Template Version Number: 01-2021

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

## Privacy Impact Assessment
## for the
## Security and Compliance Services (SCS)

Reviewed by: Deborah Stephens, 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

Digitally signed by BRIAN ANDERSON
Date: 2025.10.29 09:25:51 -04'00'

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

# U.S. Department of Commerce Privacy Impact Assessment
# USPTO Security and Compliance Services (SCS)

**Unique Project Identifier: EIPL-SCS-01-00**

**Introduction: System Description**

*Provide a brief description of the information system.*

Security and Compliance Services (SCS) is a general support system comprised of subsystems which work together to provide enterprise level monitoring and security operations for United States Patent and Trademark Office (USPTO). The subsystems include:

Security Information and Event Management (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) – is a network-enabled investigative infrastructure that enables Cybersecurity Investigators to conduct 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) – provides connectivity for the USPTO network to reach applications, external devices, and networks which are not located on the USPTO 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) – 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) – Office of Management and

Budget (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.

Address the following elements:

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

SCS is a General Support System (GSS).

*(b) System location*

SCS is located at Alexandria, VA.

*(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:

**Archangel** is a Software as a Service (SaaS) solution that enables the USPTO to streamline cybersecurity lifecycle; Governance, Risk, and Compliance (GRC) and Continuous Diagnostics and Mitigation (CDM) by eliminating redundancy and automating the process of security accreditation via Continuous Authorization to Operate (cATO

**Agile Delivery Platform (ADP)** is an integrated software engineering development solution that includes a central artifacts repository, version control, automated compile, build, test reporting, metering, and analytics that can be built in Amazon Web Services (AWS) cloud. This allows for the continuous delivery of production ready codes to the various testing environments prior to promotion for the production deployment. ADP provides a platform that promotes a continuous automated system build in support of USPTO's Next Generation applications.

**Adobe Experience Manager (AEM-MS)** is an enterprise service for signature. The service provides signed receipts to the users for their payment. The system is deployed as a Software

as a Service (SaaS) platform with Adobe Corporation managing and maintaining infrastructure and software. The mission of the system is to provide electronic signature services as part of the enterprise services to the consumers of the USPTO systems.

**Building, Assets & Property Management (BAPM)** boundary consist of four (4) components: Radio Frequency Identification (RFID) is 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; Property & Facility Scheduling (PFS) consist of two schedulers, FLU Shot, and RoomRez and are applications used for scheduling appointments around USPTO; Emergency Notification System (ENS) is a network-based emergency notification system which provides rapid dissemination of emergency messages to USPTO personnel; and Warehouse File Tracking System (WFTS) is a tracking program used by the USPTO to track the location of each patent and trademark file as it is transported in and out of the Springfield, VA Repository.

**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.

**Corporate Administrative Office System-Cloud (CAOS-C)** will be hosted in USPTO's AWS cloud. The initial applications in the system enables eligible USPTO employees to manage their telework agreements along with the information about their primary and secondary telework sites. USPTO employee supervisors use this to review and approve employee telework sites.

**Cloudflare** via its DNS service provides protection for USPTO infrastructure by defending against DDoS attacks, ensuring data integrity through DNSSEC support using technology as well as providing content filtration and malware defense.

**Secure Access Service Edge (SASE)** that covers a number of security capabilities around increased security and network resilience capabilities to improve policy enforcement and reduce latency associated with detailed security monitoring. SASE is a SaaS implementation of Netskope's Government Cloud that focuses on 6 Security Service Edge (SSE) capabilities: Zero Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), Remote Browser Isolation (RBI), Secure Web Gateway (SWG), Firewall as a Service (FWaaS), and Software Defined Wide Area Network (SD-WAN).

**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.

**CredPriv-ICAM-CredMGMT (CredPriv):** The USPTO uses SailPoint Lifecycle Management (LCM) also known as ICAM-CredMGMT through Continuous Diagnostics and Mitigation (CDM), to manage USPTO privileged users access to devices and users credential workflow. USPTO integrates ICAM-CredMGMT components to incorporate and correlate data into the Master User Record (MUR) for reporting to a centralized SailPoint IIQ at NIST/DOC.

