception to a specific business requirements prevent it, such as Pay.gov Payer Profile functionality which involves Bank Account Data. Credit Card data is always masked.

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 can individuals grant consent.)

Pay.gov 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. Authenticated users must accept a Rules of Behavior before accessing the system.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

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

Records for payments and associated transactions will be retained for seven years or as otherwise required by statute or court order.

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

Records in electronic media are electronically erased using industry-accepted techniques. The procedures for this process are document in the Pay.gov system security plan.

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 Pay.gov production environment has a primary and an alternate site, alternating between the Consolidation Center 3 (CC3) at the FRB of Dallas, Texas and the Federal Reserve Information Technology (FRIT) Consolidation Center 1 (CC1) at the East Rutherford Operations Center (EROC) in New Jersey. In the event of a primary site failure, Pay.gov

production will be relocated to the alternate site. Data replication, along with additional backups, is used to facilitate the recovery.

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

Pay.gov is not using technologies in 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.

Pay.gov maintains and monitors audit logs of user activity while accessing the system

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

User activity is logged to identify the processes performed by the user but the financial transaction information such as account numbers or Credit Card data is not logged.

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

Access to audit logs are strictly controlled and limited to authorized personnel

ACCESS TO DATA:

1) Who will have access to the data in the system?

Check all that apply:

Contractors

Users

Managers

System administrators

System developers

Others (explain) _____

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

Pay.gov uses roles and their associated functions or permissions to assign access and enforce “separation of duties”. Roles in Pay.gov are broken down as follows:

System-level roles

Application-level roles

Customer-level roles

Resource-level roles

A role would allow the user to perform a specific function but Pay.gov has an additional control as to what they will be able to see at a data level, at either an application or a resource.

Pay.gov has an Agency Guide for Access Control for our Agency partners and an Administrative Guide for Access Control used internally. A Roles and Permissions matrix is maintained to identify the various permissions assigned to each role. Over twenty roles have been defined for Pay.gov.

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

For Pay.gov, the roles and permissions defined have been created enforcing the principle of “separation of duties” and “least privilege”.

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)

Pay.gov maintains audit trails of who accesses data. In addition, all Pay.gov FRBC users are made aware of security, confidentiality, and “unauthorized access of customer data” through mandatory Annual Security Awareness training.

Pay.gov encrypts all of the financial data (account numbers and credit cards) within the database.

Credit card information returned to our customers is masked, only showing the last four characters. Except for special roles involving Payer Profile, account number information is also masked.

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?

N/A

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

yes

no

If yes,

a. Explain the interface.

The Debit Gateway will store information transmitted from Pay.gov for ACH payments.

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

Debit Gateway access is restricted to personnel only at FRBC.

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

yes

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.