Template Version Number: 01-2020

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

Privacy Threshold Analysis
for the
Security and Compliance Services (SCS)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Security and Compliance Services (SCS)

Unique Project Identifier: EIPL-SCS-01-00

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 and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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).

Security and Compliance Services (SCS) is a general support system comprised of subsystems which work together to provide enterprise level monitoring to the USPTO. The subsystems include:

Security Information and Event Management (SIEM) – SIEM provides a centralized command and control console with integrated enterprise log management, security information and event management, network behavior analysis, and reporting through a collection of events, network/application flow data, vulnerability data, and identity information. This solution consolidates events and data flows from a wide range of sources, and provides appropriate alerts on suspicious behavior to USPTO security, infrastructure, and operational personnel. **Collection of PII is incidental to the logs collected.**

Enterprise Forensic (EF) – EF is a network-enabled investigative infrastructure that enables Cybersecurity Investigators to conduct undetected/stealth PTO-wide, in-house forensic computer investigations and hard drive (bit by bit) acquisitions over the network as well as Incident Response alerting capabilities. EF provides immediate insight and awareness to threatened systems and information. EF performs state full inspection of incoming USPTO internet traffic to detect malicious software and cyber-attack signatures.

Security and Defense (SD) – SD provides connectivity for the USPTO network to reach applications, external devices, and networks which are not located on the Alexandria campus or not controlled by the USPTO. These include the Internet, Government sites, commercial sites, and contractor sites. SD also provides secure public and trusted users access to USPTO resources and applications. SD is responsible for maintaining the security and integrity of USPTO's internal (or private) network infrastructure while providing services for the public and partners of the USPTO, remote access for USPTO staff, and connectivity to external systems and other Government agencies for USPTO staff.

Enterprise Scanner (ES) – ES provides agency-wide scanning capabilities such as vulnerability assessment, auditing compliance, configuration and patch management. ES security scan tools are used to detect software vulnerabilities and ensure that information systems are compliant to USPTO baselines. Scans are performed on a quarterly basis for all information systems as part of continuous monitoring.

Enterprise Cybersecurity Monitoring Operations (ECMO) – OMB memoranda M-10-15 and M-10-19 require all Federal agencies to continuously monitor security-related information across the enterprise and present this information to the various levels of agency-wide management to enable timely decision making. The Department of Commerce (DOC)-wide ECMO initiative fulfills this requirement, providing near real-time security status, increasing visibility into system operations, and helping security personnel make risk-management decisions based on increased situational awareness. The DOC ECMO working group includes the USPTO.

Dynamic Operational Support Plan (DOSP) – DOSP is a centralized Operational Support Plan creation and display system. When a username is entered, it pulls name, work email address, and telephone number from the Active Directory Domain (ADD). The DOSP has the capabilities of:

- Correlation, alignment, decomposition and pre-population of a product's system boundaries obtained from EMS network discovery and cybersecurity monitoring (CM) processes;
- Correlation and pre-population of a product's operational attributes based on manually entered values;
- Intake of configuration artifacts, formatted static text and images;
- Near real-time web publication and change tracking;
- Editing and viewing based on Role Based Access Controls (RBAC);
- Drafting and Approval functionality; and
- Archival ability.

DOSP uses web forms to intake product attributes provided by Technical Leads (TL) and various support groups. These values are stored in a centralized location with the EMS database. This data is then processed and aligned with the already obtained network and CM data stored within the database and is used to publish a web accessible and RBAC controlled operational view of the product.

Situational Awareness and Incident Response (SAIR) – SAIR has implemented a technology platform to provide an Enterprise Common Operational Picture (ECOP) of the operational status of enterprise systems. ECOP provides enterprise situational awareness: the monitoring of the health and performance of devices and systems supporting PTONet. The CIO Command Center (C3) provides the means from where the CIO, operational teams, Support Groups, and/or designated CIO representatives can either physically or virtually view the ECOP, a near real time status of either internal and/or selected external events, providing an enterprise-wide Situational Awareness perspective from which to make decisions. This detailed enterprise-wide visibility is derived from the monitoring of information systems (ISs) in near real time**.** This system pulls and stores data such as telephone number and IP address.

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

SCS is a general support system.

b) System location

SCS is located at 600 Dulany Street, Alexandria, VA 22314.

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

SCS is a system that utilizes its subsystems to connect with all the USPTO systems for enterprise monitoring and security operations. In addition to connecting with the Office of Networking and Telecommunications Office (ONTO) at the Herbert C. Hoover Building (HCHB), SCS also interconnects with the follow systems:

Agency Administrative Support System (AASS) is a master application that is made up of six subsystems that provide the USPTO cost-effective and reliable services such as statistical analysis, document imaging, managing and tracking hardware, software, and other IT resources.

