Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Consolidated Financial System (CFS)

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

Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry
Date: 2023.04.04 09:23:48 -04'00'

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

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

Unique Project Identifier: PTOC-001-00

Introduction: System Description

Provide a brief description of the information system.

The Consolidated Financial System (CFS) 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 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 Momentum 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.

Concur Government Edition (CGE): CGE is a web-based travel and planning management solution owned, hosted, maintained and operated by Concur, Inc. This is a general support application of 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.

eAcquisition Tool (ACQ): ACQ is a web-based COTS solution to support users in the acquisition community at the USPTO. This general support application 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).

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

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system

CFS is a major application.

(b) System location

Momentum: Momentum is located in Alexandria, Virginia PTO Data Center; disaster recovery is located in Manassas, Virginia. Momentum will be hosted by Amazon Web Services (AWS) cloud services in 2023.

Concur Government Edition (CGE): The Concur application is an externally hosted SaaS offering and managed by GSA.

eAcquisition Tool (ACQ): ACQ is located in Alexandria, Virginia PTO Data Center; disaster recovery is located in Manassas, Virginia. ACQ will be hosted by Amazon Web Services (AWS) cloud services in 2023.

VendorPortal: VendorPortal is located in Alexandria, Virginia PTO Data Center; disaster recovery is located in Manassas, Virginia. VendorPortal will be hosted by Amazon Web Services (AWS) cloud services in 2023.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

Momentum: Momentum interconnects with:

- eAcquisition Tool (ACQ): ACQ is a web-based COTS solution to support users in the acquisition community at the USPTO.
- Enterprise Data Warehouse (EDW): EDW is an information system that provides access to integrated USPTO data to support the decision-making activities of managers and analysts to answer strategic and tactical business questions.
- Fee Processing Next Generation (FPNG): Fee Processing Next Generation is the USPTO "Next Gen" solution for free process.
- Electronic Library for Financial Management Systems (EL4FMS) is an information system that provides access to USPTO financial-related documents to support the decision-making activities of managers and analysts. EL4FMS also supports users' business operations by providing access via FPNG to various financial documents relating to their FPNG account.
- General Services Administration Concur Government Edition (CGE): CGE is a web-based travel and planning management solution owned, hosted, maintained and operated by Concur, Inc.
- General Services Administration System Award Management (SAM) GSA's SAM is a combined system of nine federal procurement systems along with the Catalog of Federal Domestic Assistance. SAM was designed to streamline the process of both obtaining and procuring federal contracts by integrating systems.
- Central Contractor Registration Connector (CCRC) application allows for the transfer, as well as daily updates, of vendor data from the SAM database into agency applications (i.e., the agency's financial, procurement, and/or travel applications).
- Department of Agriculture (USDA) National Finance Center (NFC) The USDA NFC is a shared service provider for financial management services and human resources management services. NFC's assists in achieving cost-effective, standardized, and interoperable solutions that provide functionality to support strategic financial management and human resource management direction.

- Department of Treasury Do Not Pay (DNP): The Department of Treasury operates DNP dedicated to preventing and detecting improper payments. DNP is authorized and governed by the Payment Integrity Information Act of 2019 (PIIA), and several Office of Management and Budget (OMB) memoranda and circulars. The authorities generally belong to OMB, which delegated the operational aspects to the Department of the Treasury.
- Department of Treasury Payment Application Modernization (PAM): The U.S. Government uses the Payment Automation Manager (PAM) to pay all bills, except payments in foreign currency.
- USPTO Amazon Cloud Services (UACS) – The UACS General Support System is a standard infrastructure platform that supports USPTO Application Information Systems (AIS) hosed in Amazon Web Services (AWS). This interconnection is expected in 2023.

Concur Government Edition (CGE): Concur interconnects with:

- 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.
- Enterprise Data Warehouse (EDW): EDW is an information system that provides access to integrated USPTO data to support the decision-making activities of managers and analysts to answer strategic and tactical business questions.
- USPTO Amazon Cloud Services (UACS) – The UACS General Support System is a standard infrastructure platform that supports USPTO Application Information Systems (AIS) hosed in Amazon Web Services (AWS). This interconnection is expected in 2023.

eAcquisition Tool (ACQ): ACQ interconnects with:

- 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.
- VendorPortal: VendorPortal is a web-based COTS solution to provide a platform for interaction and information exchange between USPTO and the vendor community.
- Enterprise Data Warehouse (EDW): EDW is an information system that provides access to integrated USPTO data to support the decision-making activities of managers and analysts to answer strategic and tactical business questions.
- Electronic Library for Financial Management Systems (EL4FMS): EL4FMS is an information system that provides access to USPTO financial-related documents to support the decision-making activities of managers and analysts. EL4FMS also supports users' business operations by providing access via FPNG to various financial documents relating to their FPNG account.

