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

JENNIFER GOODE
Digitally signed by JENNIFER GOODE
Date: 2021.06.07 16:27:52 -04'00'

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

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 associated with the plan. ACQ integrates with Momentum, Vendor Portal, Enterprise Data Warehouse (EDW), and the Electronic Library for Financial Management Systems (EL4FMS).

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

CFS is a major application (MA).

(b) System location

Momentum
Momentum is located in Alexandria, Virginia PTO DataCenter; disaster recovery is located in Boyers, PA.

Concur Government Edition (CGE)
Concur integration is located in Alexandria, Virginia PTO DataCenter; disaster recovery is located in Boyers, PA. The Concur application is externally hosted and managed by GSA.

e Acquisition Tool (ACQ)
ACQ is located in Alexandria, Virginia PTO DataCenter; disaster recovery is located in Boyers, PA.

VendorPortal
VendorPortal is located in Alexandria, Virginia PTO DataCenter; disaster recovery is located in Boyers, PA.

(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:
- e Acquisition Tool (ACQ)
- VendorPortal
- Enterprise Data Warehouse (EDW)
- Electronic Library for Financial Management Systems (FL4FMS)
- Fee Processing Next Generation (FPNG)
- General Services Administration Concur Government Edition (CGE)
- General Services Administration System Award Management (SAM)
- Central Contractor Registration Connector (CCRC)
- Department of Agriculture National Finance Center (NFC)
- Department of Treasury Do Not Pay (DNP)
- Department of Treasury Payment Application Modernization (PAM)
Concur Government Edition (CGE): Concur interconnects with:
- Momentum
- Enterprise Data Warehouse (EDW)

eAcquisition Tool (ACQ): ACQ interconnects with:
- Momentum
- VendorPortal
- Enterprise Data Warehouse (EDW)
- Electronic Library for Financial Management Systems (EL4FMS)

VendorPortal: VendorPortal interconnects with ACQ

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

Momentum
Momentum serves as 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 serves 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 serves 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 serves 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.

Concur Government Edition (CGE)
Concur - information is transmitted via various integrations and user data entry.

eAcquisition Tool (ACQ)
ACQ information is transmitted via various integrations and user data entry.

VendorPortal
VendorPortal information is transmitted via various integrations and user data entry.

(g) 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 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

- Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; and Federal Claim Collection Act of 1966

(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.)*

<table>
<thead>
<tr>
<th>Changes That Create New Privacy Risks (CTCNPR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Conversions</td>
</tr>
<tr>
<td>b. Anonymous to Non-Anonymous</td>
</tr>
<tr>
<td>c. Significant System Management Changes</td>
</tr>
<tr>
<td>j. Other changes that create new privacy risks (specify):</td>
</tr>
</tbody>
</table>

☐ 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 (version 01-2015 or 01-2017).

☐ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later).


**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.)*

<table>
<thead>
<tr>
<th>Identifying Numbers (IN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Social Security*</td>
</tr>
<tr>
<td>b. Taxpayer ID</td>
</tr>
<tr>
<td>c. Employer ID</td>
</tr>
<tr>
<td>d. Employee ID</td>
</tr>
<tr>
<td>e. File/Case ID</td>
</tr>
<tr>
<td>n. Other identifying numbers (specify):</td>
</tr>
</tbody>
</table>

*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. VendorPortal and ACQ capture DUNS number for vendor records.

<table>
<thead>
<tr>
<th>General Personal Data (GPD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Name</td>
</tr>
<tr>
<td>b. Maiden Name</td>
</tr>
<tr>
<td>c. Alias</td>
</tr>
<tr>
<td>d. Gender</td>
</tr>
<tr>
<td>e. Age</td>
</tr>
<tr>
<td>f. Race/Ethnicity</td>
</tr>
<tr>
<td>g. Citizenship</td>
</tr>
<tr>
<td>u. Other general personal data (specify):</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work-Related Data (WRD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Occupation</td>
</tr>
<tr>
<td>b. Job Title</td>
</tr>
<tr>
<td>c. Work Address</td>
</tr>
<tr>
<td>d. Work Telephone Number</td>
</tr>
<tr>
<td>l. Other work-related data (specify):</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Distinguishing Features/Biometrics (DFB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Fingerprints</td>
</tr>
<tr>
<td>k. Signatures</td>
</tr>
</tbody>
</table>
2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

### Directly from Individual about Whom the Information Pertains

<table>
<thead>
<tr>
<th>In Person</th>
<th>Hard Copy: Mail/Fax</th>
<th>Online</th>
</tr>
</thead>
<tbody>
<tr>
<td>☒</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telephone</td>
<td>Email</td>
<td>☒</td>
</tr>
<tr>
<td>Other(specific):</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Government Sources

<table>
<thead>
<tr>
<th>Within the Bureau</th>
<th>Other DOC Bureaus</th>
<th>Other Federal Agencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>☒</td>
<td></td>
<td>☒</td>
</tr>
<tr>
<td>State, Local, Tribal</td>
<td>Foreign</td>
<td></td>
</tr>
<tr>
<td>Other(specific):</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Non-government Sources

