

PRIVACY IMPACT ASSESSMENT

Once the Privacy Impact Assessment is completed and the signature approval page is signed, please submit an electronic copy and hard copy with original signatures of the PIA to the SBA Senior Advisor to the Chief Privacy Officer in the Information Privacy Office of the OCIO.

Name of System/Application: Contract Management System

Program Office: Office of Chief Financial Officer

A. CONTACT INFORMATION

1) Who is the person completing this document?

Bruce Swartz
Information Security and Compliance Analyst
Office of Financial Services, OCFO
Denver Finance Center
712 19th Street
Denver, CO 80259
Bruce.swartz@sba.gov

2) Who is the system owner?

Tong Qin
Deputy Chief Financial Officer
Office of Chief Financial Officer
Small Business Administration,
409 Third Street, SW, 6th Floor
Washington, DC 20416
tong.qin@sba.gov

3) Who is the system manager for this system or application?

Tami Perriello
Director, Office of Financial Systems
Office of Chief Financial Officer
Small Business Administration,
409 Third Street, SW, 6th Floor
Washington, DC 20416
Tami.Perriello@sba.gov

4) Who is the IT Security Manager who reviewed this document?

Ja’Nelle DeVore
Chief Information Security Officer
SBA Office of the CIO
(202) 205-7103
JaNelle.DeVore@sba.gov

5) Who is the Senior Advisor who reviewed this document?

Ethel Matthews
Senior Advisor to the Chief Information Officer
SBA Office of the CIO
202-205-7173
Ethel.Matthewa@sba.gov

6) Who is the Reviewing Official?

Paul Christy
Chief Information Officer
SBA Office of the CIO
202-205-6708
Paul.Christy@sba.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION

1) Does this system contain any information about individuals? If yes, explain.

a. Is the information about individual members of the public?

No

b. Is the information about employees?

Yes

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

CMS replaces a manual process to create, track and archive acquisition documents, including contracts and purchase orders. CMS uses PRISM, a COTS end-to-end contract and grant management solution.

CMS enables SBA to increase productivity through streamlined workflow, improved control, and automated collaboration of the end-to end procurement process. CMS performs end-to-end electronic processing of contracts and grants. It ensures SBA is in conformance with OMB e-Procurement guidance. CMS provides the following functionality:

- Implements End-to-End electronic handling of federal contracts and purchase orders during the entire lifecycle of these documents, including online creation, processing, approval, tracking and archiving;
- Provides functionality and technical standards that are compliant with OMB e-Procurement initiatives;
- Is Compliant with FFSIO (formerly JFMIP);
- Interfaces with FedBizOpps, FPDS-NG, CCR and ORCA;
- Supports RFP and RFI documents in a manner compliant with FAR and Federal regulations;

- Provides standard maintenance updates to FAR database;
- Supports the development and/or processing of requisition documents;
- Supports the development and/or processing of invoice documents;
- Supports the modeling, analysis and implementation of workflow management;
- Provides flexible grants application formatting; and
- Supports the preparation, archiving and retrieval of Standard Form 424

It provides standardization of data and limited visibility into the acquisition and grants issued by the agency.

3) Is the system in the development process?

No

4) How will the technology investment (new or updated) affect existing privacy processes?

CMS will not affect existing privacy processes.

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

- 44 U.S.C. § 3101 (Records Management by Federal Agencies)
- Paperwork Reduction Act of 1995; 44 U.S.C. 3501 (10).
- 44 USC §3504 (FEDERAL INFORMATION POLICY)
- Federal Acquisition Regulation (FAR) subpart 4.8
- The Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Systems." OMB Circular A-130 implements a number of Federal laws relating to information resources ID (for example, the Paperwork Reduction Act, the Clinger-Cohen Act; and the Government Performance and Results Act).

6) Privacy Impact Analysis: What privacy risks were identified and describe how they were mitigated for security and access controls?

CMS has a C&A package that outlines the security and access controls that protect CMS and the data it stores, processes, or transmits and also identifies any residual security risk. There were no additional privacy risks identified.

C. SYSTEM DATA

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

Information is maintained on individuals in CMS who are:

- Select Procurement, Grant, Financial and Management employees who work at SBA, and
- Select employees of organizations doing business with SBA (employees at SBA vendors or grantees)

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?**

SBA employee information in CMS is obtained from the individual or their manager. Information regarding vendor companies and individual employee representatives at these companies is entered in CMS by SBA employees based on CMS privileges or for company information through integration to the GSA sponsored Central Contractor Registration (CCR). The General Services Administration (GSA) sponsors the Central Contractor Registration (CCR)

- b. What Federal agencies are providing data for use in the system?**

The General Services Administration (GSA) sponsors the Central Contractor Registration CCR for vendors who wish to do business with the United States Government. Vendor company information comes from CCR, including employee contacts at vendor organizations. CCR is sponsored by GSA, but technically managed within the Department of Defense (DOD).