- USPTO Amazon Cloud Services (UACS): The UACS General Support System is a standard infrastructure platform that supports USPTO Application Information Systems (AIS) hosed in Amazon Web Services (AWS). This interconnection is expected in 2023.

VendorPortal: VendorPortal interconnects with ACQ (see descriptions above).

- USPTO Amazon Cloud Services (UACS) – The UACS General Support System is a standard infrastructure platform that supports USPTO Application Information Systems (AIS) hosed in Amazon Web Services (AWS). This interconnection is expected in 2023.

(d) The way the system operates to achieve the purpose(s) identified in Section 4

Momentum: Momentum operates as 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.

Concur Government Edition (CGE): CGE operates as 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.

eAcquisition Tool (ACQ): ACQ operates as 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).

VendorPortal: VendorPortal operates as 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.

(e) How information in the system is retrieved by the user

Momentum – Graphical User Interface (GUI)
Concur – Graphical User Interface (GUI)
ACQ – Graphical User Interface (GUI)
VP – Graphical User Interface (GUI)

(f) How information is transmitted to and from the system
Momentum: Momentum information is transmitted via various integrations and user data entry, as explained in introduction (C).

Concur Government Edition (CGE): Concur - information is transmitted via various integrations and user data entry, as explained in introduction (C).
eAcquisition Tool (ACQ): ACQ information is transmitted via various integrations and user data entry, as explained in introduction (C).

VendorPortal: VendorPortal information is transmitted via various integrations and user data entry, as explained in introduction (C).

(g) Any information sharing
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 revenue accounting information from 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.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
- E.O. 9397
- 31 U.S.C. 3325, 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

(i) The Federal Information Processing Standards (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, and there is not a SAOP approved Privacy Impact Assessment.

☒ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

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*	☒	f. Driver's License	☐	j. Financial Account	☒
b. Taxpayer ID	☒	g. Passport	☐	k. Financial Transaction	☒
c. Employer ID	☐	h. Alien Registration	☐	l. Vehicle Identifier	☐

d. Employee ID	☒	i. Credit Card	☒	m. Medical Record	☐
e. File/Case ID	☐				

n. Other identifying numbers (specify):

*Explanation for the business 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.

General Personal Data (GPD)					
a. Name	☒	h. Date of Birth	☒	o. Financial Information	☒
b. Maiden Name	☐	i. Place of Birth	☐	p. Medical Information	☐
c. Alias	☐	j. Home Address	☒	q. Military Service	☐
d. Gender	☐	k. Telephone Number	☒	r. Criminal Record	☐
e. Age	☐	l. Email Address	☒	s. Marital Status	☐
f. Race/Ethnicity	☐	m. Education	☐	t. Mother's Maiden Name	☐
g. Citizenship	☐	n. Religion	☐		

u. Other general personal data (specify): credit card information (limited to type of card, last four, and expiration date). Sex (male, female)

Work-Related Data (WRD)					
a. Occupation	☐	e. Work Email Address	☒	i. Business Associates	☐
b. Job Title	☐	f. Salary	☐	j. Proprietary or Business Information	☐
c. Work Address	☐	g. Work History	☐	k. Procurement/contracting records	☐
d. Work Telephone Number	☒	h. Employment Performance Ratings or other Performance Information	☐		

l. Other work-related data (specify): Unique Entity Identifier (UEI)

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	☐	f. Scars, Marks, Tattoos	☐	k. Signatures	☐
b. Palm Prints	☐	g. Hair Color	☐	l. Vascular Scans	☐
c. Voice/Audio Recording	☐	h. Eye Color	☐	m. DNA Sample or Profile	☐
d. Video Recording	☐	i. Height	☐	n. Retina/Iris Scans	☐
e. Photographs	☐	j. Weight	☐	o. Dental Profile	☐

p. 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	☐	f. 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 Describe how the accuracy of the information in the system is ensured.