<table>
<thead>
<tr>
<th>Public Organizations</th>
<th>Private Sector</th>
<th>Commercial Data Brokers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Third Party Website or Application</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other(specific):</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### System Administration/Audit Data (SAAD)

- a. User ID
- b. IP Address
- c. Date/Time of Access
- d. Queries Run
- e. ID Files Accessed
- f. Contents of Files
- g. Others system administration/audit data (specify):

### Other Information (specify)

- Palm Prints
- Voice/Audio Recording
- Video Recording
- Photographs
- Hair Color
- Eye Color
- Height
- Weight
- Vascular Scans
- DNA Sample or Profile
- Retina/Iris Scans
- Dental Profile
- Other distinguishing features/biometrics (specify):
2.3 Describe how the accuracy of the information in the system is ensured.

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.

2.4 Is the information covered by the Paperwork Reduction Act?

- [x] 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.)

<table>
<thead>
<tr>
<th>Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNNPD)</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Cards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Caller-ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal Identity Verification (PIV) Cards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other (specify):</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- [x] 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.)

<table>
<thead>
<tr>
<th>Activities</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio recordings</td>
<td></td>
<td>Building entry readers</td>
</tr>
<tr>
<td>Video surveillance</td>
<td></td>
<td>Electronic purchase transactions</td>
</tr>
<tr>
<td>Other (specify):</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- [x] 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.)

<table>
<thead>
<tr>
<th>Purpose</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>For a Computer Matching Program</td>
<td></td>
</tr>
<tr>
<td>For administrative matters</td>
<td></td>
</tr>
<tr>
<td>For litigation</td>
<td></td>
</tr>
<tr>
<td>For civil enforcement activities</td>
<td></td>
</tr>
<tr>
<td>To improve Federal services online</td>
<td></td>
</tr>
<tr>
<td>For web measurement and customization technologies (single-session)</td>
<td></td>
</tr>
<tr>
<td>For web measurement and customization technologies (multi-session)</td>
<td></td>
</tr>
<tr>
<td>Other (specify):</td>
<td></td>
</tr>
</tbody>
</table>

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/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.)
Private information exposure through insider threat and unauthorized access by foreign entities pose potential risks to this system. 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.

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.

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.)

<table>
<thead>
<tr>
<th>Recipient</th>
<th>How Information will be Shared</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Case-by-Case</td>
</tr>
<tr>
<td>Within the bureau</td>
<td></td>
</tr>
<tr>
<td>DOC bureaus</td>
<td></td>
</tr>
<tr>
<td>Federal agencies</td>
<td></td>
</tr>
<tr>
<td>State, local, tribal gov’t agencies</td>
<td></td>
</tr>
<tr>
<td>Public</td>
<td></td>
</tr>
<tr>
<td>Private sector</td>
<td></td>
</tr>
<tr>
<td>Foreign governments</td>
<td></td>
</tr>
<tr>
<td>Foreign entities</td>
<td></td>
</tr>
<tr>
<td>Other(specify):</td>
<td></td>
</tr>
</tbody>
</table>

☐ 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)  
  - Momentum  
  - ACQ  
  - VendorPortal  
- Information Delivery Product (IDP)  
  - Enterprise Data Warehouse (EDW)  
  - Electronic Library for Financial Management Systems (ELAFMS)  
- 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 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.

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

<table>
<thead>
<tr>
<th>Class of Users</th>
<th>Government Employees</th>
<th>Other (specify):</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Public</td>
<td>☐</td>
<td>☒</td>
</tr>
<tr>
<td>Contractors</td>
<td>☒</td>
<td></td>
</tr>
</tbody>
</table>

**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.
<table>
<thead>
<tr>
<th></th>
<th>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: __________________________.</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>No, notice is not provided. Specify why not:</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th></th>
<th>Yes, individuals have an opportunity to decline to provide PII/BII. Specify how:</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th></th>
<th>Yes, individuals have an opportunity to consent to particular uses of their PII/BII. Specify how:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th></th>
<th>Yes, individuals have an opportunity to review/update PII/BII pertaining to them. Specify how:</th>
</tr>
</thead>
</table>
| | 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
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): 08/07/2020
  - 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 I 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, 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 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–IO**: Deposit Accounts and Electronic Funds Transfer Profile

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

<table>
<thead>
<tr>
<th>Disposal</th>
<th>Shredding</th>
<th>Overwriting</th>
<th>Degaussing</th>
<th>Deleting</th>
</tr>
</thead>
</table>

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.
- [x] 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.)*

- [x] Identifiability
  
  Provide explanation: Name, Social security number, taxpayer ID, home/business address, email address, telephone number, financial information

- [x] 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.

- [x] Data Field Sensitivity
  
  Provide explanation: Combination of name, SSN, and financial information may be more sensitive.

- [x] 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;
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. 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.  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>□</td>
<td>Explanation:</td>
</tr>
<tr>
<td>✗</td>
<td>No, the conduct of this PIA does not result in any required technology changes.</td>
</tr>
</tbody>
</table>