U.S. Department of Commerce
U.S. Patent and Trademark Office

Privacy Impact Assessment
for the
Consolidated Financial System

Reviewed by: John B. Owens II, Senior Agency Official for Privacy

☐ Concurrence of Senior Agency Official for Privacy
☐ Non-concurrence of Senior Agency Official for Privacy

_____

Signature of Senior Agency Official for Privacy   Date

U.S. Department of Commerce Privacy Impact Assessment
USPTO Consolidated Financial System

Unique Project Identifier: PTOC-001-00

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) a general description of the information in the system
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 three (3) Automated Information Systems:

- **Momentum:** A full-featured Commercial off-the-shelf (COTS) financial management and acquisitions 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). System devices are physically located in the Data Center in the Madison East. CGE users are USPTO employees and contractors.

- **E-Acquisition (ACQ)**

  The eAcquisition Tool (ACQ) is a web-based COTS software. ACQ provides an automated solution for the procure-to-pay process in the acquisition community at the USPTO, allowing procurement users to create acquisition plans and track the life of procurement actions and documents associating with the plan. ACQ integrates with Momentum, the Enterprise Data Warehouse (EDW) and the Electronic Library for Financial Management Systems (EL4FMS).

(b) a description of a typical transaction conducted on the system

Momentum: 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 authorizations and vouchers.

ACQ does not store any information related to an individual.

(c) any information sharing conducted by the system

National Finance Center's transactions payroll data is updated into Momentum Financials; from Revenue Accounting and Management System for revenue transactions; data sent to the Department of Treasury for disbursements; and employee information is imported from Human Resources via the Enterprise Data Warehouse (EDW) for the purpose of making reimbursements consistent with how employees receive their payroll.

CGE receives employee information from a combination of Momentum and EDW for creating and maintaining travelers; and CGE shares both itinerary and credit card information with Momentum.

ACQ does not share any personal information.

(d) a citation of the legal authority to collect PII and/or BII

The USPTO collects customer financial information for fee processing. Under 35 U.S.C, Section 41 and 15 U.S.C. Section 11 13, as implemented in 37 CFR.

(e) the Federal Information Processing Standard (FIPS) 199 security impact category for the system

Moderate

Section 1: Status of the Information System

1.1   Indicate whether the information system is a new or existing system.

☐   This is a new information system.

☐☐   This is an existing information system with changes that create new privacy risks.
        (Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions	☐	d. Significant Merging	☐	g. New Interagency Uses	☐
b. Anonymous to Non-Anonymous	☐	e. New Public Access	☐	h. Internal Flow or Collection	☐
c. Significant System Management Changes	☐	f. Commercial Sources	☐	i. Alteration in Character of Data	☐
j. Other changes that create new privacy risks (specify):					

☒   This is an existing information system in which changes do not create new privacy risks.
       Continue to answer questions, and complete certification.

Section 2: Information in the System

2.1   Indicate what personally identifiable information (PII)/business identifiable information
        (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	☒	e. File/Case ID	☐	i. Credit Card	☒
b. Taxpayer ID	☒	f. Driver's License	☐	j. Financial Account	☒
c. Employer ID	☐	g. Passport	☐	k. Financial Transaction	☒
d. Employee ID	☒	h. Alien Registration	☐	l. Vehicle Identifier	☐
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: Momentum captures the social security numbers for employees so that it may be used for payroll.					
*If SSNs are collected, stored, or processed by the system, please explain if there is a way to avoid such collection in the future and how this could be accomplished:					

General Personal Data (GPD)					
a. Name	☒	g. Date of Birth	☐	m. Religion	☐
b. Maiden Name	☐	h. Place of Birth	☐	n. Financial Information	☒
c. Alias	☐	i. Home Address	☒	o. Medical Information	☐
d. Gender	☐	j. Telephone Number	☒	p. Military Service	☐
e. Age	☐	k. Email Address	☒	q. Physical Characteristics	☐
f. Race/Ethnicity	☐	l. Education	☐	r. Mother's Maiden Name	☐
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	☐	d. Telephone Number	☒	g. Salary	☐
b. Job Title	☐	e. Email Address	☒	h. Work History	☐
c. Work Address	☐	f. Business Associates	☐		
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	☐	d. Photographs	☐	g. DNA Profiles	☐
b. Palm Prints	☐	e. Scars, Marks, Tattoos	☐	h. Retina/Iris Scans	☐
c. Voice Recording/Signatures	☐	f. Vascular Scan	☐	i. Dental Profile	☐
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	☒	c. Date/Time of Access	☒	e. ID Files Accessed	☐
b. IP Address	☐	d. Queries Run	☐	f. Contents of Files	☐
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2　Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	☐	Hard Copy: Mail/Fax	☐	Online	☐
Telephone	☐	Email	☐		
Other (specify):					

Government Sources					
Within the Bureau	☒	Other DOC Bureaus	☐	Other Federal Agencies	☒
State, Local, Tribal	☐	Foreign	☐		
Other (specify):					

Non-government Sources					
Public Organizations	☐	Private Sector	☐	Commercial Data Brokers	☐
Third Party Website or Application			☐		
Other (specify):					

