Financial Management Service
Privacy Impact Assessment Template

Name of Project: Pay.gov
Project's Unique ID: Pay.gov

A. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes

a. Is this information identifiable to the individual[1]?
(If there is **NO** information collected, maintained, or used that is identifiable to the individual in the system, the remainder of the Privacy Impact Assessment does not have to be completed).

Yes

b. Is the information about individual members of the public?
(If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security C&A documentation).

Yes

c. Is the information about employees? (If yes and there is no information about members of the public, the PIA is required for the FMS IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation).

Yes, employees could be part of the system either as: admin, general public and self enrolled. System coverage of payment information currently is limited to a handful of agency records, e.g., social security administration payments, IRS payments, and payments to federal employees. Employees could fall into these categories.

[1] "Identifiable Form" - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

2) What is the purpose of the system/application?

Pay.gov has been developed to meet the FMS commitment to process collections electronically using Internet technologies. Pay.gov also meets the directives outlined in the Government Paperwork Elimination Act, primarily the reduction of paper transactions through the use of electronic processing via the Internet.

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. The information includes forms and billing data and associated collections, payment information, and authentication information that can draw in part upon the payment and collection histories. Intra-Governmental transactions are not included.

Form and billing information can cover any of the items that appear on a Federal agency form or bill, if processed by Pay.gov. Eventually, this information may include form and billing information processed by the FMS' paper lockboxes.

Collection and payment information can include transaction amounts, methods, financial account information, names, addresses, Taxpayer Identification Numbers, agency deposit and debit ticket numbers, Treasury and agency account symbols, agency location codes, Treasury and agency transaction identifiers, transaction dates, and transaction statuses. System coverage of collection information currently is limited to certain electronic transactions handled by Pay.gov, but this coverage may eventually expand to include other information, including paper lockbox transactions. System coverage of payment information currently is limited to a handful of agency records, including Social Security Administration payments, Internal Revenue Service payments, and payments to Federal employees, but will include other methods in the future. With the exception of certain credit card credits, Pay.gov does not process payments but rather uses this information only for authentication purposes.

Authentication information can include the above as it relates to specific persons, as well as telephone numbers, driver's license numbers, dates of birth, employer information, and usernames and passwords. It will include the end-user's roles for particular electronic resources (Web pages or applications) as well as a handful of agency-specific "extension" fields that limit the scope of particular roles, can be used for pre-population of forms, or the handling of application-level business rules.

3) What legal authority authorizes the purchase or development of this system/application?

This development of this system was authorized by the Bureau's Governance Board. The Pay.gov application has undergone a stringent certification and accreditation process, resulting in approval of full authority to operate (ATO).

B. DATA in the SYSTEM:

1) What categories of individuals are covered in the system?

This system collects data from the public, both consumers and businesses.

2) What are the sources of the information in the system?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

In addition to credit/debit card and ACH transactions processed by Pay.gov, Pay.gov obtains payments information from daily files received from Treasury agents that are fed into a larger Treasury payments database, named PACER. Pay.gov obtains collection information from the Treasury agents and contractors that process collections. Pay.gov authentication administrators will provide some authentication information.

b. 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 service, but some of this information may be changed by end-users at the time of transaction to the extent the agency allows. Federal agencies also eventually will provide authentication information, for end-users that the agency authenticates before redirecting into Pay.gov for the completion of a form, bill, or collection. The particular Federal agencies that provide data will change and accumulate over time.

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

No state and local agencies are directly providing data, but some information from third party databases used by Pay.gov's verification engine may include information originally in state databases, such as driver's license numbers.

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

Some of the collection information will result from processing by collection networks run by third parties, particularly the Automated Clearing House and credit card networks. Businesses may eventually provide some authentication information through business authentication administrators. Finally, the verification engine will require input from third party databases, in addition to the internal payment and collection records noted above, to judge the accuracy of information provided by end-users. Information obtained from third party databases will be maintained only for a short time in audit logs.

e. What information will be collected from the employee and 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 self-selected usernames and passwords.

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. Pay.gov also applies certain edits prescribed by PACER to ensure that the information is properly formatted.

Collection information provided by end-users is subject to browser-based and server-based error 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 (internal checking of information) and balancing (checking information against external sources) is planned for future releases.

Authentication information provided by end-users is compared with information contained in Pay.gov and 3rd party databases (Government and commercial) to ensure that the information is accurate. Multiple databases are used because of the possibility that any one database is inaccurate in its information. A Pay.gov "verification engine" will consolidate the results from the various database comparisons to provide confidence levels associated with each data element supplied by the end-user, as well as overall. If these confidence levels meet Pay.gov or another agency's standards, the end-user is authenticated and authorized to use those services that required this type of "ad hoc," time-of-transaction, knowledge-based authentication.

b. How will data be checked for completeness?