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

**Data Storage Management System (DSMS)** is a General Support System (GSS) which 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.

**DA-DDS-Data Delivery Application (DDS)** was developed to manage lists of code values. Although DDS can maintain any list of codes, the primary use has been to manage lists of Country Codes and geographic territories. DDS acts as a backend service AIS to provide standard PTO country and geo-region data for patent applications.

**Enterprise Data Services-Databricks (EDS-DBX)** Databricks provides tools for the Big Data Reservoir (BDR) application to perform data processing and Machine Learning initiatives against datasets to support the agency mission. It performs analysis and studies massive amounts of data.

**DS-ID-AUTH Identity Management Authenticator (ID-AUTH)** is an application information system that provides personalization and issuance of the smart card identification credentials under HSPD-12. ID-AUTH consists of the following two (2) sub-systems: Card Management System (CMS) and Internal Public Key Infrastructure-Smart Card (IPKI/SC).

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

**Enterprise Gateway Services (EGS)** is comprised of the Layer7 API Gateway (GWs) by Broadcom and is leveraged as a specialized tool for API management at USPTO. The tool efficiently controls APIs, bolsters application security, and streamlines integration across diverse systems. Its pivotal role lies in ensuring the availability, reliability, and performance of services, pivotal for our digital endeavors' success.

**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 procureto- 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.

**CCE-CXM-Qualtrics XM (CXM)** primary function is to display surveys and capture qualitative and quantitative user feedback from websites/applications. The capture mechanisms are on page initiated (javascript) or standalone. The Qualtrics platform provides data analysis, insights, and reporting capabilities. This SaaS product is widely used in federal government (including Commerce), and has 22 listed prior authorizations.

**Compute Historical Analytics and Reporting Tools (CHART)** is composed of multiple major tools in CHART are DIAMOND, LSM, CBO, DIME, and COIN. CHART provides technical and financial analyst staff members at USPTO with a single, unified view of all hosts, both on-premises and cloud, and storage assets managed by the Infrastructure and Hosting Services Division (IHSD) of the Enterprise Infrastructure Delivery Office (EIDO). A growing amount of AWS cloud storage is also contained within DIAMOND.

**Chatbot Cloud (Chatbot-C)** is an online helpdesk that responds to customer questions without human interaction. It provides the following benefits and capabilities:

- 24/7/365 Service: Ability to operate without human help 24 hours a day, 7 days a week, 365 days a year
- Convenience: New communication channel utilizing Artificial Intelligence (AI)/Machine Learning (ML) and the latest technology to understand and respond to customer questions accordingly
- Customer Insight Gathering: Quickly identify trends to better address customer concerns

**Customer Interaction Platform (CIP-SF)** is a cloud-based Software as a Service (SaaS) Customer Relationship Management application that provides functionality focused on events management, event registration, customer service and analytics. USPTO CIP-SF system, also known as Salesforce, provides a customer relationship management and event management service to the USPTO and its customers. CIP-SF primary focus is to manage and log customer inquiries, including all actions taken by the business units to resolve the service request.

**Collection of Multiple Enterprise Tools (COMET)** is a collection of independent applications that live on the ORACLE's Application Express (APEX) lightweight database. A majority of the applications within COMET do not collect, use or maintain any additional BII or PII other than the general information that comes from the interconnections with USPTO Microsoft Azure Cloud Services (UMACS).

**Crowdstrike** enables the USPTO to identify unknown malware, detect zero-day threats, identify advanced adversaries, and prevent damage from targeted attacks in real-time. Crowdstrike relies on its Falcon Platform, a redundant and highly scalable and secure cloud architecture, that correlates intelligence and security events in real-time from its global network of agents, and provides an advanced level of insight into adversary activities and business impact from their attacks. The Crowdstrike Endpoint Detection and Response (EDR) agents which are installed on endpoints look at operating systems, processes, network and behavioral activities to identify anomalies.

