Privacy Impact Assessment for the

Consolidated Information Business System (CBIS)

April 18, 2017

Dennis Coleman
Chief Financial Officer
Office of Personnel Management

Reviewing Official
Kellie Cosgrove Riley
Chief Privacy Officer
Office of Personnel Management

Abstract

The United States Office of Personnel Management's (OPM) Consolidated Business Information System (CBIS) is a multi-tier, distributed, financial management system supporting dynamic interoperability with other federal systems. CBIS provides financial and procurement management functions for OPM and is designated as the core financial management system for Salaries and Expenses and Revolving Fund business processes. CBIS is used to create and maintain records of each commitment, obligation, expenses, travel reimbursement, and accounts receivables issued and managed by the agency. This Privacy Impact Assessment is being conducted because CBIS contains personally identifiable information (PII) about OPM employees, vendors, and customers that engage in OPM business operations.

Overview

CBIS is the OPM core financial management system supporting all financial functions for OPM's Salaries and Expense and Revolving Fund business operations. It provides agency compliance with Federal proprietary and budgetary accounting and financial reporting requirements and is a comprehensive source of financial, budget, and performance information to OPM program offices. CBIS records purchasing, accounts receivable, accounts payable, disbursements, and other budget activities that are integrated so the transactions, when processed, can update budgets, financial plans, and the general ledger. CBIS also performs revolving funds billing and collection, project costing, and funds control and offers the functions needed to consolidate financial reports and controls. Some PII is required within CBIS to support its primary business functions of recording and processing financial accounting records for collection and payment of financial obligations made on behalf of OPM.

OPM uses a combination of cross-servicing, federal shared service providers, and other providers to perform key financial management functions and administer systems and operations (i.e. IT hosting, helpdesk, database administration, etc.). Systems at these entities may be OPM owned or OPM used. CBIS includes two Commercial-Off-the-Shelf products that support OPM's core financial management operations. These are Oracle's Enterprise Business Suite (EBS) for Federal Financials and CompuSearch PRISM.

EBS is a web-based Enterprise Resource Planning (ERP) system used by OPM to manage its core financial business processes for Salaries and Expense and Revolving Funds business operations on a single integrated information architecture. The Oracle EBS modules used by OPM and their purpose are described below:

- *Accounts Payable:* Tracks all information needed to properly record the expenditure and liquidation of agency funds.
- *Accounts Receivable:* Records, monitors, and controls all activities in the client's billing and collection process.
- *Automated Disbursements:* Allows OPM to disburse funds through the United States Treasury.
- *Budget Execution:* Automates the budget execution process by recording numerous budgetary control levels and validates budgetary financial activity.

- *Cost Allocation:* Provides the capability to distribute costs or revenues for accounting or reporting purposes based on client defined criteria (e.g. this is specific to payroll).
- *General Ledger:* Provides all the necessary financial postings for all transactions across all subsystems, and provides a complete audit trail of transactions processed in CBIS.
- *Project Cost Accounting:* Allows the client to track project costs incurred, record reimbursable agreements, and distribute project costs to the agreements which are funding the projects, bill customers based upon terms of agreement, and track billing and collection activity against agreements and projects.
- *Purchasing:* Supports the procurement process by tracking a purchase's financial and descriptive information from pre-commitment to funds to a vendor invoice.
- *Fixed Assets:* Allows the client to track capitalized and accountable property from acquisition to disposal, including asset depreciation.
- *Travel Accounting:* Allows the client to track and account for travel obligation (based on travel orders) and vouchers (i.e. expenditures).