Corporate Administrative Office Systems (CAOS) an application system that supports USPTO human resources activities including all activities associated with the recruitment and management of USPTO personnel.

Contractor Access System (CAS) is an infrastructure information system and provides off-site contractors and selected USPTO employees with limited, monitored, and secured access to PTONet applications, resources, and services.

Database Services (DBS) is an infrastructure information system and provides a database infrastructure to support mission of USPTO database needs.

Enterprise Desktop Platform (EDP) is an infrastructure information system that provides a standard enterprise-wide environment that manages desktops and laptops running on the Windows operating system (OS), providing United States Government Configuration Baseline (USGCB) compliant workstations.

Enterprise Record Management and Data Quality System (ERMDQS) is a major application consisting of one subsystem called Data Architecture Tool – Metadata (DAT-Metadata). This subsystem supports a standard-based approach to managing digital records electronically by storing metadata about a record but leaving that record in its native repository and provides a metadata management solution used for creating a centralized repository of USPTO metadata information.

Enterprise UNIX Services (EUS) is an infrastructure operating system with a sole purpose of providing a UNIX based hosting platform to support other systems at USPTO.

Enterprise Windows Services (EWS) is an infrastructure information system and provides a hosting platform for major applications that support various USPTO missions.

Consolidated Financial System (CFS) is a master system composed of the following four subsystems: Momentum, Concur Integration, E-Acquisition (ACQ), and VendorPortal. 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. Concur Integration works with Momentum and passes data back and forth between the systems using web services. ACQ provides an automated solution for the procure-to-pay process in the acquisition community at the USPTO. VendorPortal provides a platform for vendor interaction whereby USPTO may publish notices, solicitations and award announcements, etc.

Enterprise Software Services (ESS) is a major application and provides an architecture capable of supporting current software services at USPTO.

Enterprise Virtual Event Services (EVES) is an application information system consisting of three subsystems: Cisco Telepresence (CT)/ Tandberg, WebEx (WebEx), and vBrick. It enables business units to share vital knowledge through collaboration capabilities that incorporate data, voice, and video communication technologies.

Free Processing Next Generation (FPNG) provides technologies that allow changes in business rules and other configuration changes without requiring code changes.

Information Delivery Product (IDP) is a master system composed of the following three subsystems: Enterprise Data Warehouse (EDW), Electronic Library for Financial Management System (EL4FMS), and Financial Enterprise Data Management Tools (FEDMT). EDW provides a tool that allows managers and analysts to analyze business processes, resource use and needs, and other facets of the business. EL4FMS provides access to USPTO financial-related documents to support the decision-making activities of managers and analysts. FEDMT is a database/user interface solution utilizing the Oracle APEX product to build small applications to support Financial Reference data.

Information Dissemination Support System (IDSS) is a major application system and provides automated support for the timely search and retrieval of electronic text and images concerning patent applications and patents by USPTO internal and external users.

Intellectual Property Leadership Management System (IPLMSS) is a major application which groups and manages seven separate subsystems to provide tools to cull and organize large amounts of legal data, to support FOIA, Privacy Act requests and appeals, to docket and track cases, manage library content, route electronic notices, develop and maintain assessments, and to register and maintain the practitioner roster and monitor practitioner disciplinary action. IPLMSS primarily supports the USPTO Director, Deputy Director, and Office of the General Counsel (OGC).

Network & Security Infrastructure (NSI) facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO applications.

OCIO Program Support System (OCIO PSS) helps authorized USPTO personnel and contractor employees obtain the information and data needed for contract related, system requirements, test plans, test requirements, and other documents important to the OCIO-PSS personnel.

Exchange/Voice Over Internet Protocol (PBX- VOIP) is an infrastructure information system, supporting analog voice, digital voice, collaborative services, and data communications for business units across the entire USPTO.

Patent Capture and Application Processing System – Examination Support (PCAPS ES) provides processing, transmitting, and the storing of data and images to support the data-capture and conversion requirements of the USPTO patent application process.

Patent Capture and Application Processing System – Capture and Initial Processing (PCAPS IP) is a major application and provides support to the USPTO for the purposes of capturing patent applications and related metadata in electronic form; processing applications electronically; reporting patent application processing and prosecution status; and retrieving and displaying patent applications.

Patent End To End (PE2E) provides examination tools for the central examination unit to track and manage cases and view documents in text format.

