Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Service Management Platform (SMP)

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

Tahira Murphy Digitally signed by Tahira Murphy Date: 2022.08.25 15:07:06 -04'00' 8/25/2022

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Service Management Platform

Unique Project Identifier: EIPL-DS-02-00

Introduction: System Description

Provide a brief description of the information system.

Service Management Platform (SMP) is a Software as a Service (SaaS) cloud-based Information Technology Services Management (ITSM) Major Application (MA) that provides a single system of record for IT services, operations, and business management by automating IT service applications and processes.

SMP is an interconnected system that uses ServiceNow's cloud-based SaaS ITSM to provide core functionality. USPTO provides authentication services to SMP via Role Based Access Controls (RBAC) and passes authentication services to ServiceNow via Management, Instrumentation, and Discovery (MID) servers. To be granted access to SMP, USPTO employees or contractors must be connected to USPTO's network environment. Additionally, Archer services will be used to provide USPTO Security Operation Center (SOC) Incident reports to the Department of Commerce (DOC).

USPTO uses SMP to track and manage IT Service Desk incidents, problems, and change requests, with enhanced functionality to meet the growing IT service management requirements from across the enterprise. It specializes in ITSM by providing the infrastructure needed to perform data collection, storage, and application development on a single platform.

SMP supports the following management and services: Asset Management, Incident Management, Problem Management, Knowledge Management, Change Management, Service Catalog Management, Survey Management, Service Level Management and Reporting, Mobile Asset Scanning, and Interactions Management.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system
Service Management Platform (SMP) is a Software as a Service (SaaS).

(b) System location
SMP is also hosted at ServiceNow's Government Community Cloud (GCC) hosting facilities located in Culpeper, Virginia and Miami, Florida.

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

Identity, Credential, and Access Management – Identity-as-a-service (ICAM-IDaaS) - IDaaS provides unified access management across applications and API based on single sign-on service. Identity and access management is provided by Okta's cloud-based solution which uses Universal Directory to create and manage users and groups.

BlackBerry Enterprise Server Mobile Device Management (BES – Blackberry) - The USPTO internal and external users require different Commercial Off-The-Shelf (COTS) productivity tools to communicate to meet their mission. BES is one of the COTS products. Additionally, the USPTO relies on the Enterprise Software Services Division to perform many, repeatable tasks as part of production support, operations & project/enhancement work. Product is used to access email on mobile devices.

Agency Administrative Support System (AASS) - Global Enterprise Architecture Repository System (GEARS) has a parent-child relationship with AASS. GEARS provides a holistic view of the USPTO Enterprise Architecture and helps identify and track strategic goals, business functions, business process, roles, organizational structures, business information, and key performance metrics to technologies including software applications, services, platforms and network infrastructure. GEARS presents views, road maps, and analytics of the Current As-Is and Future To-Be state of the enterprise. The Enterprise Architecture Division (EAD) is supported by GEARS, which also extends enterprise interests and relationships, to key partners, suppliers, and customers.

Workstation Services (WS)- Configuration Management (ConfigMgmt) - WS-ConfigMgmt provides remote control, patch management, software distribution, operating system deployment, reporting, and hardware and software inventory. The main enterprise tools used to support the WS-ConfigMgmt for deployment, maintenance and management are Microsoft System Center Configuration Manager (SCCM).

Corporate Administrative Office System (CAOS) – CAOS has a parent-child relationship with Radio Frequency Asset Control Radio Frequency Identification (RFID) via use of the RFID technology tracks assets (formerly ALC). The RFID readers, deployed throughout the USPTO campus, read the RFID tags associated with laptops, monitors and other IT assets. This asset data is forwarded to a UL running ItemAware 2.9 asset management software - this data is in turn sent to the Remedy ITSM Asset Management module.

Security and Compliance Services (SCS) - Enterprise Cybersecurity Monitoring Operations (ECMO) has a parent-child relationship with SCS. The ECMO product provides near real-time security status (vulnerabilities, patch levels, and compliance)

through an endpoint agent on supported ULs, UD and server platforms, which reports (one-way communication) to relay servers in USPTO data center. These relay servers report to master servers at the DOC level (hosted NIST). ECMO plays a big role in implementing Continuous Diagnostic Mitigation (CDM) Phase I program, which provides USPTO with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. CDM Phase I utilizes ECMO Console to deploy BigFix Inventory (BFI) to all USPTO Endpoints.