2.3   Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards	☐	Biometrics	☐
Caller-ID	☐	Personal Identity Verification (PIV) Cards	☐
Other (specify):			

☒	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1   Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	☐	Building entry readers	☐
Video surveillance	☐	Electronic purchase transactions	☐
Other (specify):			

☒	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1   Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility	☐	For administering human resources programs	☐
For administrative matters	☐	To promote information sharing initiatives	☐
For litigation	☐	For criminal law enforcement activities	☐
For civil enforcement activities	☐	For intelligence activities	☐
To improve Federal services online	☐	For employee or customer satisfaction	☐
For web measurement and customization technologies (single-session)	☐	For web measurement and customization technologies (multi-session)	☐
Other (specify): "Momentum is USPTO's system of record for all payments and collections. It is also used for generating statements of non-payroll income." CGE stores personally identifiable information for travelers that is necessary to facilitate making their travel arrangements. e-ACQ does not store any information related to an individual.			

Section 5: Use of the Information

5.1   In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

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. PII stored in the system is for a combination of Employees, Contractors, Vendors, Domestic Customers, and International Customers.

Section 6: Information Sharing and Access

6.1   Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	☐	☒	☒
DOC bureaus	☐	☐	☐
Federal agencies	☐	☒	☐
State, local, tribal gov't agencies	☐	☐	☐
Public	☐	☐	☐
Private sector	☒	☐	☐
Foreign governments	☐	☐	☐
Foreign entities	☐	☐	☐
Other (specify):	☐	☐	☐

☐	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

☒	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: • USPTO's Revenue Accounting and Management (RAM) • USPTO's Enterprise Data Warehouse (EDW) • General Services Administration's System for Award Management (SAM) • Department of Agriculture's National Finance Center (NFC) • Department of Treasury's Do Not Pay (DNP) • Department of Treasury's Payment Application Modernization (PAM) • Concur Inc.'s Concur Government Edition (CGE) All data transmissions are encrypted and require credential verification. All data transmissions not done through dedicated lines require security certificates. Inbound transmissions as well as outbound transmissions to government agencies pass through a DMZ before being sent to endpoint servers.
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	☐	Government Employees	☒
Contractors	☒		
Other (specify):			

Section 7: **Notice and Consent**

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

☐	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
☐	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: _____.	
☐	Yes, notice is provided by other means.	Specify how:
☒	No, notice is not provided.	Specify why not: All financial information is required as 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. All employee information for payroll and identifying/assigning

		user accounts described herein is required.

7.2　Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

☐	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: the use of the information is a required use and therefore necessary.

7.3   Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

☐	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: There is no additional use of the information beyond the required use and therefore no "consent process" is necessary.

7.4   Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

☒	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Some vendor information can be changed by logging into the General Services Administration's System for Award Management (SAM). Employees can update some of their information by contacting USPTO's Human Resources.
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Financial system audit requirements mandate that much of this information be maintained about each transaction for a period of 75 months.

Section 8: Administrative and Technological Controls

8.1   Indicate the administrative and technological controls for the system. *(Check all that apply.)*

☒	All users signed a confidentiality agreement or non-disclosure agreement.
☒	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
☒	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
☒	Access to the PII/BII is restricted to authorized personnel only.
☐	Access to the PII/BII is being monitored, tracked, or recorded.
☒	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): _____ ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
☒	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
☒	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☒	Contracts with customers establish ownership rights over data including PII/BII.
☒	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
☐	Other (specify):

8.2   Provide a general description of the technologies used to protect PII/BII on the IT system.

CFS is secured by the USPTO's infrastructure systems and other OCIO established 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

Section 9: Privacy Act

9.1   Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered*

by an existing SORN).

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

☐	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*:
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☒	No, a SORN is not being created. 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

Section 10: Retention of Information

10.1   Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

☒	There is an approved record control schedule. Provide the name of the record control schedule: 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).
☐	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
☒	Yes, retention is monitored for compliance to the schedule.
☐	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2   Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	☐	Overwriting	☐
Degaussing	☐	Deleting	☐
Other (specify): USPTO keeps all Momentum electronic records.			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1   Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

☐	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
☒	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
☐	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

☒	Identifiability	Provide explanation: PII stored in the system is for a combination of Employees, Contractors, Vendors, Domestic Customers, and International Customers.
☒	Quantity of PII	Provide explanation: PII stored in the system is for a combination of Employees, Contractors, Vendors, Domestic Customers, and International Customers.
☒	Data Field Sensitivity	Provide explanation: PII stored in the system is for a combination of Employees, Contractors, Vendors, Domestic Customers, and International Customers.
☒	Context of Use	Provide explanation: PII stored in the system is for a combination of Employees, Contractors, Vendors, Domestic Customers, and International Customers.
☐	Obligation to Protect Confidentiality	Provide explanation:
☐	Access to and Location of PII	Provide explanation:
☐	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

☐	Yes, the conduct of this PIA results in required business process changes. Explanation:
☒	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

☐	Yes, the conduct of this PIA results in required technology changes. Explanation:
☒	No, the conduct of this PIA does not result in any required technology changes.