CompuSearch PRISM is a web-based application that supports the acquisition management lifecycle, from requisitioning through source selection, award, post award management, and closeout. The PRISM components used by OPM are:

- Contract Solicitations
- Contract Awards
- Delivery/Task Orders
- Multiple Award Schedules (i.e. IDIQ's)
- Blanket Purchase Agreement (BPA) and BPA Calls
- Interagency Agreements
- Contract Modifications
- Receiving/Inspection/Acceptance
- Contract Closeout

1.1 CBIS Business Processes

OPM uses CBIS to execute three financial business processes: Procure to Pay, Order to Cash, and Plan to Report. The Procure to Pay Process is the end-to-end process that begins with the requisition, includes contracting/purchase of goods and services, and ends with payment for those goods and services. This area includes activities associated with contracting, invoicing, disbursements, and vendor management, and includes disbursements for payroll and travel/expense reimbursements. Data generated from the this business process include contract award data, requisition data, purchase order data, invoice data, credit card data, disbursement/payment data, travel reimbursement data, payroll data, workflow data, and vendor data.

The Order to Cash Process is the end-to-end process that addresses activities from initial order receipt and credit authorization, to revenue recognition, receivables and collections. This area includes activities associated with reimbursable agreements, billing, collections, adjustments, customer management, and receivable management. Data generated from the this business process include reimbursable agreement data, billing and collections data, customer data, project management data, project contract data, project cost data, and case data for the National Background Investigations Bureau.

The Plan to Report Process is the end-to-end process that begins with planning the budget, includes recording financial activity to the general ledger and execution of operating plans, and ends with create accounting, management and performance reports. This area includes activities associated with planning and executing budgets, validating and reconciling accounts, closing the books on a monthly and yearly basis, and creating financial reports. Data generated from the this business process include, budget data, general ledger accounting data, cost allocation data, month-end close data, year-end close data, and reporting data.

1.2 CBIS Interfaces

CBIS supports varied interfaces with external and internal systems to obtain its financial data and information. These interfaces use batch-file transfer technology that is machine based in its authentication and authorization mechanism as well as technology that masks sensitive information and ensures that it is communicated securely.

CBIS interfaces with one internal OPM system, the National Background Investigation Bureau's (NBIB) Personnel Investigation Processing System (PIPS). Through this interface, CBIS obtains background investigation case financial data for payment, billing and collections, and revenue generation.

In addition, CBIS interfaces with six systems that are external to OPM. The Department of Treasury's Intergovernmental Payment and Collection (IPAC) System provides an automated, standardized, interagency funds expenditure transfer mechanism for Federal agencies on a daily basis. It facilitates intra-governmental federal e-commerce by transferring funds, with related descriptive data between OPM and other federal agencies. CBIS also has interfaces daily with Treasury's Secure Payment System (SPS) to generate payment schedules (i.e. requests) for the payment on the delivery of goods and services to vendors and travel reimbursement to Federal employees.

CBIS also interfaces with two General Service Administration (GSA) systems. GSA's Electronic Time and Attendance Management System (ETAMS) provides OPM with labor cost data by pay cycle based on information recorded by OPM time keepers in ETAMS. The ETAMS data from this file is used to record direct labor costs for projects defined in CBIS. GSA's System for Award Management (SAM) is a government-wide portal that OPM uses to obtain primary vendor (supplier) data to support OPM's contract acquisition and internal agreement processes.

The remaining two external systems with which CBIS interfaces are the Carlson Wagonlit Sato Travel (CWST) E2 Solutions System, an electronic travel system that includes travel authorizations, travel vouchers, and miscellaneous reimbursements (includes local travel) that it converts into CBIS format for obligations and expenditure invoices; and the JP Morgan Chase (JPMC) Credit Card system, from which CBIS obtains credit card and payment information.

Section 2.0 Authorities and Other Requirements

2.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

Several statutes and other authorities support the collection of the information contained in CBIS. These include 31 U.S.C., Subtitle II, which defines the budget process and describes the method for establishing and accounting for an agency's Federal budget, and 31 U.S.C., Subtitle III, which describes the Federal financial management requirements and responsibilities to record accounting activities related to debt, deposits, collections, payments, and claims and to ensure effective control over, and accountability for, assets for which the agency is responsible.

Several other federal financial mandates and legal authorities that govern financial management systems support the collection of the information in CBIS. These include The Chief Financial Officers Act of 1990, Public Law 101-576, and the Federal Financial Management Improvement Act (FFMIA) of 1996, Public Law 104-208, as well as guidance issued by the Office of Management and Budget: OMB Circular A-123 Management's Responsibility for Internal Control; OMB Memorandum 16-11, Improving Administrative Functions Through Shared Services (May 2016); and OMB Memorandum 13-08, Improving Financial Systems Through Shared Services.

