The Bureau of the Fiscal Service

Privacy Impact Assessment

The mission of the Bureau of the Fiscal Service (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/fspia/fs_pia.htm

Name of System: Pay.gov

Document Version: Version 1.7

Document Date: 02/03/2018

SYSTEM GENERAL INFORMATION:

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

Pay.gov offers a suite of online services that federal agencies can use to meet their responsibilities towards the public. The purpose of the Pay.gov system is to provide federal agencies with a transaction portal to use in processing forms, bill, authentication decisions, collections, and for obtaining information about those transactions. The information concerns federal agency transactions involving the public; both consumers and businesses.

2) Under which Privacy Act Systems of Records Notice (SORN) does the system operate? Provide number and name.

Not Applicable-- primary use of the system is not to search on personal identifiers.

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
_X_ 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
_X_ Public
_X_ Federal agencies
__ State and local agencies
_X_ Third party

a. What information will be collected from employees or contractors?
None

b. What information will be collected from the public?
Pay.gov obtains forms information and edited bill information from end-users. Pay.gov also obtains collection information from end- users, as well as authentication information from end-users, including user profile information from its customers.

c. What Federal agencies are providing data for use in the system?
Pay.gov helps many 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 so both remittance data through bills and forms and transaction data are stored.

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?
- Settlement data from digital wallet providers will be collected for payments made on their sites originating from Pay.gov.
- Authorization and settlement data from financial institutions will be collected for the purposes of transaction processing in Pay.gov.
- Transaction risk scores will be collected from fraud monitoring vendors for the purposes of fraudulent transaction screening in Pay.gov.

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

a. How will data collected from sources, other than Fiscal Service 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 also 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.

The data returned from fraud mitigation vendors will adhere to Pay.gov system specifications. The Pay.gov application will also perform a check against various data elements to ensure that they tie to the correct transaction.

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?
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.

The data returned from fraud mitigation vendors is a result of real-time risk scoring, so it is inherently always current.

d. In what document(s) are the data elements described in detail?
Pay.gov has developed a process for capturing data elements, which are stored in the application's Configuration Management tool.

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 sent 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.

The settlement data from the digital wallet providers is relevant and necessary for collections from those payment mechanisms.

The data returned from fraud monitoring vendors is relevant and necessary to evaluate transactions for risk scoring purposes.

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?**

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 federal agencies.

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.)**

The data will be retrieved by running reports using fields such as transaction ID, dollar amount, and/or date range. No personal identifiers are used to retrieve information on individuals.

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

Reports can be generated to identify activity surrounding transactions and processes performed by individuals. Pay.gov masks any Personally Identifiable Information when presented in reports unless there is an exception to a specific business requirement that prevents it. Access to these reports is granted based on proper authorizations and need to know.

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?**

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 transactions will be retained for seven years or as otherwise required by statute or court order. However, except as required by law or business, transactions will be archived after 18 months and that data will not be directly accessible through reports.

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 documented in the 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?**

Pay.gov production environment has a primary and an alternate site. 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 Fiscal Service has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

The system is leveraging fraud monitoring services for the purposes of fraudulent transaction screening.

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

As stated in Pay.gov's Privacy and Security Policy (www.pay.gov/public/home/privacy), transaction data that is necessary for fraud screening is sent to third party vendors. Access to this data is limited based on need to know, any sensitive/PII data is encrypted both during transmission and at rest, and appropriate controls are in place to ensure that there is no impact to public privacy.

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

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

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

The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event to help troubleshoot issues or to support after-the-fact investigations of security incidents. However, any information identified as sensitive is not stored in these records.

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
_X_ 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 additional controls relative to what they will be able to see at a data level.

Pay.gov has an Agency Guide to Access Control for its Agency partners and an Administrative Guide to Access Control that is used internally. A Roles and Permissions matrix is also 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 to enforce the principles 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 user activity. In addition, all Pay.gov Federal Reserve Bank (FRB) 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 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?**
Not Applicable

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

If yes,

a. Explain the interface.
- Transaction data will be passed to the Debit Gateway application for ACH payment settlement.
- Transaction data will be passed to digital wallet providers for payment processing.
- Transaction data will be passed to fraud monitoring vendors for fraud risk scoring.
- Federal Agency systems will be able to pull their own reporting data from Pay.gov.

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

The System Owner is responsible for protecting the privacy rights of the public and employees affected by any systems that interface with Pay.gov.

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.

Agencies can access transaction data for their own applications for the purposes of reporting and accounting.

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

The security contacts at each federal agency and the Pay.gov User Provisioning Team are jointly responsible for assuring proper use of the data.