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: Henry J. Holcombe, Bureau Chief Privacy Officer

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry
Date: 2022.12.21 16:23:41 -05'00'

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 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.

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.

(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:

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.

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.

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 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 Servers (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.

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.

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.

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.

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) promotes 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.

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 (PEWLAN) is an infrastructure system that facilitates secure network connectivity from anywhere within the organization's space. 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.

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.

WWW.USPTO.GOV-Cloud is the Corporate Web Site system which includes the main public USPTO Web servers and the internal Drupal content management system enabling the production and publication of content.

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

SCS is a product of 7 subsystems, SIEM, EF, SD, ES, ECMO, DOSP, and SAIR that work together to provide an enterprise-level monitoring of 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 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 and ECOP to the C3 staff.

(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. Gender	☐	k. Telephone Number	☒	r. Criminal Record	☐
e. Age	☐	l. Email Address	☒	s. Marital Status	☐
f. Race/Ethnicity	☐	m. Education	☐	t. Mother's Maiden Name	☐
g. Citizenship	☐	n. Religion	☐		
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	☒	e. Work Email Address	☒	i. Business Associates	☐
b. Job Title	☒	f. Salary	☐	j. Proprietary or Business Information	☐
c. Work Address	☒	g. Work History	☐	k. Procurement/contracting records	☐
d. Work Telephone Number	☒	h. Employment Performance Ratings or other Performance Information	☐		
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	☐	f. Scars, Marks, Tattoos	☐	k. Signatures	☐
b. Palm Prints	☐	g. Hair Color	☐	l. Vascular Scans	☐

c. Voice/Audio Recording	☐	h. Eye Color	☐	m. DNA Sample or Profile	☐
d. Video Recording	☐	i. Height	☐	n. Retina/Iris Scans	☐
e. Photographs	☒	j. Weight	☐	o. Dental Profile	☐
p. Other distinguishing features/biometrics (specify): Photographs may be part of the employees or contractors email profiles but this is a voluntary action.					

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)
Although SCS is not designed to save certain PII, anything that is saved and stored on a USPTO computer could become ad hoc PII saved, stored, etc. and would be the possession of USPTO until retention period ends.

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 is secured using appropriate administrative, physical and technical safeguards in accordance with the NIST security controls (encryption, access control, auditing). Mandatory IT Awareness and role-based training is required for staff who have access to the system and addresses how to handle, retain, and dispose of data. All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access and changes as part of verifying the integrity of data.

2.4 Is the information covered by the Paperwork Reduction Act?

☐	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
☒	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards	☐	Biometrics	☐
Caller-ID	☐	Personal Identity Verification (PIV) Cards	☐
Other (specify):			

☒	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	☐	Building entry readers	☐
Video surveillance	☐	Electronic purchase transactions	☐
Other (specify): Click or tap here to enter text.			

☒	There is 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.

SCS-SAIR provides a template for its personnel that are part of the USPTO incidence response team to provide their contact information (telephone number). The incidence response users have the opportunity to accept or decline to provide their personal telephone number. Only USPTO members of the incidence response team have access to any incidence response member's contact information. The telephone number 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 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.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	☒	☐	☐
DOC bureaus	☒	☐	☐
Federal agencies	☒	☐	☐
State, local, tribal gov't agencies	☐	☐	☐
Public	☐	☐	☐
Private sector	☐	☐	☐
Foreign governments	☐	☐	☐
Foreign entities	☐	☐	☐
Other (specify):	☐	☐	☐

☐	The PII/BII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

☐	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☒	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.

☐	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

☒	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: 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.
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	☐	Government Employees	☒
Contractors	☒		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

☒	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
☒	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.uspto.gov/privacy-policy	
☒	Yes, notice is provided by other means.	Specify how: See appendix A: Warning Banner
☐	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. They consent to the banner shown on logging into their PTO systems and they can limit what they save and download on their computer system to control how much personal data PTO has access to.

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: SCS is used for the acquisition of any hard drive (bit by bit) image for in-house forensic computer investigations. It has the potential to store such PII data if they are included within the data being captured through the logs or image capture. Because of the nature of how the data is collected, users do not have the opportunity to consent to particular uses of their PII/BII.

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. Explanation: Only authorized users have access to SCS-SIEM, which collects the USPTO log files. Only authorized users have access to SCS-EF, which collect forensic data on USPTO computers. Users access

	those applications using their USPTO domain credentials, and all the user's actions are recorded, tracked and monitored.
☒	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 9/12/2022 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
☒	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
☒	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
☒	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☐	Contracts with customers establish DOC ownership rights over data including PII/BII.
☐	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
☐	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

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."

☒	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: PAT-TM-17, USPTO Security Access Control and Certificate Systems PAT-TM-3: Employee Production Records Commerce/Dept-13: Investigative and Security Records Commerce/Dept-18: Employees Personnel Files Not Covered by Notice of Other Agencies Commerce/DEPT-25: Access Control and Identity Management System 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.)*

☒	There is an approved record control schedule. Provide the name of the record control schedule: Non-recordkeeping copies of electronic records, GRS 5.1:020 Computer security incident handling, reporting, and follow-up reports, GRS 3.2: 020 System and data security records, GRS 3.2: 010 System Access Records, GRS 3.2:030 and 031
☐	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
☒	Yes, retention is monitored for compliance to the schedule.