2.2 What Privacy Act System of Records Notice(s) (SORN(s)) applies to the information?

OPM/Internal 5: Pay, Leave, and Travel Records. (http://www.ofr.gov/Privacy/2011/opm.aspx).

2.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes, CBIS has an Information System Security Plan (SSP) which was last updated in July, 2016. A full Security Assessment and Authorization review of CBIS was conducted to ensure the proper security controls and protocols were in place. The CBIS application was granted an Authority to Operate (ATO) in September 2016. OPM is currently working with the Department of Transportation's (DOT) Enterprise Service Center (ESC), under an interagency agreement, to migrate CBIS to its infrastructure and platform. A new ATO is required to support the migration and is expected to be completed on April 19, 2017.

2.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes. The records contained in CBIS are covered by the National Archives and Records Administration General Records Schedule 1.1, items 001 (records relating to managing financial activities and reporting; destroy when 3 years old unless longer retention is needs for business use), 010 (financial transaction records related to procuring goods and services; destroy 6 years after final payment or cancellation unless longer retention is required for business use), 012 (bids and proposals neither solicited nor accepted; destroy when no longer needed for business use), 013 (data submitted to the Federal

Procurement Data System; destroy when 6 years old unless longer retention is required for business use), 020 (records supporting agency financial statements and related audits, and records of other reports; destroy when 3 years old unless longer retention is required for business use), 040 (records of cost accounting for stores, inventory, and materials; destroy when 3 years old unless longer retention is required for business use) , 070 (vendor and bidder information re disbarment for violation of Drug Free Workplace Act; destroy 5 years after removal from approved status unless longer retention is required for business use), and 071 (vendor and bidder information re other disbarment; destroy 3 years after removal from approved status unless longer retention is required for business use).

2.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Information contained in CBIS that pertains to OPM employees and vendors is not subject to the requirements of the Paperwork Reduction Act (PRA) because the information is not collected directly from the public. CBIS collects information from Federal agency financial management systems that represent federal and commercial companies, some of which are covered by the PRA.

Section 3.0 Characterization of the Information

3.1 Identify the information the project collects, uses, disseminates, or maintains.

CBIS collects, uses, disseminates, and maintains information about OPM employees, vendors, customers, and members of the public. Specifically, the CBIS application contains the following information:

- **Vendor Data:** This is limited to vendor or contractors conducting business with OPM and includes company name, point of contact, mailing address, remittance address, telephone number, contract/award number, email address, tax identification number (TIN) [which could be a SSN in the case of sole proprietors set up as individuals], and DUNS number.
- **Employee Data:** This is limited to OPM employees and includes employee name, employee 'E' Number (used for travel reimbursement identification), and bank account information.
- **Customer Data:** This is limited to Federal agencies and entities with which OPM has an interagency agreement and includes customer name, treasury account symbol, agency location code, and trading partner.
- **Financial and other Banking Data:** This includes bank routing transit number, bank account number, and credit card number for all OPM purchase card, travel card, and fleet card holders.

CBIS also supports external and internal financial reporting requirements (i.e. for tax and unpaid debt collection purposes). Both routinely and on an *ad hoc* basis, CBIS is used to generate standard financial reports such as for status of funds, open obligations and commitments, aged receivables, vendor payments, and status of a specific financial transaction.

3.2 What are the sources of the information and how is the information collected for the project?

The information maintained in CBIS is primarily received from other systems via direct, automated system interfaces. As noted in the Overview, CBIS interfaces with one internal OPM system and six external systems.

The National Background Investigation Bureau's (NBIB) Personnel Investigation Processing System (PIPS) interfaces background investigation case financial data for payment, billing and collections, and revenue generation. On a daily basis, CBIS receives new customer billing invoices and adjustments for closed investigation cases for Federal agencies utilizing OPM's investigative services. The interface also generates, on daily basis, invoice data for the NBIB background investigation vendors for payment purposes.