**The Digital Media System (DMS)** is an Infrastructure information system, and provides a communication foundation for multimedia professionals that allows for real time training and collaboration on large projects. Such efforts include, but are not limited to video, audio, animation, and photography. In addition, this system allows USPTO DMS multimedia professionals to download recorded videos from local cameras and download system firmware from the Internet, and anti-virus and software to accomplish business objectives.

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

**E-Discovery Software System - Cloud (EDSS-C)** is a commercial e-Discovery SaaS (Software as a Service) implemented with RelativityOne for Government. This SaaS provides for the Collection, Processing, Review, Analysis, and Production phases of the EDRM (Electronic Discovery Reference Model). Attorneys and litigation support personnel employ the tool in a variety of legal matters to help organize, search, and review large volumes of Electronically Stored Information (ESI).

**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.

**Executive Document Management System Cloud (EDMS-C)** is an application information system, and is used by the Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office to receive and respond to a wide range of official correspondence, by electronically capturing, routing, and tracking both incoming and response documents, thereby improving workflow.

**Enterprise Management System (EMS**) provides for automated, proactive system management, and service-level management for application and database servers. The EMS AIS supports high availability for all the USPTO servers and AIS software including MicroFocus Operations Bridge Manager, OpenNMS, Prometheus, Grafana, and Netdata. This software provides EMS with the capabilities to perform automatic network device discovery, availability (up/down) monitoring, network mapping, data collections, reporting, and a centralized console to perform event correlation and alerting.

**Fee Processing Next Generation (FPNG)** system is the fee management and revenue collection system at USPTO. FPNG provides the following four main categories of functionality: User presentation, Core accounting, Reporting and Fee Processing Common Web Services.

**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.

**International Data Exchange – MODERATE (IDE-M)** comprise of applications and services that help exchange published and unpublished application data with international stakeholders that include foreign IPO's.

1. CPC-INTL is a web-based application used to exchange, update and retrieve CPC classification data between EPO and USPTO.
2. CPC-IP OCT is an information system that is a shared repository for all patent schemed approved by USPTO and EPO.
3. CPC-CDS is a web-based application that maintains current patent classification information for USPTO.
4. GD is a web-based application that allows internal and external users to access global dossier services and view foreign IP office published patent application dossier contents via public web page.
5. CPC Auto-Classification provides an AI based service to reduce/replace the current manual classification functions.

**ICAM Identity as a Service (ICAM IDaaS)** provide an enterprise authentication and authorization service to applications/AISs. As part of the enterprise services, the system provides; user provisioning and life cycle management, user roles and entitlement management, user authentication and authorization to protected resources as well as application integration/protection.

**Intellectual Property Assignment System (IPAS)** allows for electronic assignment of a patent or trademark via a website. Users are able to create an assignment document, fill in all required data, and attach required supporting legal documents. This is a document management workflow system that supports the processing of assignment documents through electronic submission, image capture, OCR text capture, automated workflow processing, management and inventory reporting and generation of computer output microfilm of recorded documents from electronic images.

**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).

**Integrated Automations (IA)** platform provides the necessary infrastructure to host the Integrated Automations technology solution in development, test, and production environments. The platform allows USPTO users to configure “robot” - a computer software – also referred to as BOTs to emulate and integrate the actions of a human interacting within digital systems to execute a business process.

**Legal Document Management System - Cloud (LDMS-C)** is a commercial SaaS (Software as a Service) implemented with FedRAMP Authorized NetDocuments software. This SaaS will support the Office of the General Counsel's (OGC) document management requirements as they provide advice to USPTO clients on the full range of federal agency legal issues: fiscal, procurement, rulemaking, administrative law, labor and employment, and information law. The system provides a centralized repository for easy storage, search, and retrieval of documents relating to legal matters.

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

**MyUSPTO Cloud** program intends to provide a single interface across the USPTO for users to register with the USPTO, house their correspondence information, interact with the office, manage their intellectual property portfolios, and access USPTO technology services based on their roles using a login with a single username.