☐	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	☒	Overwriting	☒
Degaussing	☐	Deleting	☒
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

☐	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
☒	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
☐	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

☒	Identifiability	Provide explanation: The 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: 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: Combination of name, address, phone number, email, and additional crash dump data will make the data fields more sensitive.
☒	Context of Use	Provide explanation: 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: 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: 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.

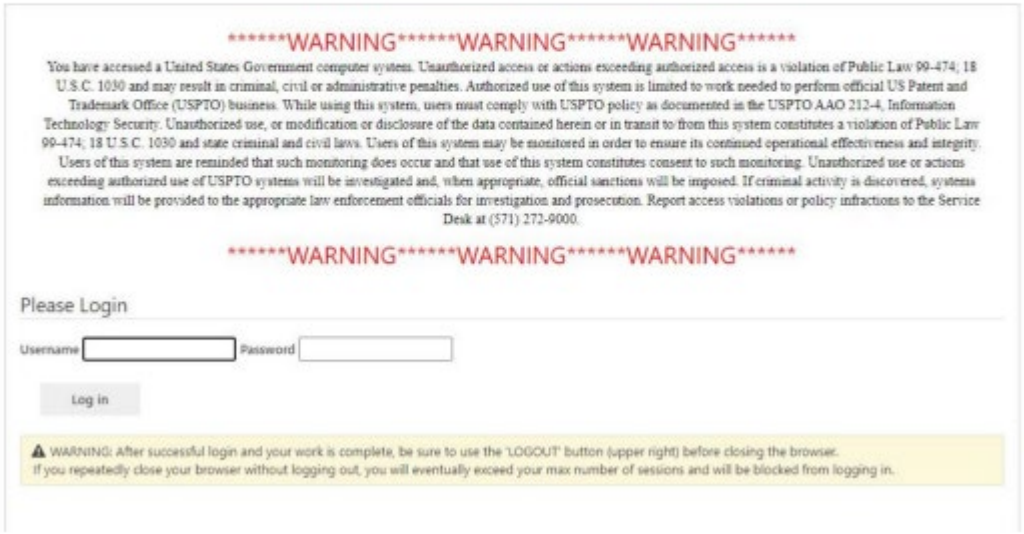
☐	Yes, the conduct of this PIA results in required business process changes. Explanation:

☒	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

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

Appendix A: Warning Banner



******WARNING******WARNING******WARNING******

You have accessed a United States Government computer system. Unauthorized access or actions exceeding authorized access is a violation of Public Law 99-474; 18 U.S.C. 1030 and may result in criminal, civil or administrative penalties. Authorized use of this system is limited to work needed to perform official US Patent and Trademark Office (USPTO) business. While using this system, users must comply with USPTO policy as documented in the USPTO AAO 212-4, Information Technology Security. Unauthorized use, or modification or disclosure of the data contained herein or in transit to/from this system constitutes a violation of Public Law 99-474; 18 U.S.C. 1030 and state criminal and civil laws. Users of this system may be monitored in order to ensure its continued operational effectiveness and integrity. Users of this system are reminded that such monitoring does occur and that use of this system constitutes consent to such monitoring. Unauthorized use or actions exceeding authorized use of USPTO systems will be investigated and, when appropriate, official sanctions will be imposed. If criminal activity is discovered, systems information will be provided to the appropriate law enforcement officials for investigation and prosecution. Report access violations or policy infractions to the Service Desk at (571) 272-9000.

******WARNING******WARNING******WARNING******

Please Login

Username Password

Log in

⚠ WARNING: After successful login and your work is complete, be sure to use the 'LOGOUT' button (upper right) before closing the browser.
If you repeatedly close your browser without logging out, you will eventually exceed your max number of sessions and will be blocked from logging in.

Points of Contact and Signatures

System Owner
Name: Michael Blevins
Office: Office of the Chief Information Officer
Phone: (571) 272-5341
Email: Michael.Blevins@uspto.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: Users, Blevins, Michael Digitally signed by Users, Blevins, Michael Date: 2022.12.07 06:28:42 -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

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: Users, Watson, Don Digitally signed by Users, Watson, Don Date: 2022.12.20 15:29:55 -05'00'

Date signed: _____

Privacy Act Officer
Name: Ezequiel Berdichevsky
Office: Office of General Law (O/GL)
Phone: (571) 270-1557
Email: Ezequiel.Berdichevsky@uspto.gov

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

Signature: Users, Berdichevsky, Ezequiel Digitally signed by Users, Berdichevsky, Ezequiel Date: 2022.12.15 11:45:52 -05'00'

Date signed: _____

Bureau Chief Privacy Officer and Authorizing Official
Name: Henry J. Holcombe
Office: Office of the Chief Information Officer (OCIO)
Phone: (571) 272-9400
Email: Jamie.Holcombe@uspto.gov

I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.

Signature: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2022.12.21 16:24:12 -05'00'

Date signed: _____

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

I certify that this PIA accurately reflects the representations made to me herein by the System Owner, the Chief Information Security Officer, and the Chief Privacy Officer regarding security controls in place to protect PII/BII in this PIA.

Signature: _____

Date signed: _____

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.