The Department of Treasury's Financial Management Systems, the Intergovernmental Payment and Collection (IPAC) System and the Secure Payment System (SPS), are other sources of data that are interfaced into CBIS. IPAC provides a daily batch file containing invoice number, document reference number, agency location code, amounts, and etc. to record payments received from other government agencies for services provided by OPM that are made payable to OPM. OPM generates payment requests to SPS daily and includes payment schedule number, payment date, amount, payee, bank account, and bank routing number for the payment on the delivery of goods and services to vendors and travel reimbursement to Federal employees.

GSA also is a source of data in CBIS for labor reporting and vendor management. GSA's ETAMS provides OPM labor cost data by pay cycle based on information recorded by OPM time keepers. On a bi-weekly basis, CBIS receive a batch file from ETAMS containing new and updated OPM employee pay, time and attendance records. The GSA SAM application provides vendor (supplier) data to support OPM's contract awards and internal agreements business processes.

CWST's E2 Solutions System interfaces travel data from CWST electronic travel system that includes travel authorizations, travel vouchers, and miscellaneous reimbursements (includes local travel) and converts them into CBIS format for obligations and expenditure invoices. On a daily basis, CBIS receives a batch file from E2 containing new and updated travel records for OPM travelers (i.e., OPM employees and invitational speakers) in order to obligate funds for temporary duty and local travel activity as well as pay funds owed to agency employees under approved travel vouchers.

CBIS interfaces daily with JP Morgan Chase (JPMC) payment.net application to receive credit card data on purchases for purchase, fleet, and travel card transactions.

3.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

While CBIS does not integrate publicly available information from commercial sources, it does receive data from commercial sources available to the general public. For example, the SAM portal is used by staff within OPM's acquisition organization to manually search and gather contractor/vendor information. The SAM database is available for the public to search; however, acquisition professionals

have privileged access to SAM in order to gather additional contractor/vendor information in SAM that is not made available to the public (e.g., DUNS number, TIN, or information not made public by the vendor). OPM's acquisition staff also uses SAM to verify the contractor/vendor is in good standing with the Federal Government. The contractor/vendor information is interfaced daily to CBIS to add new or updated vendor information to support OPM contract awards, obligations, and expenditures for contractors/vendors that provide services to OPM. This information is used when generating payments for services rendered and transmitting required information to Treasury for tax purposes (e.g., 1099-INT and 1099-MISC forms).

3.4 Discuss how accuracy of the data is ensured.

CBIS receives data through automated interfaces and using manual entry. The information maintained in CBIS is primarily received from other systems (described in Question 2.2). These source systems generally gather the information directly from agencies, vendors, and other commercial providers, and as such are considered to be accurate. In addition, CBIS has various internal controls and procedures to ensure the data accuracy. For instance, the majority of data in CBIS is received through automated system interfaces; the built in system edits and configuration increases data accuracy by minimizing data entry errors. Before uploading to CBIS, the source data is also automatically evaluated for errors (e.g., file format, duplicate records, incorrect financial data), and if errors are found, CBIS will not accept the record(s) and will generate an error log that must be reviewed and reconciled by a user in consultation with the source system or provider. Once reconciled, the record is re-submitted to CBIS as part of the next automated transmission.

CBIS embeds 'Role Based Access Controls (RBAC)' to ensure end user roles and access levels are established following the separation of roles and duties principle, which inherently creates accuracy checks in the CBIS when processing transactions. These controls also ensure no one user can create and approve a single financial transaction. Transactions are generated by one user and then reviewed and approved by another user. With each layer of review and approval, information in CBIS is checked for accuracy purposes, and errors are returned to the originating user for correction. Furthermore, when making corrections, users validate the information against the source data, which increases the data accuracy. Even CBIS' database security activates an 'always-on' encryption to minimize data loss or theft.

3.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that PII will be unnecessarily collected and maintained in CBIS.