**M365** product of the Enterprise Infrastructure Product Line (EIPL) provides communication and collaboration tools and services using Microsoft Office 365.Microsoft Office 365 provides support and is responsible for the core infrastructure of Office 365 including Exchange Online, SharePoint Online, OneDrive, TEAMS, Office Services. Each Service Team is responsible for the configuration and feature settings within their perspective Service.

**Madrid International Trademark System (MITS)** assists the Office of Trademark in sending, receiving, reviewing and verifying data from International Bureau (IB)-related to international applications that are being handled by the USPTO as governed by the Madrid Protocol. The business mission will be enabled through a technical approach of cloud-native infrastructure and DevSecOps pipelines that will enable cost-conscious elastic scalability and quick turnaround time of features and business rule changes utilizing continuous integration and deployment.

**Master Data Management (MDM)** system is comprised of a FedRAMP authorized Software as a Service (SaaS) suite and Collibra Data Intelligence Cloud (CDIC). CDIC is a platform in which USPTO internal users can build their own data governance management system. This platform includes user management, privilege management, data catalog, workflows, and data stewardship. The CDIC platform ingests metadata, and authorized users are responsible for managing and controlling the permission and policies surrounding the data. The tool allows users to store and track metadata, create dashboards, create a business glossary, capture an inventory of reports, and use workflows to manage their data.

**Office of Enrollment and Discipline Item Bank-Cloud (OEDIB-C**) is a FedRAMP Authorized Software as a Service (SaaS) product implemented with Question mark OnDemand

for Government (OD4G). OEDIB-C is used by the Office of Enrollment and Discipline (OED) staff to develop and maintain exam content for the Attorney and Agent Registration Exams.

**OCCO-WEB** provides the public, internal and key stakeholders with information from USPTO about all aspects of intellectual property. It serves as the main web-based information dissemination channel for the Agency and provides links to public-facing, web-based applications used to conduct the Agency's day-to-day operations at www.uspto.gov. It also includes USPTO's corporate intranet website, PTOWeb serving as the primary internal communication, information dissemination and collaboration system for employees and contractors.

**Open Data/Big Data Master System (OD/BD MS)** consists of subsystems which support the Big Data Portfolio. OD/BD resides on the UACS platform, which employs IaaS and PaaS services from AWS. The current subsystems under this master system consists of Big Data Reservoir (BDR)/Data Modeling Tool (DMT), Developer Hub (DH)/Open Data Portal (ODP), Collection of Economic Analysis Tools (COEAT) and Bulk Data Storage System (BDSS).

**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 Administrative Center (PAC)** provides central tracking and recording of patent application status and bibliographic data; and its components will directly support the administration of the application processing lifecycle by facilitating the scanning of application documents, initialization of new patent applications, review of security, formality, document & fee requirements; automated routing of applications; generation, review and mailing of official correspondence to applicants; tracking examiner productivity; and the publication and issuing of patents

**Patent Business Management Information (PBMI)** is a master system portfolio consisting of a collection of automated information systems (AIS) under the Patents product line. The goal of PBMI is to facilitate and support examiner production, quality assurance, and report dissemination to USPTO employees and contractors. PBMI provides access to easy-to-acquire validated data and metrics. PBMI will contain the following subsystems: Patents Reporting Oversight (PRO) which has a collection of daily-created denormalized tables that effectively makes reporting more efficient and reliable and Web, Marketing and Communications (WMC) which is collection of web services/applications providing business solutions to Patents and/or to the enterprise.

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

**PE2E-DAV Docket Application Viewer (DAV)** provides the Patent Examiners with tools to facilitate the examination of cases and help store, track, and receive case-based knowledge and state information as the examiner accumulates it. DAV ensures that the solution provides value to the wider audience of patent examiners; implements a stable architectural framework using SOA-based principles that allows for the modular addition and modification of well-defined components and services while allowing the system to change as needed over time without significant overhauls.

**Patent Exam Center (PEC)** allows the USPTO Patent Examiners the ability to search U.S. patent documents in the USPTO databases. The PEC application is deployed in Amazon Web Services (AWS) and operates in an AWS virtual private cloud (VPC). It is a standalone application that interface with other USPTO information systems like PSAI, DAV and OC. The patent text and image data provided to the patent examiners is a replica of examiner search collections used internally in USPTO.