Enterprise Data Warehouse (EDW) - is an automated information system (AIS) that provides access to integrated United States Patent and Trademark Office (USPTO) data to support the decision-making activities of managers and analysts in the USPTO's business areas as needed to achieve business goals. It helps USPTO managers and analysts to answer a variety of strategic and tactical business questions using quantitative enterprise business information. EDW has a parent-child relationship with Information Delivery Product (IDP).

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

USPTO uses SMP to track and manage IT Service Desk incidents, problems, and change requests, with enhanced functionality to meet the growing IT service management requirements from across the enterprise. SMP helps USPTO to maintain employee satisfaction and for administrative services. It specializes in ITSM by providing the infrastructure needed to perform data collection, storage, and application development on a single platform.

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

SMP Users will use service and incident tickets to populate information such as user name, contact number, and assigned assets etc. through lookup tables linked to fields on ticket forms.

(f) ***How information is transmitted to and from the system***

Information is transmitted to and from SMP via USPTO MID Server.

(g) ***Any information sharing***

Information is shared within the bureau on a case by case basis.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

5 U.S.C. 301; 35 U.S.C. 2; E-Government Act of 2002; OMB Circular A-130; and Foundations for Evidence-Based Policymaking Act.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

SMP has a FIPS 199 rating of 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: The rationale for having the SSN is to verify someone's identity before we provide them potential sensitive information / assistance in relation to account issues. These accounts are USPTO's so it is important that we					

verify the employee's identity before we offer assistance. We cannot use birthday because this is something that people often post online and therefore could be easily discovered.

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): Business Unit					

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): Port numbers and protocols for both victim and attacker as part of security incident investigation.					

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): Interfaces with EDW.					

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.

End users will have the ability to select pre-populated fields from predefined criteria to mitigate input errors prior to submitting a ticket. When reviewing a submitted ticket SMP Technicians will verify ticket data for accuracy and completeness. After ticket submission only authorized SMP technicians will have ability to modify data in the modules they have access.

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). 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 screen. 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.

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.
☒	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):			

☒	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).

SMP collects, maintains, or disseminates PII about Department of Commerce (DOC) employees, contractors working on behalf of DOC that uses ServiceNow's cloud-based SaaS ITSM to provide core functionality. The system is used to track and manage IT Service Desk incidents. The incidents that are documented could be from contractors or DOC employees. The PII is used to identify which employees have issues that may need to be resolved and for customer satisfaction. USPTO provides authentication services to SMP via Role Based Access Controls (RBAC) and passes authentication services to ServiceNow via Management, Instrumentation, and Discovery (MID) servers.

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.)

Foreign and adversarial entities as well as insider threats are the predominant threat to the systems privacy and data leakage. USPTO has implemented National Institute of Standards and Technology (NIST) security controls (encryption, access control, auditing) and selected ServiceNow which is a Federal Risk Authorization Management Program (FedRAMP) authorized cloud provider to reduce the risk. Mandatory IT Awareness and role-based training are required for staff that have access to the system and address how to handle, retain and dispose of data. Contract terms between ServiceNow and USPTO provide guidance on how data should be handled, retained and disposed.

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: Information Delivery Product (IDP) Identity, Credential, and Access Management – Identity-as-a- (ICAM-IDaaS) Agency Administrative Support System (AASS) Security and Compliance Services (SCS) Corporate Administrative Office System (CAOS) SMP has put certain security controls 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: Please see Appendix A.
☐	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: Users' opportunity to decline to provide PII/BII is available through source systems.

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: As a condition of employment at USPTO, employees and contractors consent to the collection and use of limited PII when using PTO technology.