Mitigation: CBIS has mitigated this risk by establishing effective policies to avoid unnecessary collection of PII and to redact PII if it is collected inadvertently. In addition, the PII that is necessary for CBIS to function, as well as any PII that may be collected inadvertently, is masked and transmitted via secure VPN connections so that its exposure is limited

Privacy Risk: There is a risk that the information in CBIS is not accurate.

Mitigation: This risk is mitigated by the detailed procedures CBIS has in place, described in Section 2.4, to ensure that the information is as accurate as possible.

Section 4.0 Uses of the Information

4.1 Describe how and why the project uses the information.

CBIS uses the information identified in Question 2.1 for the following purposes:

- **Payments/Disbursements**
    - **Employees:** CBIS uses employee information such as name, banking information to process employee reimbursement for temporary duty travel and local travel vouchers. When received from the GSA ETAMS, employee personnel information is used to verify and match employee records against payroll files to interface successfully into CBIS.
    - **Vendor/Contractors:** CBIS uses business-related information such as company name, address, TIN/DUNS number, and banking information to generate payment for services rendered. CBIS also use this information, including the TIN, to submit information about the contractor/vendor to the IRS for tax purposes.
- **Contract Awards/Modifications:** CBIS uses business-related information (interfaced from SAM) such as company name, address, DUNS number, point of contact, and contract number to generate contract awards, commitments, and obligations.
- **Billing/Collections:** CBIS uses business-related and financial information for Federal agencies name, address, treasury account symbol, trading partner number, and point of contact to generate obligations, bills i.e. billing invoices), and collections for debts owed to OPM for services provided to customer agencies.
- **Reporting:** CBIS uses the information to generate regulatory, routine and ad hoc reports described in Question 2.1 above. Such reporting also includes sharing any of the aforementioned categories of information with other Federal agencies such as GSA for payroll information and Treasury for tax-related and debt collection purposes as required by law.

There is some data and information identified in Question 2.1 used for public purposes. CBIS uses information from the PRISM to generate information on contracts awarded to contractors/vendors (with a value of $3,000 or more) to the Federal Procurement Data System - Next Generation (FPDS-NG) which is a requirement under the Federal Funding Accountability and Transparency Act (FFATA) of 2006.

4.2 Does the project use tools, programs, or other technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how OPM plans to use such results.

CBIS end-users have the ability to query and analyze information within the financial system. A variety of standard financial reports are available to monitor and detect differences or anomalies.

4.3 Are there other programs/offices with assigned roles and responsibilities within the system?

Yes. All OPM program offices that use CBIS have access to the discrete functionality that supports their organization with assigned user roles and responsibilities (described below in Question 8.3). There are approximately 550 CBIS end-users across all Program Offices within OPM.

4.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk of misuse of the information through unauthorized access to the information and a related risk that information within CBIS may be used in a manner that is inconsistent with the purpose for which it is being collected and maintained in CBIS. For example, authorized users of CBIS could utilize their access for unapproved or inappropriate purposes, such as performing searches on themselves, friends, relatives, or neighbors.

Mitigation: This risk is mitigated through the use of Role Based Access Controls (RBAC) comprised of user provisioning, permissions management, and access controls. More specifically, user access is also mapped to organizational duties performed to ensure that users are only processing data specific to their specific authorized functions. The access roles are pre-designated by the individuals' position, which ensures users are only granted access to information necessary to perform their official duties. CBIS has functionality built to track and identify what has been accessed by an individual end user using the RBAC. A fundamental element of these controls is the segregation of certain key roles and duties. The basic idea underlying segregation of duties is that no end user or group should be in a position both to perpetrate and to conceal errors or fraud in the normal course of their duties. In general, the principal incompatible duties to be segregated include:

- Custody of assets
- Authorization or approval of related transactions affecting those assets
- Recording or reporting of related transactions
- Execution of the transaction or transaction activity

Additionally, all users receive training regarding the proper use of CBIS and rules of behavior prior to being granted access to the system. All OPM employees (thereby, CBIS end-users) complete annual mandatory security and privacy awareness training, which stresses the importance of appropriate and authorized use of personal data in agency systems.

Privacy Risk: There is a risk that the PII in CBIS will be inappropriately exposed in the system, leading to unauthorized use.