**Patent Public Search system (PPUBS)** is a custom developed application information system provided by USPTO to replace legacy public search systems with a unified search system. PPUBS is a simplified version of PE2E Search used by patent examiners internally within USPTO and is deployed and operating in the cloud for public use. The Patent text and image data provided to the public is a replica of examiner search collections used internally in USPTO.

**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.

**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.

**Public & Enterprise Wireless Local Area Network 2 (PEWLAN2)** is a is a productivity enhancer for the mobile staff, guests, and contractors. A smoothly implemented wireless LAN facilitates secure wifi network connectivity from anywhere within the organization's spaces. It also provides simple flexibility for cube-sharing, hoteling, and other situations where staff move around and the number of network connections varies over time. Staff with wireless connectivity may not need or even want docking stations, reducing cost and equipment clutter. The USPTO enterprise system is designed to provide not only secure access to PTONet, but to provide guest access outside of the secure boundary using the same infrastructure.

**Patent Search Artificial Intelligence (PSAI)** is a platform used to provide Patent End-to-End (PE2E) Search process with AI capabilities allowing Patent Examiners to perform searches faster, identify more relevant search results, and in a high-compute and secure cloud environment hosted in Google Cloud Platform (GCP). The GCP cloud environment is comprised of several sub-components including, Containers/Compute, Databases & Storage, Cloud Network, Management, Operation and Development Tools.

**Patent Trial and Appeal Case Tracking (P-TACTS)** is an application information system and provides supporting USPTO's administrative law body Patent Trial and Appeal Board for electronically filing documents in connection with the proceedings established under the Leahy-Smith America Invents Act (AIA). The objective of P-TACTS is to meet its statutory obligations under AIA, the USPTO Strategic Goal of Optimizing Patent Quality and Timeliness and improving the post-Grant Processes. P-TACTS also now addresses or handles Pre-grant Appeals and Interferences.

**Performance Monitoring Tools Amazon Cloud Services (PMTACS)** maintains the Instana COTS product to provide application visibility (i.e. Instana encompasses enterprise observability, automatic application performance monitoring, end-user monitoring/website monitoring and hybrid/multi-cloud monitoring. Instana automates monitoring and tracing for all applications and services by monitoring every service and tracing every request.) to USPTO product teams. The Instana implementation utilizes servers provided by AWS Cloud Services (UACS). All users of Instana are internal USPTO personnel.

Performance Monitoring Tools (PMT) utilizes a number of COTS products used by the Systems Performance Branch (SPB) to:

• Analyze USPTO-developed applications and PTONet Network performance to ensure performance objectives are being met.
• Establish and implement monitoring standards.
• Monitor existing capacity and projects future capacity requirements.
• Formulate performance improvements and capacity changes.
• Recommends changes to systems, java virtual machines, databases, and PTONet to optimize application experience.
• Compile capacity and performance statistics for executive level reporting.

SPB is responsible for working with Systems Development Staff on architecting a standard performance monitoring and metric reporting system, as well as its upkeep and daily use within the CIO Command Center.

**Reference Document Management Services (RDMS) system** is designed to serve as USPTO's enterprise-wide content management solution for reference and guidance documents – a critical tool for patent and trademark examiners and applicants. The current RDMS system allows intranet web-based access to Manual for Patent Examination Procedures (MPEP) and the Trademark Manual for Examination Procedures, the primary guidance document utilized by Patent and Trademark examiners. RDMS was just recently upgraded to allow public internet access to applicants who wish to submit patent and trademark applications.

**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.

**Storage Infrastructure Information Service (SIMS)** is a system that provides access to consolidated, block level data storage and files system storage. SIMS is primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes. It is accessible to servers so that the devices appear like locally attached devices to the operating system. SIMS has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

**Service Management Platform (SMP)** is a cloud-based IT services management (ITSM) tool that provides a single system of record for IT services, operations, and business management by automating IT service applications and processes. USPTO uses the 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. 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.