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: DOC employees and contractors can update their information via USPTO's Office of Human Resources.
☐	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: Administrator conducts monthly audits of the system, to include when and by whom the system was accessed and what info was updated, changed corrected, etc.
☒	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): 4/16/21 ☐ 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).*

Automated operational controls include securing all hardware associated with SMP in the ServiceNow Data Center. The Data Center is controlled by using various methods including camera, motion detectors, card entry, audits, physical locks and alarms. Contingency planning has been prepared for the data. Backups are performed on the processing databases. All backup tapes that contain PII or information covered under the Privacy Act are encrypted with FIPS 140-3 compliant algorithms by the ServiceNow Database Administration Team. Technical

controls: Information is also secured through the application itself, by only allowing authorized users access to the application and to data to which they have access and privilege. Also the information system controls attacks and unauthorized attempts on the application and database through strict logins, AV protection, and through firewalls.

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/DEPT-27, Investigation and Threat Management Records COMMERCE/DEPT-16, Property Accountability Files COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies COMMERCE/PAT-TM-20, Customer Call Center, Assistance and Satisfaction Survey Records COMMERCE/PAT-TM-18, USPTO Personal Identification Verification (PIV) and Security Access Control Systems
☐	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 5.8, item 010, Technical and Administrative Help Desk Operational Records; • GRS 3.2, item 020: Computer Security Incident Handling, Reporting, and Follow-Up Records; • GRS 3.1, item 020, Information Technology Operations and Maintenance Records; and • GRS 3.1, item 030, Configuration and Change Management Records.

☐	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: Employee ID, File/Case ID, Name, SSN and Home Address in combination can be used to identify an individual.
☒	Quantity of PII	Provide explanation: SMP contains USPTO employee's and contractor's names and addresses which is passed from interconnected systems for an estimated 100 cases per year.
☒	Data Field Sensitivity	Provide explanation: PII that is stored within this system includes limited personal and work-related elements to ensure proper user identification. Any unauthorized access to this data would have a moderate impact on the organization and its operations.
☒	Context of Use	Provide explanation: SMP provides a single system of record for IT services, operations, and business management by automating IT service applications and processes. USPTO uses SMP to track and manage IT Service Desk incidents, problems, and change

		requests, with enhanced functionality to meet the growing IT service management requirements from across the enterprise.
☒	Obligation to Protect Confidentiality	Provide explanation: NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 5 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) and the Privacy Act of 1974.
☒	Access to and Location of PII	Provide explanation: To be granted access to SMP, USPTO employees or contractors must be connected to USPTO's network environment. PII in SMP is parsed to SMP via USPTO ICAM-RBAC and is stored in the user table, or is entered into SMP tickets by SMP users and is stored in the task record.
	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.)

Foreign and adversarial entities as well as insider threats are the predominant threat to the systems privacy and data leakage. Any PII that is used by SMP will be stored and maintained in interconnected and passed to SMP as required. This reduces the potential attack surface of SMP and lowers the overall risk to privacy. SMP collects the minimal amount of PII from potential users, and all system users undergo mandatory training regarding the appropriate handling of information.