Mitigation: This risk is mitigated by the proper implementation of security controls. CBIS has been identified as 'moderate' impact baseline to ensure the confidentiality, integrity, and availability of the system, its resources, and data. The CFO conducts semi-annual reviews of system users and their access to ensure all user access is in alignment with NIST Access Control (AC) and Audit and Accountability (AU) controls.

Section 5.0 Notice

5.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

CBIS does not generally collect information directly from individuals. Rather, it compiles information from several other sources that may collect information directly from individuals. Those systems that collect information directly from individuals are responsible for providing notice at the time of collection. CBIS does not provide notice directly to individuals to inform them of the collection, maintenance, and us of their information but notice is provided through this PIA and the SORN identified in Question 2.1.

5.2 What opportunities are available for individuals to consent to all uses, decline to provide information, consent to particular uses of the information, or opt out of the project?

Since information in CBIS is primarily received from other sources, individuals do not have the option to consent to particular uses of their information once transmitted to CBIS. Once collected, their information is used for the purposes described in response to Question 3.1 of this PIA. If consent is required, notification of use of PII was previously established in external/interface source system and distributed the individual.

5.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals are not aware that CBIS collects and uses their information.

Mitigation: This PIA provides notice that CBIS uses and shares data with internal and external source systems. Notice is also provided that individual information may be shared outside of OPM through the Routine Use sections of the applicable SORN.

Section 6.0 Data Retention by the project

6.1 Explain how long and for what reason the information is retained.

Under the National Archives and Records Administration General Records Schedule 1.1 and the item numbers set forth in Section 1.4, the information in CBIS is maintained for 7 years. Retention of the information for this amount of time is necessary in order to apply any additional expenditures, make adjustments to payments (i.e., for over bills) and account balances, and for auditing purposes.

6.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk of retaining information longer than is necessary.

Mitigation: This risk is mitigated by carefully considering the business need to retain the information and retaining it only for that period of time. Accordingly, OPM has determined that it has a business need to retain the information in CBIS for 7 years, which is permitted under the applicable retention schedule.

Section 7.0 Information Sharing

7.1 Is information shared outside of OPM as part of normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Yes. OPM shares information maintained in CBIS outside of OPM with the Department of Treasury, the General Services Administration, and Financial Institutions.

CBIS shares information with the Department of Treasury Financial Management Service (FMS) to facilitate payment disbursements to contractors/vendor, employees, and other Federal customers. Information shared with FMS is transmitted electronically via a direct upload to Treasury's SPS system. Transmission of data to Treasury via SPS is protected using public key infrastructure (PKI) encryption. The information includes the payee's name, address, TIN (when applicable), and bank account information, and is shared at the time the disbursements are submitted to Treasury for execution. Treasury uses the information provided to issue federal payments on behalf of OPM in the form of a paper check or EFT transaction. An Interconnection Security Agreement (ISA) and Memorandum of Understanding (MOU) allow OPM to conduct data exchanges in support of these financial management transactions (i.e. collections, obligations, etc.).

As required on an annual basis, OPM shares financial information maintained in CBIS with the Internal Revenue Service (IRS) to report payments issued to vendors/contractors for services rendered to OPM. This includes interest payments distributed to obligors (IRS Form 1099). This information includes vendor or individual's name, address, TIN (when applicable), and amounts paid and withheld. This information is shared with the IRS to support the federal income tax processing and in accordance with the Internal Revenue Code and IRS regulations.

OPM also shares information on debts with Treasury pursuant to the Debt Collection Improvement Act of 1996. The information shared could relate to all categories of individuals for whom financial transactions are processed as well as all categories of information maintained in CBIS. The information shared could or does include name, vendor or individual's name, address, TIN (when applicable), and debt amount (e.g., unpaid amount, overpayment amount). OPM accounting staff prepares data files that are sent electronically to Treasury via an encrypted transmission to the Treasury Cross-Servicing Program and/or Treasury Offset Program for appropriate handling/processing including sending out debt collection letters, establishing repayment agreements, withholding wages, and other debt collection activities.

