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/rpt/fspia/fs_pia.htm

Name of System: OneVoice Customer Relationship Management

Document Version: 2.0

Document Date: 01/18/2017

SYSTEM GENERAL INFORMATION:

1) System Overview:

The OneVoice Customer Relationship Management (CRM) is a cloud-hosted application used to manage interactions with business customers and vendors. All business areas within the bureau may access information based upon need-to-know. Customers include federal program agency contacts, state and local municipality organization contacts, and financial or fiscal agents.

2) Under which Privacy Act Systems of Records Notice (SORN) does the system operate?

Treasury/Bureau of the Fiscal Service .024-OneVoice Customer Relationship Management and Administrative Records – Treasury/FMS.001

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, The system could contain contact information for sole proprietors.

b. Is the information about employees or contractors?

Yes.

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

5 U.S.C. 301

DATA in the SYSTEM:

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

X Others (describe)

Federal program agency contacts, state and local municipality contacts, financial institutions contacts and vendors.

2) **Identify the sources of information in the system**
Check all that apply:
X Employee
X Public
X Federal agencies
X State and local agencies
X Third party

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

Last and first names, agency or organization identifier, position information (title and expertise area), contact information (physical work address, phone number, fax number and email address), status of agency implementations, key agency meeting dates, attendees, and meeting topics of discussion.

b. What information will be collected from the public?

If a contractor or vendor is a sole proprietor (or similarly structured) they may supply personal contact information.

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

Federal agencies provide contact or agency information to customer relationship managers throughout the Fiscal Service as part of doing business with the bureau.

d. What state and local agencies are providing data for use in the system?

State and local agencies provide contact or agency information to customer relationship managers throughout the Fiscal Service as part of doing business with the bureau.

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

Information may be collected directly from contractors and vendors and from Fiscal and Financial agents as part of doing business with the bureau.

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

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

Customer relationship managers check this data when it is entered. Information will also be verified when it is used.

b. How will data be checked for completeness?

Customer relationship managers check that information is complete when it is entered. If information is somehow incomplete, the oversight will be detected and corrected as the information is used.

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

Customer relationship managers entering and using data keep it current. For example, when speaking to a contact at an agency, a customer relationship manager will validate the latest contact information. A "last updated" field will be displayed on all records.

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

FS Design Document v4 (dated March 16, 2014)

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?

In order to successfully manage interactions with vendors and customers, the customer relationship managers must have ready access to relevant contact information.

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?

Currently this data exists in multiple spreadsheets located throughout the bureau. Some data will manually be entered and some will be loaded from existing spreadsheets or internal "flat files."

How will this be maintained and filed?

It will be maintained in the software service with appropriate security controls, views and controls.

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

Any updated data will be reflected in the organization contact record. The individual will always be associated with a business organization.

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

No. The system improves internal communication so that interactions between employees and Fiscal Service contractors, vendors and customers is more consistent and reliable, but doesn't make any new determinations possible.

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

Each time a customer relationship manager uses the system, they will be using the contact data. If it is incorrect, manual processes will be in place to update the data.

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

Data access will be consistent with Fiscal Service security baselines governing the principles of need-to-know and least privilege. Access controls have been identified by user roles and profiles. These rights are identified in the design document "FS Design Document v4 (dated March 16, 2014)."

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

Processes are not being 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.)

Identifying data will be retrieved via search/lookup functionality to include but not limited to:

- Last/first names
- Agency identifiers (district/location code; department/agency name; bureau name)
- Position information (i.e. title; expertise areas)
- Contact information (physical work address; e-mail address; work phone; cell phone/fax numbers;
- Information on the bureau's products and services;
- Information on upcoming meetings, conferences, and forums; and
- Updates on agency implementation status.

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 will be produced that are focused on business contact information per business relationship. These reports could include outstanding issues, specific contact information, account activity, etc.

What will be the use of these reports?

These reports will be used to more effectively work with the bureau's vendors and clients by allowing for more collaboration across the bureau's business areas.

Who will have access to them?

Individuals whose official duties include performing customer relationship management, agency outreach and program management roles, and SES leaders at Fiscal Service and Executive Leaders at the Federal Reserve.

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?**

Information collected and maintained in the system is provided by government agency employees, vendors, and contractors as business contact information. Contact information is collected from business cards, emails, conference attendance records, etc. Contacts are not specifically notified that their contact information is being kept in this system. It is implied at time of collection that the information will be kept in some system. Contact information is removed if anyone specifically asks us to remove them.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

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

The data will be regularly updated and therefore the contact information and reports will be available in adherence with Fiscal Service policy. For deleted data, the Fiscal Service vendor will ensure the system is supported in accordance with the requirement for Federal agencies to manage their electronic records in accordance with 36 CFR § 1236.20 & 12366.22 (ref. a), including but not limited to capabilities such as those identified in: DoD STD-5015.2 V3 (ref. b), Electronic Records Management Software Applications Design Criteria Standard, NARA Bulletin 2008-05, July 31, 2008, Guidance concerning the use of e-mail archiving applications to store e-mail (ref. c), 25 NARA Bulletin 2010-05 September 08, 2010, Guidance on Managing Records in Cloud 26 Computing Environments (ref. 8).

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

The disposition of all data will be at the written direction of the Fiscal Service Contracting Officer. This may include documents returned to Government control, destroyed, or held as specified until otherwise directed. Items retuned to the Government shall be hand carried or sent by certified mail to the COR. In addition, data disposition will comply with Fiscal Service policies and procedures.

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 contractor will provide assurance that the application will be available to users 24x7, with the sole exception of scheduled and approved maintenance periods. Maintenance times must be approved by the Fiscal Service.

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?**

Employee and public privacy should not be affected. However, not all of the relevant security controls are directly managed by the bureau. A breach of a third-party's security could compromise the confidentiality of bureau information.

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

Individual contact information (agencies, state and local government, financial institutions and vendors) will be collected in order to better manage the business of the Fiscal Service. This information will only allow individuals to be contacted via work information reported. Monitoring of individuals through this data will not be possible.

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

No information is collected as a function of the monitoring of individuals.

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

The system does not allow the monitoring of individuals.

ACCESS TO DATA:

1) **Who will have access to the data in the system?**
Check all that apply:
X Contractors
X Users
X Managers
X System Administrators
X System Developers
X Others (explain)_____

Financial or Fiscal agents representing Fiscal Service.

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

Data access will be consistent with Fiscal Service security baselines governing the principle of least privilege. Managers will only grant data access to senior executives and individuals whose official duties include performing customer relationship management agency outreach or program management roles. Planned access controls have been identified by user roles and profiles. These rights are identified in the configuration document (dated September 6, 2016)."

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

User access will be limited to their assigned roles following the principle of 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)**

The system provides technical controls to limit access based on user role and user activity is logged. Users of any Fiscal Service system are vetted and trained by the bureau prior to being granted access and are required to take Annual Privacy Awareness Training and Annual Cyber Security Awareness Training.

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. Privacy Act contract clauses are included in all Fiscal Service contracts along with other regulatory measures.

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?**

X_yes
__no

If yes,

a. Check all that apply:

__Federal
__State
__ Local
X Other (explain) Fiscal Service Agents

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

Same as above.

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

Privacy Officers.