The system is secured using appropriate administrative physical and technical safeguards in accordance with the National Institute of Standards and Technology (NIST) security controls (encryption, access control, and auditing).

Administrators and specialists have the ability to modify user information and work with employees to validate the accuracy of the information. From a technical implementation, USPTO implements security and management controls to prevent the inappropriate disclosure of sensitive information. Security controls are employed to ensure information is resistant to tampering, remains confidential as necessary, and is available as intended by the agency and expected by authorized users. Management controls are utilized to prevent the inappropriate disclosure of sensitive information. Access controls, including the concept of

least privilege, are in place within the system to protect the integrity of this data as it is processed or stored. Mandatory IT awareness and role-based training is required for staff who have access to the system and address how to handle, retain, and dispose of data. All access has role based restrictions and individuals with privileges have undergone vetting and suitability screening. The USPTO maintains an audit trail and performs random, periodic reviews (quarterly) to identify unauthorized access and changes as part of verifying the integrity of administrative account holder data and roles. Inactive accounts will be deactivated and roles will be deleted from the application. The Perimeter Network (NSI) and Security and Compliance Services (SCS) provide additional automated transmission and monitoring, mechanisms to ensure that PII/BII information is secure. In addition, USPTO Amazon Cloud Services (UACS) 2023, will provide additional automated transmission and monitoring, mechanisms to ensure that PII/BII information is secure.

2.4 Is the information covered by the Paperwork Reduction Act?

☒	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. 0651-0043 Financial Transactions
☐	No, the information is not covered by the Paperwork Reduction Act.

2.5 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): Click or tap here to enter text.			

☐	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			
For a Computer Matching Program	☐	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 system contains information about DOC employees, contractors, and members of the public.

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/BII stored in the system is for a combination of employees, contractors, and vendors.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating

unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

In the event of computer failure, insider threats, or attach against the system by adversarial or foreign entities, any potential PII data stored within the system could be exposed. To avoid a breach, the system has certain security controls in place to ensure the information is handled, retained, and disposed of appropriately. Access to individual's PII is controlled through the application, and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. These audit trails are based on application server out-of-the-box logging reports as well as developed audit reports reviewed by the CFMPD Admin team and any suspicious indicators are promptly investigated and appropriate action taken. Also, system users undergo annual mandatory training regarding appropriate handling of information.

All data transmissions are encrypted and requires 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.

NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees.

The following are USPTO current policies; Information Security Foreign Travel Policy (OCIO-POL-6), IT Privacy Policy (OCIO- POL-18), IT Security Education Awareness Training Policy (OCIO-POL-19), Personally Identifiable Data Removal Policy (OCIO-POL-23), USPTO Rules of the Road (OCIO-POL- 36).

All offices adhere to the USPTO Records Management Office's Comprehensive Records Schedule or the General Records Schedule and the corresponding disposition authorities or citations.

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 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

☒	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☐	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☐	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 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) External Systems: • General Services Administration Concur Government Edition (CGE)

	• General Services Administration System for Award Management (SAM) • Department of Agriculture National Finance Center (NFC) • Central Contractor Registration Connector (CCRC) • Department of Treasury DoNotPay (DNP) • Department of Treasury Payment Application Modernization (PAM) All data transmissions are encrypted and requires 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. NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. The following are USPTO current policies; Information Security Foreign Travel Policy (OCIO-POL-6), IT Privacy Policy (OCIO- POL-18), IT Security Education Awareness Training Policy (OCIO-POL-19), Personally Identifiable Data Removal Policy (OCIO-POL-23), USPTO Rules of the Road (OCIO-POL- 36). All offices adhere to the USPTO Records Management Office's Comprehensive Records Schedule or the General Records Schedule and the corresponding disposition authorities or citations.
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 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: https://www.uspto.gov/privacy-policy.	
☒	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.
☐	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 is

		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: Access to PII/BII is monitored and tracked via (ARMS). General system logging is monitored and tracked.
☒	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 8/4/2022 ☐ 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 (POA&M).
☒	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☒	Contracts with customers establish DOC 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. *(Include data encryption in transit and/or at rest, if applicable).*

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, standards and NIST requirements.