Form and billing information provided by end-users is subject to error checking to ensure the completeness of the information. 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. Incomplete information will be rejected. Billing information provided by agencies is checked for completeness by the agency and is subject to checks by Pay.gov to ensure completeness. If incomplete, the information will be rejected.

Payment information provided by Treasury agents is checked for completeness by the agents. Pay.gov also applies certain edits prescribed by PACER to ensure that the information is properly formatted.

Collection information provided by end-users is subject to browser-based and server-based error checking to ensure that the information is complete. These edits include ensuring that all necessary fields are provided. Information processed as files by agents will have header information that summarizes the transactions contained in the file; if the file information differs from the header, an exception is thrown. Additional proofing (internal checking of information) and balancing (checking information against external sources) is planned for future releases.

Authentication information provided by end-users is subject to browser-based and server-based error checking to ensure that the information is complete. The verification engine will invoke multiple databases to mitigate the possibility that any one database is incomplete in its coverage.

c. **Is the data current?** What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

All information provided by end-users, Treasury agents and contractors is presumed to be current when first provided, except for certain authentication information obtained from third party databases. This information could be out of date. In addition, when used for authentication, payment and collection information from Treasury databases could be out of date. Due to the limitations of knowledge-based authentication systems (accuracy, completeness, timeliness), multiple databases are used to provide the best chance of a true result.

d. **Are the data elements described in detail and documented?** If yes, what is the name of the document?

At a high level, the data elements are spelled out in a definition appendix to the document, "Pay.gov Concept of Operations." More particularly, form and bill elements are set out in agency configuration templates (ACTs) or, for documents that pre-date the ACT, in agency-specific requirements documents. Collection elements and payment elements are spelled out in two data dictionaries. Verification engine elements are spelled out in the interface to that service.

C. ATTRIBUTES OF THE DATA:

1) 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. Authentication information includes a wide range of information when used for knowledge-based authentication, but this is unavoidable in creating a workable knowledge-based system. Pay.gov authentication credentials also include a wide range of values, but use of this data facilitates agency program needs, simplifies completion of form, bill, and collection transactions, and in any event, end-users are able to edit many profile fields.

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?

The verification engine will develop confidence percentages based upon the consolidation of query results posed to multiple databases. Pay.gov will not retain these confidence percentages except in audit logs. Pay.gov also may reformat certain financial account information to ensure that it can be processed. Otherwise, Pay.gov will not derive new data or create previously unavailable data about an individual through aggregation.

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

No new data or create previously unavailable data about an individual created through aggregation will be placed in an end-user's record.

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

The verification engine requires consolidated results to ensure the best chance of a true result. Certain Automated Clearing House transactions would be impossible without reformatting of end-user data.

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

The databases used by the verification engine are subject to review to ensure that they provide relevant, accurate, and complete information, and the verification engine accounts for imperfections between databases. The system used to reformat collection information is an off-the-shelf system used by major financial institutions; furthermore, if there are problems with the data, the data will trigger returns when submitted for collection.

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

Consolidated data is maintained only in audit logs, which are available only to system administrators with two-factor authentication issued by the Treasury Web Application Infrastructure. Information also will be made available to other program representatives, including developers, as determined by the Pay.gov program manager or the Pay.gov information system security officer as needed to investigate improvements, security breaches, or possible error resolution. However, all access is subject to the same restraints as set out above for non-consolidated data.

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

Pay.gov consolidates several processes:

- Collections
  - ❑ Automated Clearing House debit
  - ❑ Credit and debit cards
  - ❑ Fedwire (initiated offline)
- Forms and bills
- Authentication
  - ❑ Ad hoc authentication
  - ❑ Agency authentication
  - ❑ Pay.gov usernames and passwords
    - ▪ Issued after ad hoc authentication
    - ▪ Issued after entry of information by:
      - Pay.gov authentication administrator
      - Agency authentication administrator
      - Business administrator
- Reporting
  - ❑ Electronic (non-Web) to agency systems
  - ❑ Web-based to reporting analysts

The controls for these processes are set out in this document.

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

Database administrators will be able to retrieve data from databases and system administrators from audit logs by personal identifier. In addition, searches of the payment information by the verification engine will be by personal identifier. Otherwise, searches by other Pay.gov personnel can only be by non-personally identifying fields, with the exception of financial account information (account or card number).

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

Reports based on personally identifying fields are not allowed.

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 individuals can grant consent.)**

Information necessary to conduct a credit card or ACH transaction is required. Agencies can also require other information based on their need. In this case, the agency determines what information individuals have the opportunity to decline.

D. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

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

The 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.

2) **What are the retention periods of data in this system?**

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

3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

Records in electronic media are electronically erased using industry-accepted techniques.

