Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Fee Processing Next Generation (FPNG) 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

Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry
Date: 2023.10.27 21:25:15 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Fee Processing Next Generation (FPNG) System

Unique Project Identifier: PTOC-004-00

Introduction: System Description

Provide a brief description of the information system.

Fee Processing Next Generation is the United States Patent and Trademark Office's (USPTO) "Next Gen" solution for fee processing. FPNG allows internal and external users to manipulate payment accounts, perform profile updates, and make payments for USPTO goods and services. It also provides all functionality related to managing payments, replenishing and transferring of deposit account balances, etc. (primarily handled by the General Ledger/Account Commercial off the Shelf (COTS) Support tier/Momentum). FPNG also supports pricing rules management as well as refund requests and approvals.

FPNG has interfaces to various USPTO systems and with the United States Treasury. USPTO system interfaces include MyUSPTO Cloud (MyUSPTO-C), ICAM Identity as a Service (ICAM IDaaS), Patent Application Location Monitoring (PALM), Momentum, Electronic Library for Financial Management Systems (EL4FMS) and the Enterprise Data Warehouse (EDW). FPNG interfaces to US Treasury include Pay.Gov and Over the Counter (OTCnet) application services.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system
FPNG is a Major Application within USPTO.

(b) System location
FPNG is hosted by Amazon Web Services (AWS) cloud services.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
FPNG sends and receives information from the following interconnect systems:

ICAM Identity as a Service (ICAM IDaaS) - provides an enterprise authentication and authorization service to all applications/AIS's.

Consolidated Financial System (CFS) - CFS provides financial management, procurement, and travel management in support of the USPTO mission.

Enterprise Desktop Platform (EDP) - EDP is an infrastructure information system that provides a standard enterprise-wide environment to manage desktops and laptops.
Information Delivery Product (IDP) - IDP is a Master System composed of the following three subsystems: 1) Enterprise Data Warehouse; 2) Electronic Library for Financial Management System (EL4FMS); and 3) Financial Enterprise Data Management Tools (FEDMT).

Network and Security Infrastructure System (NSI) - NSI is an infrastructure information system that facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO IT applications.

MyUSPTO-Cloud (MyUSPTO-C) – MyUSPTO-C is a major external-facing web site application. MyUSPTO Cloud provides external stakeholders with one unified place to register with the USPTO, manage their contact information and other identifying information, and manage their fees. Provide a foundation architecture that allows other NG applications to interact with MyUSPTO-C and provide data consistency for all customer account information.

Intellectual Property Assignment System (IPAS) – IPAS is a major application that allows for electronic assignment of a patent or trademark via a website. It is a document management workflow system that supports the processing of assignment documents.

Security and Compliance Services (SCS) – SCS is a general support system that provides enterprise level monitoring to USPTO systems.

Patent Trial and Appeal Case Tracking System (PTACTS) – P-TACTS is an application information system and provides support to USPTO's administrative law body Patent Trial and Appeal Board for the purpose of electronically filing documents in connection with the Inter Parties Disputes established under the Leary-Smith America Invents Act (AIA).

Trademark Processing System-External (TPS-ES) – Is a major application that provides customer support for processing Trademark applications for USPTO.

Trademark Trial and Appeal Board Center (TTAB-C) – TTAB-C is a major application that provides an online interface for USPTO customers to submit forms to the USPTO's Trademark Trial and Appeal Board electronically.

Trademark Processing System (External)(TPS-ES) - TPS-ES is Major Application Information System that provides customer support for processing Trademark applications.

Patent Capture and Application Processing System (PCAPS-IP) - PCAPS-IP is a Major Application Information System that supports USPTO patent application processes.

Patent End to End (PE2E) - PE2E is a Master system portfolio for USPTO patent users.

Information Dissemination Support System (IDSS) - IDSS is a Major Application that interconnects with Patent Capture and Application Processing System – Examination Support (PCAPS-ES), a collection of tools to facilitate USPTO examiners' ability to process, examine and review patent applications.

Intellectual Property Leadership Management System (IPLMSS) - IPLMSS is an Application Information System that provides capabilities and functionality for patent examiners to perform their roles.

USPTO Amazon Cloud Services (UACS) - The UACS General Support System is a standard infrastructure platform that supports USPTO Application Information Systems (AIS) hosted in Amazon Web Services (AWS).

U.S. Treasury (Bureau of the Fiscal Service) / Pay.gov – Pay.gov is a federal program that provides a secure way to pay U.S. federal government agencies.

U.S. Treasury (Bureau of the Fiscal Service) / Over-the-Counter Channel Application (OTCnet) – OTCnet is a federal web-based application that offers federal agencies flexible solutions to streamline management and reporting of payment transactions and deposits.

(d) The way the system operates to achieve the purpose(s) identified in Section 4
FPNG provides USPTO customers a modern payment system. FPNG provides services to the public and internal facing functionality that enables USPTO employees to support customers. FPNG allows internal and external users to manage payment accounts, perform profile updates, and make payments for USPTO goods and services, etc. via the FPNG User Interface (UI). It also provides all functionality related to managing payments and replenishing and transferring deposit account balances.

