IBB

Broadcasting Board of Governors

International Broadcasting Bureau

Momentum Financials System

Privacy Impact Assessment

June 2008

Approval Signatures

System owner / Point of Contact:

_____ _____

Doug M Bennett Date
BBG / CFOA
(202) 203-4622

Reviewer:

_____ _____

Curtis Huyser Date
BBG / Senior Agency Official for Privacy
(202) 382-7382

Abstract

The Broadcasting Board of Governors (BBG) Office of the Chief Financial Officer has procured a COTS application, Momentum, to implement as its financial and procurement system. This privacy impact assessment was conducted because Momentum utilizes personally identifiable information.

Overview

The BBG CFO's office owns the Momentum system. The purpose of the system is to manage BBG's financial and procurement operations. The system contains all budgetary and procurement information needed for BBG to obligate funds and disburse payments to vendors the agency does business with.

Typical Transaction Chain:
An employee or contractor enters a commitment of funds in Momentum. This action can be accomplished by a person given the proper security rights on their system profile to commit and certify funds availability, typically the agency's administrative officers (AOs). The commitment is passed to a contracting officer who will solicit and award the contract. Once the contract is awarded, and invoices are received from the vendor for services rendered, the responsible AO will certify the invoice and send it to the payments office for payment. The payments office will process a payment transaction, which will be scheduled and disbursed in accordance with the prompt payment act.

1.0 Information Collected and Maintained

1.1 What information is collected, used, disseminated, or maintained in the system?

Employee Data: social security number (SSN), last name, first name, home address, bank and routing information.
External Vendor Data: social security number (SSN) or tax identification number (TIN), last name, first name, address, bank and routing information, DUNS number (where applicable).

1.2 What are the sources of the personal information in the system?

Employee Data: Employee data is provided by the employee's respective AO on an Automated Clearing House (ACH) form, which is manually completed by the employee.
Domestic External Vendor Data: Central Contractor Registration (CCR).
Foreign External Vendor Data: Foreign external vendor data is provided by the requisitioning AO on an ACH form, which is manually completed by the vendor.

1.3 Why is the information being collected, used, disseminated, or maintained?

All personal employee and vendor information is collected, used, and maintained in order to disburse payments to the employees and external vendors as part of BBG's standard business practices. Employee salaries are not disbursed from Momentum; however; employee reimbursements for incidentals and travel are.

1.4 How is the information collected?

Employee Data: All employee data is entered in the system, by the payments office, based on a form provided by the employee's AO. Any requested changes to the employee's information follow the same protocol.
Domestic External Vendor Data: All domestic vendor data is pulled from CCR database subject to the CCR guidelines. Momentum interfaces with CCR using the CCR connector, which pulls the most recent vendor information from CCR on a daily basis.
Foreign External Vendor Data: Foreign external vendor data and any domestic vendors not subject to CCR guidelines are input in the system using the same protocol as employee data.

1.5 How will the information be checked for accuracy?

Employee Data: The manual ACH form is filled out by the employee and reviewed by the AO for accuracy. Ultimately the employee is responsible for the accuracy of the data.
Domestic External Vendor Data: All domestic vendor data is pulled from CCR database subject to the CCR guidelines. Momentum interfaces with CCR using the CCR connector, which pulls the most recent vendor information from CCR on a daily basis.
Foreign External Vendor Data: The manual ACH form is filled out by the vendor and reviewed by the AO for accuracy. Ultimately the vendor is responsible for the accuracy of the data.

1.6 What specific legal authorities, arrangements, and /or agreements defined the collection of information?

The following information is provided to comply with the Privacy Act of 1974 (P.L. 93-579). All information collected is required under the provisions of 31 U.S.C. 3322 and 31 CFR 210. This information will be used by the Treasury Department to transmit payment data, by electronic means to a vendor's financial institution.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The privacy risk associated to the type of data collected is the possibility of employee and vendor banking, TIN, and SSN information being available or visible to those in the agency that do not need access to it. Providing access to the system to only those agency employees and contractors who require it in order to complete their job responsibilities has mitigated this risk.

2.0 Uses of the Information

2.1 Describe all the uses of the information.

The personal information is used to send payment information to the Treasury department for disbursement of electronic and check payments.

2.2 What types of tools are used to analyze data and what type of data may be produced?

No tools are used to analyze the data. The data produced from the personal information are the payments sent to the Treasury Department for disbursement.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

The system stores publicly available bank routing information, ensuring that any bank routing number entered for an employee or vendor is indeed a valid routing number.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The bank routing information is only stored on the bank routing number reference table. Access to the bank routing number reference table is limited to those users in M/CON and payables who manage vendor and employee updates and additions.

3.0 Retention

3.1 What information is retained?

All information identified in section 1.1 of this PIA.

3.2 How long is information retained?

The information is retained indefinitely. Once a vendor or employee record is utilized on a purchasing transaction, that record cannot be deleted from the system. If the vendor is no longer utilized by the agency or the employee leaves the agency, their respective records will be deactivated and no longer kept up-to-date.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

No.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The risk associated to retaining the vendor and employee information indefinitely is simply that the information will be viewable in the system indefinitely; however, limiting access to only those users who must review it in order to complete their job responsibilities mitigates this risk.