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

Yes. The Web-enabling of forms, bills, collection authorizations, reports, and use of usernames and passwords is on a more robust scale than previously, but the FMS has provided solutions in these regards before. However, the verification engine presents new technology.

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

As noted above, the verification engine is a tool that is appropriate in some, but not all, situations. Used properly, it can enhance the public's privacy by giving greater electronic access to information and services. Used improperly, it can wrongly deny access to electronic services or allow another to wrongly access electronic services while impersonating someone else.

For these reasons, Pay.gov will require agencies to justify the reasonableness of their use of the verification engine, provide alternative methods of access, and use the verification engine only to verify information provided by the end-user. The verification engine will not be used for credit checks and requires that the database providers not keep information provided to it. Pay.gov also will ensure that any information transmitted to or from Pay.gov is done so securely. Pay.gov also will provide comprehensive notices to end-users as to the operation of the verification engine.

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

The verification engine and site monitoring software can be used to determine information relating to persons. The verification engine, described above, confirms information from end-users, including the end-user's name and address. It does not track or monitor individuals.

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

Like most Web sites, when a page is requested the FMS can obtain information about the request, such as the name of domain from which the visitor accesses the Internet (e.g. "a company.com"; "a school.edu; or "an agency.gov"), the Internet protocol number, date and time the Web site is visited, and type of browser and operating system used to access the site. This information is needed to maintain Pay.gov's audit logs.

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

Information in this regard will be made available only to system administrators. System administrators will have to sign a standard Treasury Security Manual Privacy Act non-disclosure agreement, if they are not FMS or fiscal agent employees. Information also will be made available to other program representatives, including developers, as determined by the Pay.gov program manager or the Pay.gov information system security officer as needed to investigate improvements, security breaches, or possible error resolution. All online access is conditioned upon agreement to the language contained on the "Notices and agreement" page, which includes rules of behavior. All personnel working on the FMS project also are bound by Pay.gov business and security requirements, standard operating procedures, and (for other agents and contractors) agreement provisions that protect privacy.

9) **Under which Privacy Act systems of records notice does the system operate? Provide number and name.**

Pay.gov will operate under the FMS' system of records entitled, "Revenue Collection Records – Treasury/FMS .017."

10) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

See the previous answer.

E. ACCESS TO DATA:

1) **Who will have access to the data in the system?** (E.g., contractors, users, managers, system administrators, developers, other)

Bill (including bills saved after editing) and saved form information will be made available to end-users, to the extent it involves their own transactions. An agency will have access to submitted bill and form information; to the extent it involves the agency. An agency will also be able to check the status of bills, as will Pay.gov customer service. Collection information will be made available to end-users, to the extent it involves their own transactions. An agency will have access to collection information; to the extent it involves the agency, as will Pay.gov customer service. Collection information also will be available to the depositary that processes the collection. By necessity, collection information must be shared with external networks such as the Automated Clearing House network and credit card network.

Authentication information will be made available to end-users to the extent it involves profile information associated with a Pay.gov username and password. This information will be made available to an agency if the end-user so agrees. It will be available to Pay.gov authentication administrator and to customer service. It will be available to an agency authentication administrator and a business authentication administrator if that administrator created the profile.

Responses from the verification engine will not be made available to end-users (except on a yes/no basis when used for limited, controlled "live demo" purposes) but will be made available to an agency if the end-user so agrees. By necessity, the information must also be shared with third parties that operate the databases that provide responses used by the verification engine.

The above will be available to Pay.gov program management and database administrators. Information also will be made available to other program representatives, including developers, as determined by the Pay.gov program manager or the Pay.gov information system security officer as needed to investigate improvements, security breaches, or possible error resolution.

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

Access to data by an end-user requires that an end-user be authenticated using a Pay.gov username and password. If it is for viewing form or bill information, the end-user also may be authenticated by an agency and handed to Pay.gov.

Access to data by an agency—either a representative or an agency system—requires authentication of the agency, either by Pay.gov username and password or by digital certificate (in the case of an agency system).

Access to data by Pay.gov program management and customer service requires a Pay.gov username and password. Pay.gov database administrators are authenticated. Access to profile data by a Pay.gov, business, or agency authentication administrator requires that the person be authenticated using a Pay.gov username and password.

All database administrators, Pay.gov management representatives, Pay.gov customer service representatives, and Pay.gov authentication administrators will have to sign Privacy Act non-disclosure agreements prescribed by the Treasury Security Manual if they are not FMS or fiscal agent[1] employees. All agents (other than fiscal agents) and contractors whose employees may access Privacy Act data have agreements that include Privacy Act provisions.