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

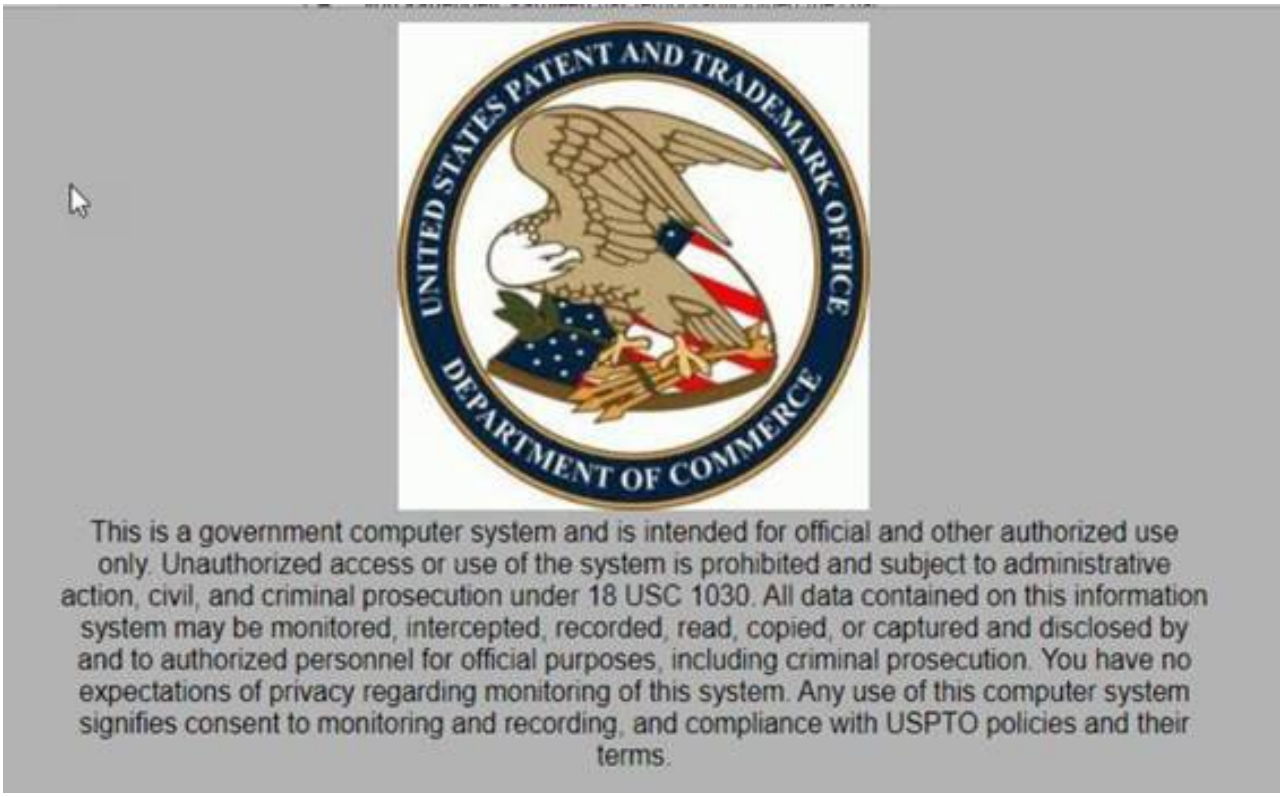
☐	Yes, the conduct of this PIA results in required business process changes. Explanation:
☒	No, the conduct of this PIA does not result in any required business process changes.

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.

Appendix A


UNITED STATES PATENT AND TRADEMARK OFFICE
DEPARTMENT OF COMMERCE
This is a government computer system and is intended for official and other authorized use only. Unauthorized access or use of the system is prohibited and subject to administrative action, civil, and criminal prosecution under 18 USC 1030. All data contained on this information system may be monitored, intercepted, recorded, read, copied, or captured and disclosed by and to authorized personnel for official purposes, including criminal prosecution. You have no expectations of privacy regarding monitoring of this system. Any use of this computer system signifies consent to monitoring and recording, and compliance with USPTO policies and their terms.

Points of Contact and Signatures

System Owner
Name: Kathryn McGlynn
Office: Office of the Chief Information Officer (OCIO)
Phone: (517) 270-2567
Email: Kathryn.McGlynn@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, McGlynn, Kathryn Digitally signed by Users, McGlynn, Kathryn Date: 2022.08.11 14:21:52 -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: 2022.08.12 09:46:03 -04'00'

Date signed: _____

Privacy Act Officer
Name: Caitlin Trujillo
Office: Office of General Law (O/GL)
Phone: (571) 270-7834
Email: Caitlin.Trujillo@uspto.gov

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

Signature: Caitlin Trujillo Digitally signed by Caitlin Trujillo Date: 2022.08.10 12:14:25 -04'00'

Date signed: _____

Bureau Chief Privacy Officer and 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.
By Direction

Signature: Users, Stephens, Deborah Digitally signed by Users, Stephens, Deborah Date: 2022.08.12 13:12:58 -04'00'

Date signed: _____

Co-Authorizing Official
Name: N/A
Office: N/A
Phone: N/A
Email: N/A

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: _____

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.