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

None

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

None

- e. What information will be collected from the employee and the public?**

SBA will collect/maintain the following information on SBA employees:

- Name (Last, First, and middle initial);
- SBA contact information (Phone, Fax, Address, E-mail);
- Procurement and Grant information used to perform their job (COR Certification and Warrant Levels; and
- System Access and Privilege information (UN, PW, Privileges)

SBA will collect/maintain the following information on vendor companies and/or Grantees
Vendor and grantee information is entered and maintained by SBA personnel.

- Primary Vendor/Grantee information that can include: Name, Address, Web site, Dun and Bradstreet Number, CAGE Number, Tax Identification Number, Company financial information (size, ABA number), Business Type, Socio-Economic information (e.g. Small Business, 8a, etc.);
- Vendor/Grantee records contain a Vendor/Grantee Code, which in the case of some vendors is the Tax Identification Number (TIN) of companies. In some small businesses this TIN may be the Social Security Number (SSN) of the owner. In addition, for some Grantees this number may be a SSN.; and

- Vendor/Grantee Point of Contact (POC) and person authorized to sign that includes: name, company phone number, company email, company fax number. In some small businesses the POC may be the owner, whose SSN is used as the TIN for this company.

3) Accuracy, Timeliness, and Reliability

a. How is data collected from sources other than SBA records verified for accuracy?

Vendor information will be verified against GSA Sponsored CCR through system-to system integration.

b. How is data checked for completeness?

Extensive validation checks are performed by CMS. The data is validated for completeness and compliance with business rules...

4) Privacy Impact Analysis: Discuss what privacy risks were identified and how they were mitigated for the types of information collected?

There is a potential for vendor and grantee records to contain an individual's Social Security Number (SSN), as passed from the Central Contractor Registry (CCR). This occurs because in some small businesses the POC may be the owner, whose SSN is used as the TIN for their company.

The Federal Acquisition Circular (FAC) 2001-16, October 1, 2003, subpart 4.11-Central Contractor Registration amends the Federal Acquisition Regulation (FAR) to require contractor registration in the Central Contractor Registration (CCR) database prior to award of any contract, basic agreement, basic ordering agreement, or blanket purchase agreement on or after October 1, 2003. Providing this information is a condition of doing business with the government.

Mitigation involves limiting access to this data to authorized users and providing this information only to those who need it to perform their job. CMS has an account management procedure to grant access to users and CMS is only accessible from within the SBA network. CMS enforces strong password authentication and has a set of parameters to configure permissions to activity or data once an individual is authenticated to the system.

Additionally, CMS has further mitigated this issue by installing a configuration switch that enables each agency to hide the TIN if they choose. It will not appear anywhere but in the profile that is transferred from CCR. The CMS System Administrators, a privileged user, are the only individuals who can view this in the profile.

D. DATA ATTRIBUTES

1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes. SBA is following Federal Acquisition Regulations (FAR) regarding what information is relevant and necessary.

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?

CMS will derive data regarding an SBA employee's amount of work and provide reports on items such as: number of contracts awarded, number of contracts pending and associate this with a CMS user. No additional individual information will be created or derived.

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

Information regarding an SBA employee's workload will be maintained and associated with their user record for management reports.

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

No

5) How is the new data verified for relevance, timeliness, and accuracy?

Managers, based on privileges, will be able to view reports and compare to historical information.

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

SBA procurement data is consolidated, but not individual employee records. CMS is hosted and managed within HQDSS and the LAN/WAN and only accessible to SBA employees or designates with proper privileges.

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? If process is not consolidated, please state, "N/A".

N/A, Individual data is not consolidated in CMS.

8) How will the data be retrieved? Does a personal identifier retrieve the data?

Records are not maintained on individuals outside of their workload in CMS. Managers, with privileges, can review an individual's workload report using queries based on name or office of assignment.

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 on SBA employees can be the following:

- Workload (for management reports)
- System Log-In (for audit and security purposes)

System Administrators, as designated and granted privileges by the system owner, through the account management process can view these reports. In addition, managers can be provided access to reports on staff they are responsible for. CMS has privileges and an organizational hierarchy that designates what access a manager can see. For instance, the Manager of the Acquisitions Division may see reports for all of SBA and other managers may only see employees at offices under their supervision.

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 authorized uses), and how individuals can grant consent.

Data in CMS is mandated by the Federal Acquisition Regulation (FAR), therefore to do their jobs, employees need to enter certain required information. All employees, when entering the system agree to CMS terms and conditions. This consent/agreement procedure is configurable in CMS to allow SBA to set frequency requirements for when it is accomplished (e.g. each log-in, daily, monthly, and annually, etc.).

11) Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is used as intended.

All employees and contractors receive mandatory computer security awareness training. All contracting officers are trained in their position and additionally are required to complete ethics training with the legal office. In addition, CMS has in place system controls (i.e. access controls, failed login attempts) if an individual is found to be inappropriately using the information.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS

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

All CMS data is housed in one location

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

The FAR requires contract data to be retained for 6 years and 3 months.

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?

CMS has a contract close-out process to delete contact information. Once a contract is closed out, data is maintained for 6 years and 3 months.

Reports are dynamically generated in CMS and not maintained as reports in CMS. Users, with proper privileges, can save reports in PDF, Excel, and Word to their desk-top.

Vendor records are dynamically updated based on integration to CCR.

Procedures for disposing data are documented in the SBA Records Management directives and National Archives records schedules.

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

No

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

N/A

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

CMS cannot locate or monitor a physical location of an individual employee. CMS for auditing purposes will maintain a record of individual log-in to CMS. In addition, CMS will maintain information regarding work-load of a particular SBA employee. A user, with privileges granted, can search for a user within CMS for the purpose of including them in their workflow (e.g. select them to be an approver) or for management reports.

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

A time and date are entered with each log-in to CMS.

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

Access to CMS will be given, based on a SBA employees need to use it for performing their assigned duties.. Each person granted access to the system will be trained and individually authorized to access the system, based on their privileges. All system users are required to follow established internal security protocols.

SBA has countermeasures in place to minimize the chance that a keystroke logger could be installed on a user's desktop machine. First, users do not have administrative rights on their machines. They are therefore limited in what software they can install, whether intentionally or unintentionally. Second, SBA runs spyware detection and elimination software on each user's machine. Keystroke loggers should be removed by this process.

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

SBA Privacy Act System of Record Number is 30

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

N/A

F. DATA ACCESS

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

The system will be accessed by authorized personnel for the creation of contracts and grants for SBA. Primarily, this includes members of the Acquisition Division and Denver Finance Center. In addition, personnel from the Office of the Chief Information Officer, who are responsible for hosting CMS will have access to data in an Oracle database associated with CMS. Contractors also support various components of CMS and are granted access based on clearance through normal SBA personal security and access control processes.**How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**

CMS has an account management procedure that governs user and system administration access. Through this process privileges are determined and granted.

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

No. Users will be restricted to information related to their particular role. Access controls following the principle of least privilege.

3) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please processes and training materials)

All users, when entering the system agree to CMS terms and conditions. This consent/agreement procedure is configurable in CMS to allow SBA to set frequency requirements for when it is accomplished (e.g. each log-in, daily, monthly, and annually, etc.). In addition, all users are trained on CMS.

4) 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?

Yes. A Privacy Act clause is in the contract.

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

Yes. Contract information, including the Contracting Officer Name is sent through an interface from CMS to the GSA sponsored, Federal Procurement Data System Next Generation (FPDSNG).

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

The designated System Manager is responsible

7) How will the shared data be used by the other agency?

GSA consolidates Federal procurement data from FPDS-NG

8) What procedures are in place for assuring proper use of the shared data?

FPDSNG system is open to the public via a website. There is a security and privacy policy statement on the site. It in part *“FPDS web servers employ industry-standard methods to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage. Unauthorized attempts to upload information or change information on FPDS servers are strictly prohibited and may be punishable by law, including the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act. In the specific context of this security monitoring, there is no expectation of privacy.”* There is no privacy data available in FPDSNG. Other wise there is no way to assure proper use of the data once accessed or download by the public.

9) Privacy Impact Analysis: Discuss what privacy risks were identified and how they were mitigated for information shared internal and external.

SBA has a Memorandum of Understanding with GSA to use the Central Contractor Registry to receive vendor and grantee information for the acquisition process. Internally, information is accessed only with a need to know.

Privacy Impact Assessment PIA Approval Page

The Following Officials Have Approved this Document:

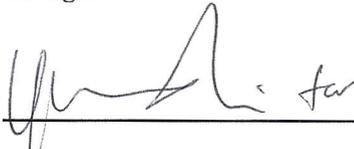
System Owner

 _____ (Signature) 5/25/11 _____ (Date)

Name: Tong Qin

Title: Deputy Chief Financial Officer

System Manager

 _____ (Signature) 5/25/2011 _____ (Date)

Name: Tami Perriello

Title: Director of Financial Systems, OCFO

IT Security Manager

 _____ (Signature) 5/25/11 _____ (Date)

Name: Ja'Nelle DeVore

Title: Chief Information Security Officer

Chief Privacy Officer

 _____ (Signature) 5/25/11 _____ (Date)

Name: Paul Christy

Title: Chief Information Officer/Privacy Officer