**Trademark Common Services (TM-CMC-C)** is a project comprising of TM Common CMS and TM Common DSM. TM-CMC-C is hosted on AWS cloud infrastructure. TM Common DSM provides data managements services and TM Common CMS provides content management services to Trademark applications. The TM-CMC-C application supports content migration and provides content management services in the AWS cloud environment. The system's objective is to be the consolidated repository for all Trademark filing documents, registrations, mark images, multimedia files, TTAB proceeding documents, and TTAB FOIA documents.

**Trademark Exam (TM-EXM)** is a center where trademark attorneys and professional staff have the ability to securely login and complete end-to-end review and processing of trademark applications/registrations. Trademark Exam provides the ability to manage workload, conduct searches of multiple databases, update/change application/registration data, communicate with internal business units and with applicants/registrants, check and update application/registration statuses, and process fees and refunds.

**Trademark Trial and Appeal Board Center (TTABC)** system boundary consists of two components: TTABC and Trademark Trial and Appeal Board Reading Room (TTAB Reading Room/TTABRR). The TTAB Center is an application information system and provides an online interface for USPTO customers to submit forms to the Trademark Trial and Appeal Board (TTAB) electronically. Using a Web-based interface, TTAB public customers can complete and submit these trademark forms electronically over the Internet. The TTAB application form is for general public, who can also be customers, to complete on-line and submit to the USPTO.

**USPTO-AINS eCase SaaS System (UAECSS)** is a tool for managing the processing of FOIA and Privacy Act requests and appeals submitted to the USPTO. This SaaS provides a correspondence capability to generate, send, and store correspondence with requesters and program offices. The system provides a document management capability to store, review, and redact documents for delivery to requesters.

**UACS-USPTO AWS Cloud Services (UACS)** is an infrastructure platform used to support PTO Product Team Components hosted in the AWS East/West environment. The AWS East/West environment is comprised of several sub-components including, Virtual Private Cloud (VPC), Elastic Cloud Computing (EC2), Identity and Authentication Management (IAM), and Simple Storage Service. below and further in the AWS East/West IaaS SSP.

**USPTO Google Cloud Services (UGCS)** is a standard infrastructure platform used to support the USPTO's Patent Search AI System, USPTOs future AI/ Auto ML systems, and other USPTO Tenants, hosted in the Google Cloud Platform (GCP) us-east4, Northern Virginia, environment. The GCP us-east4 environment is comprised of several sub-components including, Virtual Private Cloud (VPC networks), Cloud Computing (GCP Compute Engine), Identity and Authentication Management (IAM), and resilient cloud storage (GCP Cloud Storage).

**USPTO MS Azure Cloud Services (UMACS)** is the cloud infrastructure platform used to support USPTO Application Information Systems hosted in the Azure East/West environment. It provides administrative efficiency, improves security, and provides better oversight across all applications which reside on the UMACS platform. The system provides a central location for where all USPTO Azure applications can be operated, managed, and monitored.

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

SCS is a product of 5 subsystems, SIEM, EF, SD, ES and ECMO that work together to provide an enterprise-level monitoring and security operations for USPTO's systems.

*(e) 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. Users with privileged accounts or roles with access to SCS subsystems are management and only a subset of authorized users who 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.

*(f) 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 Enterprise Cyber Operations Platform (ECOP) data such as system logs, alerts and monitoring results to the CIO Command Center staffs for centralized visibility and threat analysis.

*(g) Any information sharing*

SCS integrates with both the physical and logical access control systems to ensure the USPTO facilities and information systems are accessed by authorized personnel. Information may be shared case-by-case within the bureau, with DOC bureaus, and other federal agencies.

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

Citation of the legal authority to collect PII is 5 U.S.C. 301 and 35 U.S.C.2; EO 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information.