Such management controls include a review process to ensure that management controls are in place and documented in the System Security Privacy Plan (SSPP). The SSPP specifically addresses the management, operational, and technical controls that are in place and planned during the operation of the system. Operational safeguards include restricting access to PII/BII data to a small subset of users. 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 authorized personnel. The system maintains an audit trail and the

appropriate personnel is alerted when there is suspicious activity. Data is encrypted in transit and at rest.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g., name or Social Security number)?

☒ Yes, the PII/BII is searchable by a personal identifier.

☐ No, the PII/BII is not searchable by a personal identifier.

9.2 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, number, and link. *(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 Profile COMMERCE/DEPT-22: Small Purchase Records
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☐	No, this system is not a system of records and a SORN is not applicable.

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 Level

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. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

☐	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 level. *(Check all that apply.)*

☒	Identifiability	Provide explanation: Name, Social security number, taxpayer ID, home/business address, email address, telephone number, and 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: Because the information containing PII must be transmitted outside of the USPTO environment, there is an added need to ensure the confidentiality of information during transmission. Necessary measures must be taken to ensure the confidentiality of information during processing, storing and transmission.
☐	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Private information exposure through insider threat pose risks and USPTO has policies, procedures and training to ensure that employees are aware of their responsibility of protecting sensitive information and the negative impact on the agency if there is a loss, misuse, or unauthorized access to or modification of sensitive private information. USPTO requires annual security role-based training and annual mandatory security awareness procedure training for all employees. Physical access to servers is restricted to only a few authorized individuals. The servers storing the potential PII are located in a highly sensitive zone within the cloud and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved and authorized accounts. USPTO monitors, in real-time, all activities and events within the servers storing the potential PII data and personnel review audit logs received on a regular bases and alert the appropriate personnel when inappropriate or unusual activity is identified.

The following are USPTO current policies; Information Security Foreign Travel Policy (OCIO-POL-6), IT Privacy Policy (OCIO- POL-18), IT Security Education Awareness Training Policy (OCIO-POL-19), Personally Identifiable Data Removal Policy (OCIO-POL-23), USPTO Rules of the Road (OCIO-POL- 36). All offices of USPTO adhere to USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.

12.2 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.

12.3 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.

Points of Contact and Signatures

System Owner
Name: Marci Etzel
Office: Office of the Core Financial Management Products Division-C/CFMD
Phone: (571) 272-5415
Email: Marci.Etzel@uspto.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: Users, Etzel, Marci M. Digitally signed by Users, Etzel, Marci M. Date: 2023.03.14 10:36:47 -04'00'

Date signed: _____

Chief Information Security Officer
Name: Don Watson
Office: Office of the Chief Information Officer (OCIO)
Phone: (571) 272-8130
Email: Don.Watson@uspto.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: Users, Watson, Don Digitally signed by Users, Watson, Don Date: 2023.04.03 19:23:41 -04'00'

Date signed: _____

Privacy Act Officer
Name: Ezequiel Berdichevsky
Office: Office of General Law (O/GL)
Phone: (571) 270-1557
Email: Ezequiel.Berdichevsky@uspto.gov

I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.

Signature: Users, Berdichevsky, Ezequiel Digitally signed by Users, Berdichevsky, Ezequiel Date: 2023.04.03 08:59:44 -04'00'

Date signed: _____

Bureau Chief Privacy Officer and Co-Authorizing Official
Name: Henry J. Holcombe
Office: Office of the Chief Information Officer (OCIO)
Phone: (571) 272-9400
Email: Jamie.Holcombe@uspto.gov

I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.

Signature: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2023.04.04 09:25:20 -04'00'

Date signed: _____

Co-Authorizing Official
Name: Jay Hoffman
Office: Office of the Chief Financial Officer-C/CFO
Phone: (571) 272-7262
Email: Jay.Hoffman@uspto.gov

I certify that this PIA accurately reflects the representations made to me herein by the System Owner, the Chief Information Security Officer, and the Chief Privacy Officer regarding security controls in place to protect PII/BII in this PIA.

Signature: Users, Mildrew, Sean Digitally signed by Users, Mildrew, Sean Date: 2023.04.10 15:01:03 -04'00'

Date signed: _____

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.