CBIS has external connections with GSA systems to collect business-related data for vendors who provide goods and services to the Federal government. Data collected for this purpose company name, point of contact, mailing address, remittance address, telephone number, contract/award number,

email address, tax identification number (TIN) [which could be a SSN in the case of sole proprietors set up as individuals], and DUNS number.

CBIS also share bank account and routing information with external financial institution for merchant card processing, and other credit card processes and payments.

7.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The sharing described above is compatible with the original purpose for which the information was collected, namely to perform financial management functions within CBIS to support OPM business operations. All external sharing falls within the scope of published routine uses defined in the OPM/Internal 5 SORN identified in response to Question 1.2.

7.3 Does the project place limitations on re-dissemination?

Yes, re-dissemination of CBIS information is subject to the terms in stated and signed contracts and interagency agreements.

7.4 Describe how the project maintains a record of any disclosures outside of OPM.

Records of information disclosed outside of OPM are maintained through interface logs (i.e. batch files, etc.) upon integration with sources noted under the response to Question 2.2. For example, OPM uses the payment schedule dates from when batch payment files are transmitted to Treasury to track disclosures of CBIS data (including PII) outside of OPM. By recording the payment schedule date from the batch file, CBIS records the disclosure of the associated records and data.

7.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information from CBIS may be inappropriately disclosed outside of OPM.

Mitigation: This risk is mitigated by the fact that information maintained in CBIS is shared in a manner consistent with the routine uses prescribed in the SORN identified in Question 1.2 or as required by law.

Privacy Risk: There is a risk that information, once shared appropriately, will be further shared or used in a manner that is inconsistent with the original purpose for which it was collected and/or shared.

Mitigation: This risk is mitigated by ensuring that the sharing is subject to written agreements that define the purposes for which the information is shared, prohibits additional uses, and appropriately limits any onward sharing with third parties.

Privacy Risk: There is a risk of data and reports being leaked, misused, lost, or further disseminated by the receiving agencies with which CBIS shares information.

Mitigation: To mitigate this risk, data interfaced into and from CBIS is transmitted via secure Virtual Private Network (VPN) connections that use NIST FIPS 140-2 validated cryptography over shared public networks, including the Internet.

Section 8.0 Redress

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

Individuals do not have direct access to CBIS. However, they may request access to records about themselves by following the procedures outlined in the OPM/Internal 5 SORN identified in Question 2.1.

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals who access their records may request correction of any inaccurate or erroneous information by submitting a request to correct the data via the procedures outlined in the OPM/Internal 5 SORN identified in Question 1.2.

8.3 How does the project notify individuals about the procedures for correcting their information?

The procedures for submitting a request to correct information are outlined in the OPM/Internal 5 SORN identified in Question 1.2.

8.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not be able to access information about them that is contained in CBIS nor be afforded adequate opportunity to correct that information.

Mitigation: To mitigate these risks, individuals are afforded opportunity to request amendment of their records by submitting a Privacy Act request by following the procedures outlined in the OPM/Internal 5 SORN.

Section 9.0 Auditing and Accountability

9.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

CBIS uses auditing to capture information associated with any viewing, creating, updating, or deleting of records in the dataset and the user that performed the activity at the database level. CBIS audit trails provide adequate information to facilitate an understanding of transactional events if compromise or

malfunction occurs. The audit trail discloses actions such as unauthorized access, modification, and destruction of data.

CBIS information is also safeguarded in accordance with applicable rules and policies, including all applicable OPM systems security and privacy policies. Controls have been imposed to minimize the risk of compromising the information being stored. Additionally, information is securely shared via encrypted system connections.

Additionally, the TINs and DUNs maintained in CBIS for OPM vendors are visible only to those authorized users with a need to know based on their user access and prescribed official duties.

9.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All OPM employees and contractors complete annual mandatory Security and Privacy Awareness Training. In addition, end-users are required to complete applicable CBIS content training specific to work responsibilities before CBIS access is granted. Awareness and training activities educate users on the appropriate use, protection, and security of information, individual user responsibilities, and ongoing maintenance necessary to protect information systems and data.