(e) How information in the system is retrieved by the user
Users retrieve information via the FPNG UI.

(f) How information is transmitted to and from the system
Communications utilize a minimum of TLS 1.1 with FIPS 140-2 compliant algorithms to provide transmission confidentiality and integrity for all connections outside the system boundary. The externally-facing VIPs supporting FPNG are configured to only support TLS 1.2.

(g) Any information sharing
Information about customers' credit card transactions is sent to (the U.S. Treasury's) Pay.gov system for authorization (real-time) and settlement (same day) and customers' banking information is sent to the Pay.gov system (daily batch- not real-time) for pre-notifications (new account verification-zero dollar transaction) and for EFT processing. Employee information is not shared with any other system or agency.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
The USPTO collects customer financial information for fee processing under 35 U.S.C. 2 and 41 and 15 U.S.C.1113, as implemented in 37 CFR 1.16–1.28, 2.6–2.7, and 2.206–2.209.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system
FPNG is categorized as a Moderate system.

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:					

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):					

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):					

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.

From a technical implementation, USPTO implements security and management controls to ensure the accuracy 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. In addition, the Perimeter Network (NSI), USPTO Amazon Cloud Services (UACS), and Security and Compliance Services (SCS) 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. OMB 0651-0016
☐	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).

PII about members of the public, DOC employees, and contractors are collected by the information system. The USPTO collects customer financial information for fee processing. Under 35 U.S.C, Section 41 and 15 U.S.C. Section 1113, as implemented in 37 CFR, the USPTO charges fees for processing and services related to patents, trademarks, and information products. In the case of payments, we collect information about the payment method in order to troubleshoot or complete a chargeback should there be a problem with the payment. All employee information is collected in order to identify the FPNG fee processor and organization in which they work. The FPNG system is set up with role-based privileges, so an employee only has access to those specific functions permitted within their organization or by their required duties.

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.)

Adversarial entities, foreign governments, insider threats and inadvertent private information exposure are all 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 current USPTO policies; Information Security Foreign Travel Policy (OCIO-POL-6), IT Privacy Policy (OCIOPOL-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 the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation. 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. All offices of the USPTO adhere to the 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.)*

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: • Consolidated Financial System (CFS) • Information Delivery Product (IDP) • Trademark Processing System (External)(TPS-ES) • Patent Capture and Application Processing System (PCAPS-IP) • Patent End to End (PE2E) • Information Dissemination Support System (IDSS) • Intellectual Property Leadership Management System (IPLMSS) • USPTO Amazon Cloud Services (UACS) • ICAM Identity as a Service (IDaaS) 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. All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.
☐	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:
☐	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: Individuals can choose not to provide their financial information but this will prevent their application from being processed.
☐	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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: Customers are given the opportunity to choose the payment options they prefer and thus limiting the amount of information they provide to the system for the processing of their transactions. All financial information collected is for payment processing to obtain services related to intellectual property and the protection of intellectual property rights.
☐	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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: Users can review/update PII/BII pertaining to them by utilizing the Financial Manager user interface.
☐	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

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 is subject to the auditing process and logs are maintained for this purpose.
☒	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): 2/17/2023 ☐ 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).*

FPNG is secured by the USPTO's infrastructure systems, FedRAMP-authorized Amazon Web Services (AWS), and established technical controls to include password authentication at the server and database levels. HTTPS is used for all data transmissions to and from the Internet, USPTO DMZ, and PTOnet. A dedicated socket is used to perform encryption and decryption. Data at rest is encrypted via database-level technical controls for ball database instances. In supporting fee collection via Internet Web storefronts, FPNG uses a secure architecture. When a fee payment is required, users of a "legacy storefront" are redirected to a Secure Hypertext Transfer Protocol (HTTPS) URL from their specific storefront Web pages. After requesting a purchase transaction, the client's web browser is redirected to the load balanced edge servers located in the USPTO Sensitive DMZ.

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)*: COMMERCE/PAT–TM–10 Deposit Accounts and Electronic Funds Transfer Profiles COMMERCE/DEPT-2 Accounts Receivable
☐	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: GRS 1.1:010: Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting.
☐	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: The combination of name, address, home address, employee ID, and user ID can easily identify a particular individual.
☒	Quantity of PII	Provide explanation: Collectively, the number of records collected constitute a large 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: The combination of name and financial information increases the sensitivity of the data in the system.
☒	Context of Use	Provide explanation: PII is collected to process payments and to communicate with external customers in case there are any problems with fee processing and also used to identify the fee processor and the organization.
☒	Obligation to Protect Confidentiality	Provide explanation: Based on the sensitive nature of 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: Security controls are in place to protect the confidentiality of PII during processing, storage, 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.)

Adversarial entities, foreign government, insider threats and inadvertent private information exposure are all 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 current USPTO policies; Information Security Foreign Travel Policy (OCIO-POL-6), IT Privacy Policy (OCIOPOL-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 the USPTO adhere to the 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