
U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

Privacy Impact Assessment



Consolidated Financial System (CFS)

PTOC-001-00

July 2, 2015

Privacy Impact Assessment

This Privacy Impact Assessment (PIA) is a requirement of the Privacy Act of 1987 and OMB Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*. A PIA documents the due diligence and oversight placed upon information associated with the project or system in question. Written from the System Owner's perspective for the American public, the PIA discloses what information is being collected, and how that information is protected. The intent is to build confidence that privacy information is secure, processes that utilize this information comply with Federal requirements, and more importantly, inform the privacy expectations of the American public.

The Privacy Threshold Analysis (PTA) is a separate artifact that must be completed prior to beginning this PIA. In many cases, the PTA will be the only required artifact to satisfy DOC privacy considerations.

SYSTEM DESCRIPTION

The Consolidated Financial System (CFS) is a Major Application (MA) that provides financial management, procurement, and travel management in support of the USPTO mission. CFS communicates with other federal agencies as part of these activities and includes the following two (2) Automated Information Systems:

- **Momentum:** A full-featured Commercial off-the-shelf (COTS) accounting software package that permits full integration of the processing of financial transactions with other normal business processes. Momentum not only provides a solution for financial management, it also enhances usability, efficiency, timeliness, and accuracy of the United States Patent and Trademark Office's (USPTO) financial management transactions through its Graphical User Interface (GUI) that provides an integrated workflow facility including seamless integration with other administrative support systems. Momentum contains a third party product, WebMethods, which is used to integrate the financial system with other external systems such as the GSA/Concur remotely hosted Concur Government Edition (CGE) travel system. System devices are physically located in the Data Center in the Madison East Building. The users of Momentum are USPTO employees and designated contractors in various Business Units.
- **Concur Government Edition Integration (CGE)**

CGE is a web-based travel and planning management solution owned, hosted, maintained and operated by Concur, Inc. In order to support the Federal Government's more broadly defined eTravel 2 (ETS2) program, including funds control, accounting and fiscal management of Agency travel, the USPTO was required to construct an interface between the CGE system and CGI's Momentum Financials. The USPTO has implemented a near real-time integration to CGE using Web Services based on a Service Oriented Architecture (SOA).

The CGE externally hosted application falls within the security boundary of the GSA and is Certified and Accredited by GSA; however the integration piece between CGE and Momentum should be included in the USPTO Security Authorization boundary. The USPTO also has a Memorandum of Understanding (MOU) & Integration Security Agreement (ISA) in place with Concur & GSA. System devices are physically located in the Data Center in the Madison East. CGE users are USPTO employees and contractors.

QUESTIONNAIRE

1. What information is collected (e.g., nature and source)?

The Consolidated Financial System (CFS) comprises the following subsystems: Momentum Financials (USPTO's financial and acquisition system of record), and Concur Government Edition Integration (CGE). A large number of financial, procurement and travel transactions are performed in CFS on a daily basis. Data is entered into CFS in numerous ways. Data is entered directly into Momentum Financials through a graphical user interface, which facilitates the data entry and processing of transactions. Data entered directly into CGE (externally hosted by Concur, Inc) is transmitted to Momentum Financials via COTS interfaces. In addition, payroll data is updated into Momentum Financials from the National Finance Center's transactions; from Revenue Accounting and Management System for revenue transactions; and data is sent to the Department of Treasury for disbursements.

Momentum captures the social security numbers, bank account numbers, credit card numbers, tax identification numbers, phone numbers, and email addresses of the vendors tracked in the system. Social security numbers are tracked for employees of PTO.

CGE does not store any information related to an individual.

Employees:

The CFS components and their uses are listed below:

Momentum Financials: Employees utilize Momentum to process requisitions, procurement and non-procurement obligations, receivers, invoices, payments, billing documents for receivables; to record payroll transactions; for planning and budget execution; to record and depreciate assets; and to disburse payments. Momentum Financials houses the general ledger that is updated as financial transactions are processed. In addition, Momentum Financials has extensive querying capabilities including activities by vendor, general ledger, and budget execution.

CGE: Employees utilize this system to perform travel transactions in support of official travel including travel requests and vouchers.

Other:

There are no other direct users of the CFS. Momentum communicates with the National Finance Center to receive payroll files and with the Department of Treasury to transmit disbursement information. USPTO's Revenue Accounting and Management system transmits financial information to Momentum Financials on a daily basis, and Momentum Financials data populates universes in USPTO's Enterprise Data Warehouse.