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

The FIPS 199 security impact category for the system is 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: | | | | | |

| **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. Sex | ☐ | 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): username | | | | | |

| **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)** |
|---|
| Anything that is saved and stored on a USPTO computer could become ad hoc PII or BII saved, stored, transmitted and would be the possession of USPTO until retention period ends, SCS may have access to this information. |
| |

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.

| |
|---|
| SCS ensures the information is accurate by obtaining the information directly from the individual with whom the information pertains. 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 screening. 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.<br>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): 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).

The information in this system is about federal employees and contractors and is used for administrative matters, litigation, and for intelligence activities.

Administratively, SCS-SIEM receives servers and applications logs within the USPTO. The logs contain system events and audit records. The logs are collected for security, events monitoring, and after-the-fact investigations. SIEM retains the logs for a least 90 days before they are backed up by the USPTO backup system and maintained for three years. The incidental presence of any of the PII identified in section 2.1 could be from a federal employee/contractor.

In terms of litigation and intelligence activities, SCS-EF collects hard drive images of a user's government issued laptop on an ad-hoc basis, or whenever there is a cyber and legal

requirement. The laptops may contain PII/BII about USPTO employees, contractors, and/or members of the public. The hard disk image could possibly contain any of the items on 2.1 that a user has stored on the government issued laptop. The contents of a hard drive, while it is being extracted, stay within the USPTO network boundary. The "image" is stored on servers which can only be accessed by a certain few individuals within cybersecurity (six total), for which they have their own firewall and the physical server has its own server rack lock. The USPTO Cybersecurity investigations keep possession of the "image" until the case closes. Once an investigation case has closed, any potential PII data identified in section 2.1 is destroyed. The incidental presence of any of the PII identified in section 2.1 could be from a federal employee/contractor.

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.)

In the event of computer failure, insider threats, or attack against the system by adversarial or foreign entities, any potential PII data from USPTO employees or contractors stored within the system could be exposed. System users undergo annual mandatory training regarding appropriate handling of information. Physical access to servers is restricted to only a few authorized individuals. The servers storing the potential PII are located in a highly sensitive zone within the USPTO internal network and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved an authorized account. The USPTO has the SIEM system that monitors in real-time all activities and events within the servers storing the potential PII data and a subset of USPTO C3 personnel review audit logs received on a regular bases and alert the ISSO and or the appropriate personnel when inappropriate or unusual activity is identified.

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 adhere to the USPTO Records Management Office's Comprehensive Records Schedule or the General Records Schedule and the corresponding disposition authorities or citations.

## 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.<br>Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:<br><br>All systems listed in the interconnections section c.<br><br>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 the privacy policy. The privacy policy can be found at: https://www.uspto.gov/privacy-policy | |
| ☒ | Yes, notice is provided by other means. | Specify how: This PIA serves as notice |
| ☐ | 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 of USPTO systems do not have the opportunity to decline to provide PII once they agree to become an employee. |

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: Individuals do not have the opportunity to consent to particular uses of their PII/BII in this system as it is required for the purpose of this system. |

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: SCS is used for incidence response within the USPTO, and the incidence response member can review and update their information (telephone number). |
| ☒ | No, individuals do not have an opportunity to review/update PII/BII pertaining to them. | Specify why not: All other individuals PII can be updated with Office of Human Resources |

## 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.<br>Explanation: Audit Logs |
| ☒ | The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.<br>Provide date of most recent Assessment and Authorization (A&A): 10/1/2024<br>☐ 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 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). |
| ☒ | 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).*

Information in SCS is secured using appropriate administrative, physical, and technical safeguards in accordance with the applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

The servers with the potential PII are located in a highly sensitive zone within the USPTO internal network, and logical access is segregated with network firewall and switch through Access Control List that limits access restricted to only a few approved and authorized accounts. The USPTO has SIEM systems that monitor in real-time all the activities and events within the servers with the potential PII, and a subset of authorized USPTO C3 personnel review audit logs received on a regular basis and alert the ISSO and/or the appropriate personnel when inappropriate or unusual activity is identified. Access is restricted on a "need to know" basis, utilization of Active Directory security groups to segregate users in accordance with their functions and the TACACS+ servers for authentication, authorization, and accounting. All physical entrances to the datacenter are monitored through electronic surveillance equipment. The hosting facility is supported by 24/7 onsite hosting and network monitoring by trained technical staff. Physical security controls include indoor and outdoor security monitoring and surveillance; badge and picture ID access screening; and pin code access screening. All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. All users with access to the applications have been vetted and authorized by the System Owner, and the USPTO maintains an audit trail to identify authorized or unauthorized access.