By necessity, certain information must flow to third party systems, such as collection information that is processed by Automated Clearing House and credit card networks. This information is subject to the same protections as other information that flows through those networks. Authentication information also is sent to third party database providers to obtain responses that can be used by the verification engine. However, by agreement, the third party database provider is not to retain any information delivered to it did not already own.

[1] Fiscal agents (Federal Reserve Banks) are waived from certain security requirements because of the strong internal controls followed by Federal Reserve Banks, as reflected in public audit results for those banks.

All online access is conditioned upon agreement to the language contained on the "Notices and agreement" page, which includes rules of behavior.

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

End-users will have Web-based access to see only their bills, saved (edited) bills, saved forms, and status of collections regarding submitted transactions, if authenticated by a Pay.gov username and password or through by agency authentication. End-users also have the ability to change profile information associated with their Pay.gov username and password.

Agency access depends upon the agency user. An agency will receive a file of electronic (but non-Web) details of forms, bills, and collections, and (for applications hosted on the agency site) authentication. A reporting representative also can receive Web-accessed reports, the details of which depend on the reporting representative's role. A detail analyst receives detail information regarding individual transactions tracked to a particular agency office; a summary analyst receives information tracked to additional agency offices, but at only a summary level. An agency authentication administrator may create (but not delete) end-users and add or remove roles or extension fields from end-users created by the administrator; the agency authentication administrator may delegate these abilities to business authentication administrators.

Depositary access entails the ability to receive detailed collection information needed to process collections, which by necessity entails use of collection networks, and provides replies on the status of collections. Depositary representatives also will be able to receive Web-based detail information regarding individual collections transactions that track to the depositary. Eventually, depositaries will provide information regarding paper lockbox transactions.

Pay.gov access depends on the Pay.gov user. Database administrators will have access to database information. System administrators will have access to audit logs. Pay.gov authentication administrators will have the ability to create and delete end-users and add or remove roles or extension fields from end-users. Pay.gov program management (including operators and information system security officer) and customer service will have access to online reporting information made available to end-users, depositaries and agencies.

Third parties will receive details of collections necessary to process collections and provide responses. Database providers will receive details necessary to provide responses back to the verification engine. Business authentication administrators will have the same access as agency administrators, insofar as business end-users for the agency's resources are concerned.

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 security requirements and the “Notice and agreement” page forbid browsing by personnel working for the Pay.gov project. In addition, only database administrators will have the ability to search records by an end-user’s name or Taxpayer Identification Number. All other personnel working for the Pay.gov project will have the ability to search only on non-personally identifying fields, with the exception of financial account information (account and card numbers). Agreements with the third party database providers require that the providers do not retain data elements not already possessed by the provider and include audit provisions.

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

No. If contractors at any point are to be used, contractors whose employees may access Privacy Act data have agreements that include Privacy Act provisions.

6) **Do other systems share data or have access to the data in the system? If yes, explain.**

No, access to data from the Pay.gov system is given on a user basis, not to other systems.

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

The Pay.gov program manager and information system security officer will have responsibility for ensuring compliance.

8) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)?**

Form, bill, and collection information is used by the agency as it chooses for its internal operations. Authentication information is shared with an agency when an agency has an application on its own site that requires authentication information. It may not be used for other purposes, such as credit checks on the end-user.

Insofar as ensuring that agencies only get the information to which are entitled, the form, bill, and collection information is needed for the agency’s programs. Although the collection information is also Pay.gov records, the information is otherwise the agency’s own information; Pay.gov is a pass-thru. Authentication information is provided only with the consent of the end-user, except for profile information created by agency authentication administrators.

In some respects, the authentication information that is shared from the verification engine is not a disclosure, let alone one under 26 § U.S.C. 6103. The information shared with the agency often reflects a consolidation of results obtained through the comparison of end-user provided data against multiple databases, some of which are not governmental databases. Other than successful confidence percentages, no additional data elements are passed to the agency other than that which was obtained from the end-user. Some confidence percentages can result from the payments database, which includes payments of IRS tax refunds, among other sources. However, there is no way to determine which payments are IRS refunds and which are payments from other agencies. Finally, sharing of detailed results with agencies will be only with the consent of the end-user, which is a stated exception to both the Privacy Act and 26 U.S.C. § 6103.

9) How will the data be used by the other agency?

Form, bill, and collection information is used by the agency as it chooses for its internal operations. Authentication information is shared with an agency when an agency has an application on its own site that requires authentication information. It may not be used for other purposes, such as credit checks on the end-user. Transaction data is used by the agency for financial reconciliation.

10) Who is responsible for assuring proper use of the data?

The proper use of the data is the responsibility of the information system security officer and the designated security contacts at the application level. As part of the Pay.gov implementation process, an implementing agency designates security contacts that are responsible for access and use of their data.