4.0 Internal Sharing and Disclosure

4.1 With which internal organization(s) is the information, what information is shared and for what purpose?

The personal information listed in section 1.1 of this PIA is not shared internally with any organization or system.

4.2 How is the information transmitted or disclosed?

N/A

4.3 Privacy Impact Analysis: Considering the extent of the internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

N/A

5.0 External Sharing and Disclosure

5.1 With which external organization(s) is the information shared, what information is shared, and for what purposes?

The personal information listed in section 1.1 of this PIA is transmitted to the Treasury Department for disbursement of payments to vendors and reimbursements to employees. Without this information, the Treasury Department cannot properly complete payment to the vendors or employees.

5.2 Is the sharing of personally identifiable information outside of the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the system is allowed to share the personally identifiable information outside of BBG.

Sharing of the personal information with the Treasury Department, so they may disburse payments to the BBG's vendors and employees on BBG's behalf, is precisely the purpose for collecting and retaining the information in Momentum. The agency is in the process of updating and publishing a SORN to reflect this routine use.

5.3 How is the information shared outside the agency and what security measures safeguard its transmission?

The information is transmitted to the Treasury Department across a secured communications circuit which safeguards against unauthorized interception of the transmission.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

The risk of sharing the personal information with the Treasury Department is that the information will be intercepted during transmission. Transmitting over a secured communications circuit mitigates this risk.

6.0 Notice

6.1 Was notice provided to the individual prior to collection of information?

Yes, employees and non-CCR vendors provided the information directly to the AOs in order to begin work at the agency. CCR vendors provided the information when they registered at ccr.gov and are required to maintain the accuracy of the information retained in that database.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

No, without the collection of this information, payments cannot be disbursed to the vendors and employees.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No, there is only one use for the information, and without that use, the vendor or employee cannot provide services to, or be employed by, the agency.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals begin unaware of the collection are mitigated.

It is not possible for vendors or employees to be unaware of the collection of this information. They purposely provide the information for this usage.

7.0 Access, Redress and Correction

7.1 What are the procedures that allow individuals to gain access to their information?

There are none. Individuals will not be able to gain access to their information unless they are authorized to view all personal information retained in Momentum.

7.2 What are the procedures for correct inaccurate or erroneous information?

Employee Data: All employee data entered in the system is based on a completed by the employee and provided to the employee's AO for data entry by the payables office. Any requested changes to the employee's information follow the same protocol.
Domestic External Vendor Data: All domestic vendor data is pulled from the CCR database. The accuracy of the information in the database is the sole responsibility of the vendor.
Foreign External Vendor Data: Foreign external vendor data and any domestic vendors not subject to CCR guidelines are updated in the system using the same protocol as employee data

7.4 If no formal redress is provided, what alternatives are available to the individual?

N/A

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

There are no privacy risks associated to the redress. Initiation of updates or corrections begins with the vendor or employee. Updates or corrections cannot be initiated without their knowledge.

8.0 Technical Access and Security

8.1 What procedures are in place to determine which users may access the system?

All users must complete a Momentum access form, have their security access certified as appropriate by their manager, then approved by the Director of Financial Operations, and finally sent to the host and owner of the system, the Department of Interior's National Business Center (NBC) for final review, approval, and setup.

8.2 Will agency contractors have access to the system?

Yes, various contractors throughout the agency have responsibilities that require them to access the system.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the system?

All agency employees annually receive privacy awareness training. In addition, every user must sign an access form agreeing to proper uses of the system and rules of behavior.

8.4 Has Certification & Accreditation been completed for the system?

Yes, the Certification & Accreditation (C&A) was completed by the host agency for Momentum, NBC. The C&A was signed on May 30, 2008.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

Providing access to the system to only those agency employees and contractors who require it in order to complete their job responsibilities provides the most optimal level of prevention of misuse possible, without overly restricting the system in a manner and preventing the functionality for which it was designed.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

The privacy risk associated to the type of data collected is the possibility of employee and vendor banking, TIN, and SSN information being available or visible to those in the agency that do not need access to it. Providing access to the system to only those agency employees and contractors who require it in order to complete their job responsibilities has mitigated this risk.

9.0 Technology

9.1 What type of project is the system?

The Momentum system is a COTS financial and procurement application, which is certified by the Joint Financial Management Improvement Program (JFMIP). The BBG will utilize the system to conduct all of its budgetary, procurement, payments, and financial reporting responsibilities.

9.2 What stage of development is the system in?

The Momentum software is COTS software and is in a maintenance stage. The Momentum system at BBG is in a deployment stage.

9.3 Does the project employ technology, which may raise privacy concerns? If so, please discuss their implementation.

The project does not employ technology that raises privacy concerns. As stated in sections 9.1 and 9.2, the project utilizes a JFMIP certified system and has a signed C&A from the owner of the system.