For SCS – EF, individuals with the roles to capture image from hard drive for forensics investigation follow the chain of custody to ensure the potential PII data at rest is encrypted within the system, and that only authorized personnel have the authorization to access it. Personnel given roles in the SIEM system must be approved by the USPTO and complete training specific to their roles to ensure they are knowledgeable about how to protect potential personally identifiable information.

## 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."

| | |
|---|---|
| ☒ | PAT-TM-17, USPTO Security Access Control and Certificate Systems<br><br>Commerce/Dept-13: Investigative and Security Records<br><br>Commerce/DEPT-25: Access Control and Identity Management System<br><br>Commerce/Dept-27: Investigation and Threat Management Records |
| ☐ | 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.)*

General Records Schedules (GRS) | National Archives

| | |
|---|---|
| ☒ | There is an approved record control schedule.<br>Provide the name of the record control schedule:<br>Non-recordkeeping copies of electronic records, GRS 5.1:020<br><br>GRS 3.1: General Technology Management Records<br>Item - 020 Information technology operations and maintenance records.<br>Which include access and audit logs.<br><br>GRS 3.2. Information Systems Security Records, Item 010, 020, 030. 031. 040, 050<br>Which include system security logs. and access logs |
| ☐ | No, there is not an approved record control schedule.<br>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:<br>The information such as Name, address, phone number, and email captured by the SCS could identify an individual. Other types of information can be collected by this system incidentally if the user of the system downloads and saves other PII on their system. |
| ☒ | Quantity of PII | Provide explanation:<br>Although SCS systems were not developed to collect PII data, there is a potential for PII data to be included over time within the logs collected by the systems. The collection of PII is large enough to be of concern since the systems monitors all PTO employees and provides information on requests to authorized business units. |
| ☒ | Data Field Sensitivity | Provide explanation:<br>Combination of name, address, phone number, email, and additional crash dump data will make the data fields more sensitive. |
| ☒ | Context of Use | Provide explanation:<br>The SIEM subsystems collect application logs which contain system events and audit records. Data from the logs are the management and the monitoring of the information systems. The EF application is used for the acquisition of any hard drive (bit by bit) image. Hard drive images are captured when necessary for PTO-wide, in-house forensic computer investigations. SAIR is used for incidence response within the USPTO and telephone numbers are used to contact personnel that are part of the USPTO incidence response team. |
| ☒ | Obligation to Protect Confidentiality | Provide explanation:<br>Based on the data collected, USPTO must protect the PII of each individual in accordance with the Privacy Act of 1974 which prohibits the disclosure of information from a system of records absent of the written consent of the subject individual. |

| | | |
|---|---|---|
| ☒ | Access to and Location of PII | Provide explanation:<br>The servers storing the potential PII are located in a highly sensitive zone within the USPTO internal network and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved an authorized account. 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. |
| ☐ | 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.)

| |
|---|
| In the event of computer failure, insider threats, or attack against the system, any potential PII data from USPTO employees or contractors stored within the system could be exposed. System users undergo annual mandatory training regarding appropriate handling of information. Physical access to servers is restricted to only a few authorized individuals. The servers storing the potential PII are located in a highly sensitive zone within the USPTO internal network and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved an authorized account. The USPTO has the SIEM system that monitors in real-time all activities and events within the servers storing the potential PII data and a subset of USPTO C3 personnel review audit logs received on a regular bases and alert the ISSO and or the appropriate personnel when inappropriate or unusual activity is identified. |

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.<br>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.<br>Explanation: |

| | |
|---|---|
| ☒ | No, the conduct of this PIA does not result in any required technology changes. |