Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
Service Management Platform (SMP)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Service Management Platform (SMP)

Unique Project Identifier: EIPL-DS-02-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system: *Provide a brief description of the information system.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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:
Centralized Desktop Services Management (CDSM) – is a component of the System Center Configuration Manager. The assets an asset management suite that provides application inventory and deployment.

Data Storage Management System (DSMS) – provides the following services or functions in support of the USPTO mission: Secure environment for archival and storage of data and records vital to USPTO's Business Continuity and Disaster Recovery plan.

Enterprise Data Warehouse (EDW) - is an information system that provides access to integrated 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).

Global Enterprise Repository System (GEARS) - 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.

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.

Mobile Devices (MD) - the use of Apple devices (iPads and iPhones) for individuals that have been determined to have a business need for mobile access to access corporate email, view documents, manage contacts, schedule appointments, access the Intranet, etc.

Radio Frequency Identification (RFID) - implements an Enterprise-Level asset tracking solution to reduce the inventory management burden of asset management while increasing asset visibility of critical assets and improved inventory accuracy.

Storage Infrastructure Managed Service (SIMS) – is a Storage Infrastructure information service that provides access to consolidated, block level data storage and files system storage.

d) The purpose that the system is designed to serve

IT Stakeholder Groups utilize the system to enter USPTO IT incident and request tickets.

e) *The way the system operates to achieve the purpose*

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.

f) A general description of the type of information collected, maintained, used, or disseminated by the system

IT incident description, IT issue description and resolution, service requests including associated tasks, reporting and metric data.

g) Identify individuals who have access to information on the system

USPTO approved SMP license holders have role-based access privileges. Access is also available to SMP development team. All users of SMP must be located on USPTO Net to gain access to SMP via Single Sign on (SSO).

h) How information in the system is retrieved by the user

SMP users use service and incident tickets to populate users name, contact number, and assigned assets through lookup tables linked to fields on ticket forms.

i) How information is transmitted to and from the system

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

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

☐ This is a new information system. *Continue to answer questions and complete certification.*

☐ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions	☐	d. Significant Merging	☐	g. New Interagency Uses	☐
b. Anonymous to Non-Anonymous	☐	e. New Public Access	☐	h. Internal Flow or Collection	☐
c. Significant System Management Changes	☐	f. Commercial Sources	☐	i. Alteration in Character of Data	☐
j. Other changes that create new privacy risks (specify):					

☐ 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. *Continue to answer questions and complete certification.*

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

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

☐ Yes. This is a new information system.

☐ Yes. This is an existing information system for which an amended contract is needed.

☐ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

☒ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

☐ Yes. *(Check all that apply.)*

Activities			
Audio recordings	☐	Building entry readers	☐
Video surveillance	☐	Electronic purchase transactions	☐
Other (specify):			

☒ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

☐ Yes, the IT system collects, maintains, or disseminates BII.

☒ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

☒ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

☒ DOC employees
☒ Contractors working on behalf of DOC
☐ Other Federal Government personnel
☐ Members of the public

☐ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

☒ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form. Only the last two digits of the SSN is collected. SSN is collected from Contractors and DOC employees through multi-factor authentication for equipment delivery.
Provide the legal authority which permits the collection of SSNs, including truncated form. 5 U.S.C. 301 35 U.S.C. 2 E-Government Act, 2002 OMB Circular A-130 Foundations for Evidence-Based Policymaking Act

☐ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

☒ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

☐ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

☐ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

☒ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

☒ The criteria implied by one or more of the questions above **apply** to the Service Management Platform (SMP) and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

☐ The criteria implied by the questions above **do not apply** to the Service Management Platform (SMP) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Kathryn McGlynn Office: Office of the Chief Information Officer (OCIO) Phone: (517) 270-2567 Email: Kathryn.McGlynn@uspto.gov Signature: Users, McGlynn, Kathryn Digitally signed by Users, McGlynn, Kathryn Date: 2023.08.11 09:33:13 -04'00' Date signed: _____	**Chief Information Security Officer** Name: Timothy S. Goodwin Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-0653 Email: Timothy.Goodwin@uspto.gov Signature: Users, Goodwin, Timothy Digitally signed by Users, Goodwin, Timothy Date: 2023.08.17 16:19:37 -04'00' Date signed: _____
Privacy Act Officer Name: Heaton John Office: Office of General Law (O/GL) Phone: 703-756-1240 Email: Ricou.Heaton@uspto.gov Signature: John Ricou Heaton Digitally signed by John Ricou Heaton Date: 2023.08.02 18:06:33 -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 Signature: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2023.08.18 09:48:28 -04'00' Date signed: _____
Co-Authorizing Official Name: N/A Office: N/A Phone: NA Email: N/A Signature: _____ Date signed: _____	