2. Why is this information being collected (e.g., to determine eligibility)?

CFS is the USPTO's financial and acquisition system of record and is responsible for processing and maintaining all financial transactions in support of the USPTO mission. Data is collected and maintained in support of this mission.

On the PII level, Momentum captures the social security numbers for employees so that it may be used for payroll. Vendor bank account numbers are stored in Momentum to correctly process EFT payments, other Vendor information is synchronized with the government CCR site.

As for Publicly Releasable PII, business addresses and bank ids are also captured within Momentum. CCRC maintains vendor information in the same way that Momentum does, both through integrations and through data entry.

CGE does not store PII, instead these keep track of a unique momentum ID in place of PII

3. What is the intended use of information (e.g., to verify existing data)?

CFS is the USPTO's financial and acquisition system of record. The use of collected data is to support this role of the CFS.

4. With whom will the information be shared (e.g., another agency for a specified programmatic purpose)?

Data is transmitted to the Department of Treasury for the processing of disbursements. Financial reports are prepared with data from CFS and provided to the various government agencies requesting the reports (i.e., Department of Commerce).

5. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how can individuals grant consent?

Within Momentum, an individual's social security information is collected upon becoming a USPTO employee.

All transactions are financial in-nature and required for the CFS. There is no consent required from individuals.

6. How will the information be secured (e.g., administrative and technological controls)?

Management Controls:

The USPTO utilizes the Life Cycle Management review process to ensure that all management controls are in place for CFS. During the upgrade, maintenance or enhancement of any component of CFS, the security controls are reviewed and reevaluated in the CFS Aggregate System Security Plan. This plan specifically addresses the management, operational, and technical controls that are in place and planned during the upgrade, maintenance or enhancement of the project. The USPTO ensures that all government and contractor staff has a National Agency Check performed.

At the CFS level a Financial Application Security Registration has been implemented and maintained for each user authorized access to any component of CFS, including data entry-level access through system development access. Each USPTO employee and designated on-site contractor support staff who has completed a Financial Application Security Registration form may obtain access to the CFS. Both the employee's supervisor approval and the Momentum Financials Security Administrator's approval are required before access is granted to the

system. The level of access to the system is determined based on the user's job function and office policy. The specific access to the data and level of authority is defined in the Momentum Financials' Security Role table. System users include: program office data entry personnel; Office of Finance and Office of Corporate Planning employees for financial and budget transactions; Office of Procurement staff for procurement transactions; managers throughout USPTO for approval and query purposes; system administrators for system security, assurance, and monitoring purposes; on-site contractor staff for user assistance, development of complex reports, and issue resolution; and database administrators.

Operational Controls:

Operational controls include securing all hardware associated with this system in the USPTO's Data Center. The Data Center is controlled by access card entry and is physically secured by a Guard Service to restrict access to the components. The Infrastructure Disaster Recovery Plan documents the contingency plan for the Data Center. In addition to securing the hardware, there are controls in place for safeguarding the databases and operating systems to include: daily, weekly, monthly back-ups; physical terminal identification; restricted admin accounts; etc.

Technical Controls:

The CFS is secured by the USPTO's infrastructure component and other OCIO established technical controls to include password authentication at the server and database levels

7. How will the data extract log and verify requirement be met?

For Momentum, and CGE, the database extracts are performed by an automated process that is managed by the Oracle DBAs. The logs for these database exports are automatically generated by Oracle and are maintained within the Oracle databases. The database exports are cleaned up using scrub scripts that remove all PII data. Since no PII data is contained in the cleaned up version of the database exports, the verify requirement is not applicable. Data extracts sent to Treasury for disbursement of funds are exempt from the log and verify requirement since this data is required by law and Department of Treasury must retain this information. Momentum and CGE do not support a database extract by end-users

8. Is a system of records being created under the Privacy Act, 5 U.S.C. 552a?

No, records contained in these systems do not constitute a new system of records within the meaning of the Privacy Act. However, the existing Privacy Act System of Records Notices (SORNs) applies to the following systems:

DEPT-1; Attendance, Leave, and Payroll Records of Employees and Certain Other Persons

- PTOC-001-01 Momentum

DEPT--2 Accounts Receivable

- PTOC-001-01 Momentum
- PTOC-001-05 CGE

DEPT--9 Travel Records (Domestic and Foreign) of Employees and Certain Other Persons

- PTOC-001-05 CGE

9. Are these records covered by a record control schedule approved by the National Archives and Records Administration (NARA)?

Yes, both the paper input records and the electronic records are covered by a NARA approved record control schedule according to Section 7 (CFO) of the USPTO Comprehensive Records Schedule (Dec. 2009).