Patent Search System – Primary Search and Retrieval (PSS PS) is a major application system and is considered a mission critical system. PSS PS supports the Patent Cost Center and consists of such tools as Search and Retrieval. Search and Retrieval provides a comprehensive prior art search capability and the retrieval of patent and related information, which comprise text and images of United States (US), European Patent Office (EPO) and Japan Patent Office (JPO patents), US pre-grant publications, Derwent data and IBM Technical Disclosure Bulletins.

Patent Search System – Specialized Search and Retrieval (PSS SS) is a master system and is considered a mission critical system. PSS SS provides access to highly specialized data that may include annual submissions of nucleic and amino acid sequence, prior-art searching of polynucleotide and polypeptide sequences, scientific or technology-based, Patent Linguistic Utility Service (a query by example search system), Chemical Drawing ability, Foreign Patent Data, for example.

Service Oriented Infrastructure (SOI) is a general support system and infrastructure information system that provides the underlying services for a mobile, feature-rich, and stable platform upon which USPTO applications can be deployed.

Trademark Processing System – External System (TPS ES) is a major application information system and provides customer support for processing Trademark applications for USPTO.

Trademark Processing System – Internal System (TPS IS) is an application information system and provides support for the automated processing of trademark applications for the USPTO.

Trademark Next Generation (TMNG) is a major application and provides support for the automated processing of trademark applications for the USPTO.
Trilateral Network (TRINET) is an infrastructure information system and provides secure network connectivity for electronic exchange and dissemination of sensitive patent data between authenticated endpoints at the Trilateral Offices and TRINET members.

Planning and Budgeting Products Division (PBP) is a master system composed of following three subsystems Activity Based Information System (ABIS), Analytics and Financial Forecasting (AFF), and Enterprise Budgeting Tool (EBT). ABIS streamlines and automates business processes. AFF supports the analysis of fee collection information and decision-making. EBT supports central planning and budgeting.

d) The purpose that the system is designed to serve

SCS provides near real-time enterprise monitoring and security operations for USPTO systems.

e) The way the system operates to achieve the purpose

SCS is a product of many subsystems that work together to provide an enterprise-level monitoring to USPTO's systems to include SIEM, EF, SD, ES, ECMO, DOSP, and SAIR.

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

SCS, through its subsystems, collects and stores all systems and application logs from the USPTO systems.

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

Only a subset of authorized users, such as the assigned system administrators, have access to SCS and its subsystems.

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

All users of SCS are USPTO domain users. SCS users are separated into security groups, having different levels of access based on their system role. All roles are defined and granted by the SCS System Owner (SO). Users with privileged accounts or roles with access to SCS subsystems are management, and only a subset of authorized users have access to the applications. SCS users must logon to their workstation systems prior to authenticating to any of the SCS systems. Authorized privileged users access the applications for administrative functions only, and authorized non-privileged users access some applications as required for their roles within their group.

i) How information is transmitted to and from the system

Information is transmitted to and from SCS via the internal USPTO network. The SCS system utilizes workstations, network devices, and servers to protect, monitor and scan the network while providing and ECOP to the C3 staff.

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 (version 01-2015 or 01-2017). *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 (version 01-2019 or later). *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.
Provide the legal authority which permits the collection of SSNs, including truncated form.

☒ 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

☒ I certify the criteria implied by one or more of the questions above **apply** to the **Security and Compliance Services (SCS)** and as a consequence of this applicability, I will perform and document a PIA for this IT system.

☐ I certify the criteria implied by the questions above **do not apply** to the **Security and Compliance Services (SCS)** and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Michael Blevins Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-5341 Email: Michael.Blevins@uspto.gov Signature: Users, Blevins, Michael Digitally signed by Users, Blevins, Michael Date: 2021.11.08 06:10:18 -05'00' 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 Signature: DON R Watson Digitally signed by DON R Watson Date: 2021.11.09 19:34:10 -05'00' Date signed: ______________________________
Privacy Act Officer Name: Ezequiel Berdichevsky Office: Office of General Law (G/GLO) Phone: (571) 270-1557 Email: ezequiel.berdichevsky@uspto.gov Signature: Users, Berdichevsky, Ezequiel Digitally signed by Users, Berdichevsky, Ezequiel Date: 2021.11.03 15:43:09 -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: 2021.11.12 17:05:02 -05'00' Date signed: ______________________________
Co-Authorizing Official Name: N/A Office: N/A Phone: N/A Email: N/A Signature: ______________________________ Date signed: ______________________________	