9.3 What procedures are in place to determine which users may access the information and how does the project determined who has access?

Each user account is assigned specific roles with a defined set of privileges to ensure overall system integrity. CBIS system administrators can elect to assign all the privileges for a given role or can select only certain privileges to assign. Access is limited to OPM employees who have a need to access the system based on their roles in support of financial administration and management operations at OPM. To gain access to CBIS, users must complete the system-specific user training and submit a request for system access to the authorized point of contact (the OPM Resource Management Officer – RMO) in their program office. The roles and privileges assigned to a particular user are predetermined depending on the user's function. The user roles defined below are similar across all CBIS instances, including:

CBIS Role	OPM Role
General Ledger Super User	Accountant, Chief Accountant
General Ledger User	Accounting Technician
General Ledger Inquiry and Reporting	Accountant, Accounting Technician, RMO, Budget Officer,
Federal Administrator	Budget Officer
Federal Administrator User	Budget Analyst
OBIEE Super User	CBIS End Users
OBIEE End User	CBIS End Users
OBIEE Admin	System Administrator
OBIEE Developer	System Developers
Payables Manager	Accounts Payables Management
Payables Inquiry and Reporting	CBIS End Users
Payables Payments Entry	CFO Certifier

CBIS Role	OPM Role
Payables Supplier Management	Master Data Administrator
Payments Manager	CFO Certifier, Accounts Payables Management
Purchasing Manager	Buyer, Contracting Officer
Purchasing Inquiry and Reporting	CBIS End Users
Purchasing Buyer	Buyer, Contracting Officer
iProcurement	Buyer, Contracting Officer, RMO, Requester
Contracting Manager	Contracting Officer
Project Billing	Billing Technician
Project Costing	Cost Analyst
Project Inquiry and Reporting	CBIS End Users
Receivables Manager	Accounts Receivable Manager
Receivables Inquiry and Reporting	CBIS End Users

9.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within OPM and outside?

CBIS program managers will coordinate with the Chief Privacy Officer (CPO) to review and assess new uses of information consistent with OPM established procedures. In addition, the CPO will work with CBIS program managers and counsel to review the OPM/Internal 5 SORN and determine whether updates are necessary.

Additionally, CBIS program managers, the CPO, and CIO will review information sharing agreements, including interconnection service agreements (ISA) and Memoranda of Understanding (MOUs), to ensure that appropriate privacy and security provisions are included to safeguard PII.

9.5 If applicable, how and why will agency contractors have access to the project? Describe how frequently contracts are reviewed and by whom. Describe the necessity of the access provided to contractors and if special conditions or training is required.

Contractors serve as system integrators to develop and maintain the financial systems at OPM. CBIS follows the following process when allowing contractors access into CBIS:

- Contract has been established with OPM
- Contractors must be successfully adjudicated from a background investigation.
- Complete Security and Privacy Awareness training
- Follow security administration processes and procedures for system access

Contractor access is based on the length of the contract and on the work the contractor is legally obligated to perform in support of CBIS and OPM. Chief Financial Officer (CFO) security personnel send CBIS user reports to each program office Resource Management Officers (RMOs) bi-annually for review. This review is to ensure all users are still in the same role or organization and that they still require the responsibilities they currently have in CBIS. CFO security will terminate access for any user that has not logged into CBIS in over 120 days from the financial system.

CFO security receives a system generated list of all users that have left OPM each month from HR system administrator and program offices. Financial System and Operations (FSO) Security team will terminate user access from any contractor or OPM employee that no longer requires access.

In addition, the OPM Network Admin team will suspend/remove access from contract personnel when the contract has expired.

Responsible Officials

DENNIS D. COLEMAN
CHIEF FINANCIAL OFFICER
U.S. OFFICE OF PERSONNEL MANAGEMENT

Approval Signature

Signed copy on file with the OPM Chief Privacy Officer

KELLIE COSGROVE RILEY
CHIEF PRIVACY OFFICER
U.S. OFFICE OF PERSONNEL MANAGEMENT