Version Number: 02-2018

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

Privacy Impact Assessment
for the
Consolidated Financial System

Reviewed by: Henry J. Holcombe, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CATRINA PURVIS Digitally signed by CATRINA PURVIS
Date: 2019.08.15 17:11:08 -04'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

July 26, 2019

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 four (4) subsystems:

Momentum: Momentum is 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. The system empowers the USPTO program offices to tie together many financial accounting functions, including plans, purchasing transactions, fixed assets, travel accounting, accounts receivable, accounts payable, reporting, security and workflow processes, general ledger, external reports, budget, payroll and automated disbursements through an integrated relational database. This AIS collects, stores, processes, and disseminates PII and BII.

Concur Government Edition (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 and Momentum. The CGE application falls within the security boundary of the General Services Administration (GSA) and is authorized to operate by GSA. The USPTO has a Memorandum of Understanding (MOU) and an Interconnection Security Agreement (ISA) in place with GSA for this integration. This AIS collects, stores, and disseminates PII.

eAcquisition Tool (ACQ): ACQ is a web-based COTS solution to support users in the acquisition community at the USPTO. ACQ allows procurement users to create acquisition plans and track the life of procurement actions and documents associating with the plan. ACQ integrates with Momentum, Vendor Portal, Enterprise Data Warehouse (EDW), and the Electronic Library for Financial Management Systems (EL4FMS). This AIS collects, stores, processes, and disseminates BII.

VendorPortal: VendorPortal is a web-based COTS solution to provide a platform for interaction and information exchange between USPTO and the vendor community.

VendorPortal provides the ability to publish notices, solicitations and award announcements; enables vendor offer, invoice and receipt submission, and provides vendors insight into awards, deliverables and invoice statuses. This AIS collects, stores, processes, and disseminates BII.

(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: Employees utilize this system to create acquisition plans to initiate the process to create a purchasing request for goods and services at the USPTO. Initial acquisition data will be created in ACQ and transfer to Momentum to create the associated draft requisitions, solicitations and awards via web service.

VendorPortal: External vendors utilize this system to follow and submit offers to posted opportunities. Verified vendors with an award with USPTO utilizes the system to manage the submission of invoices and eDeliverables.

(c) any information sharing conducted by the system

Momentum: Momentum processes payment activities and sends files to the Department of Treasury for disbursements. Momentum receives payroll data from the Department of Agriculture National Finance Center. A component of Momentum allows for integration with the General Services Administration (GSA) System for Award Management (SAM) database. The integration allows for scheduled updates from SAM to be updated in the Central Contractor Registration Connector before ultimately updating the Momentum vendor table. In addition, Momentum receives data from the USPTO Revenue Accounting and Management System (RAM) via the Fee Processing Next Generation (FPNG).

CGE: CGE receives employee information from USPTO internal systems (Momentum and Enterprise Data Warehouse) for creating and maintaining travelers; and CGE shares both itinerary and credit card information with Momentum.

ACQ: ACQ shares acquisition documents with the Electronic Library for Financial Management Systems (EL4FMS) and procurement data with the Momentum and the Enterprise Data Warehouse (EDW).

VendorPortal: VendorPortal shares information and documents related to the submission of offers, invoices and eDeliverables with ACQ.

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

The legal authority to collect PII and/or BII derives from

- 5 U.S.C. 301; 31 U.S.C. 3512, 3322; 44 U.S.C. 3101, 3309
- 5 U.S.C. 5701-09, 31 U.S.C. 3711, 31 CFR Part 901, Treasury Financial Manual
- Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; and Federal Claim Collection Act of 1966
- 35 U.S.C. 2 and 41 and 15 U.S.C. 1113

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

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):					

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. VendorPortal and ACQ capture DUNS number for vendor records.

*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:

There is no way to avoid such collection because SSNs and Taxpayer IDs are required to disperse payments.

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):			

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, and vendors.

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 Systems:
	• Consolidated Financial System (CFS)
	  o Momentum
	  o ACQ
	  o VendorPortal
	• Information Delivery Product (IDP)
	  o Enterprise Data Warehouse (EDW)
	  o Electronic Library for Financial Management Systems (EL4FMS)
	• Fee Processing Next Generation (FPNG)
	• Revenue Accounting and Management (RAM)
	
	External Systems:
	• General Services Administration Concur Government Edition (CGE)
	• General Services Administration System for Award Management (SAM)
	• Department of Agriculture National Finance Center (NFC)
	• Department of Treasury Do Not Pay (DNP)
	• Department of Treasury Payment Application Modernization (PAM)
	
	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. SSNs and Taxpayer IDs are encrypted while at rest.

☐	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: CFS receives PII/BII indirectly from other application systems (i.e. front end systems). Individuals may be notified that their PII/BII is collected, maintained, or disseminated by the primary application ingress system. In addition, CGE provides a privacy act notice on its website: https://cge.concursolutions.com/
☐	No, notice is not provided.	Specify why not:

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: CFS receives PII/BII indirectly from other application systems (i.e. front end systems). These front end systems provide this functionality for the data that is being collected. CFS has no authorization to decline any type of information since it's owned by the primary application.

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: CFS receives PII/BII indirectly from other application systems (i.e. front end systems). These front end systems provide this functionality for the data that is being collected.

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:
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: CFS receives PII/BII indirectly from other application systems (i.e. front end systems). These front end systems provide this functionality for the data that is being collected. CFS has no authorization to review/update any type of information since it's owned by the primary application.

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. Explanation:
☒	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 08/07/2018 ☐ 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.

Personally identifiable information in CFS is secured using appropriate administrative, physical, and technical safeguards in accordance with the applicable federal laws, Executive Orders, directives, policies, regulations, and standards. All access has role based restrictions, and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorize personnel. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access. Additionally, CFS is secured by various USPTO infrastructure components, including the Network and Security Infrastructure (NSI) system and other OCIO established technical controls to include password authentication at the server and database levels. SSNs and Taxpayer IDs are encrypted while at rest.

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)*: Existing Systems Records cover the information pulled from other systems residing in the CFS. These include: • COMMERCE/DEPT-1: Attendance, Leave, and Payroll Records of Employees and Certain Other Persons • COMMERCE/DEPT-2: Accounts Receivable • COMMERCE/DEPT-9: Travel Records (Domestic and Foreign) of Employees and Certain Other Persons • COMMERCE/PAT–TM–10: Deposit Accounts and Electronic Funds Transfer Profiles
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☐	No, a SORN is not being created.

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: General Accounting and Management Files: N1-241-05-1:5a1 Assignment Accounting and Management Files: N1-241-05-1:5a2 Fee Refund and Accounting Management Files: N1-241-05-1:5a3
☐	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):			

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: Name, Social security number, taxpayer ID, home/business address, email address, telephone number, financial information
☒	Quantity of PII	Provide explanation: Collectively, the number of records collected generate an enormous amount of PII and a breach in such large numbers of individual PII must be considered in the determination of the impact level.
☒	Data Field Sensitivity	Provide explanation: Combination of name, SSN, and financial information may be more sensitive.
☒	Context of Use	Provide explanation: PII stored in the system is for processing 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.
☒	Obligation to Protect Confidentiality	Provide explanation: Based on the data collected USPTO must protect the PII of each individual in accordance to the Privacy Act of 1974
☒	Access to and Location of PII	Provide explanation: Due to obtaining PII, necessary measures must be taken to ensure the confidentiality of information during processing, storing and transmission.
☐	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.