Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Network and Security Infrastructure (NSI)

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: 2026.03.10 07:18:13 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Network and Security Infrastructure (NSI)

Unique Project Identifier: EIPL-IHSN-01-00

Introduction: System Description

Provide a brief description of the information system.

The Network and Security Infrastructure (NSI) is an Infrastructure information system, and provides an aggregate of subsystems that facilitates the communications, secure access, protective services, and network infrastructure support for all United States Patent and Trademark Office (USPTO) IT applications. NSI is made up of network switch and router network infrastructure and supporting servers and COTS appliances that help users connect with all other internal USPTO systems.

Address the following elements:

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

NSI is a general support system

(b) System location

NSI reside at the USPTO facilities in the states of Virginia, Michigan, Colorado, California, and Texas.

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

NSI interconnects with the following systems:

USDA National Finance Center (NFC) Payroll/Personnel System: The National Finance Center is a federal government agency division under the United States Department of Agriculture that provides human resources, financial and administrative services for agencies of the United States federal government.

US Department of Treasury Financial Management System (FMS): The Department of the Treasury Bureau of the Fiscal Service provides a central payment service for users on behalf of government agencies.

Department of Commerce (DoC) Enterprise Continuous Diagnostic Monitoring (ECDM): DOC effort to adhere to continuous monitoring processes and overall ECDM compliance requirements.

US Department of Treasury HRConnect: Offers automated Human Resources (HR) capabilities to cross-examine, display and modify personnel data.

International Business Management Corporation (IBM) Maximo / TRIRIGA: Interconnection with IBM Maximo/TRIRIGA (Integrated Workplace Management System (IWMS) at USPTO) to collect employee data from Enterprise Data Warehouse (EDW) to IBM.

NOAA Enterprise Network (N-Wave/NOAA0550): Through a shared national network infrastructure, N-Wave provides reliable, secure and sustainable enterprise network services to support both operations and research for NOAA and other entities within the DOC.

Building, Assets & Property Management (BAPM): Building, Assets and Property Management System. he BAPM Boundary will consist of two (2) P&FM 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.

Consolidated Financial System (CFS): is a Master System composed of the following four subsystems: 1) Momentum 2) Concur Integration, 3) E-Acquisition (ACQ) and 4) 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 is a web-based COTS product that handles handle USPTO's travel needs. The eAcquisition (ACQ) is a web-based COTS software that provides an automated solution for the procure-to-pay process in the acquisition community at the USPTO, allowing procurement users to create acquisition requests and track the life of procurement actions and documents associating with the plan. The VendorPortal is a web-based COTS that provides a platform for interaction and information exchange between USPTO and the vendor community. It provides the ability to publish notices, solicitations and award announcements; enables vendor offer, invoice and receipt submission, and provides vendors insight into awards, deliverables and invoice statuses.

Reference Document Management Services (RDMS): provides Reference Document Management Services for USPTO.

Master Data Management (MDM) System: 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.

Fee Processing Next Generation (FPNG): is the fee management and revenue collection system at USPTO.

Information Delivery Product (IDP): is a Master System composed of three subsystems: Enterprise Data Warehouse, Electronic Library for Financial Management Services, and Financial Enterprise Data Management Tools.

Enterprise Data Warehouse (EDW): is a subsystem of the IDP master system and provides Enterprise Data Warehouse capabilities.

Information Dissemination Support System (IDSS): supports the Trademark and Electronic Government Business Division, the Corporate Systems Division (CSD), the Patent Search System Division, the Office of Electronic Information Products, and the Office of Public Information Services. It provides automated support for the search and retrieval of electronic text and images concerning patent applications and patents by USPTO internal and external users.

Intellectual Property Leadership Management Support System (IPLMSS): is a Major Application that facilitates reporting for a range of inquiries regarding USPTO business.

E-Discovery Software System-Cloud (EDSS-C): C-E-Discovery Software System - Cloud. The 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).

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.

MyUSPTO Cloud (MyUSPTO-C): is an external-facing web site application. It is comprised of internal and external users. The purpose of the system is to reduce the number of logins for external USPTO customers and to provide a single location from where they can conduct their business with the USPTO.

Planning and Budgeting Products (PBP): is a Master System composed of three subsystems: 1) Activity Based Information system (ABIS), 2) Analytics and Financial Forecasting (AFF), 3) Enterprise Budgeting Tool (EBT).

Patent Examination Data System (PEDS): formerly known as Pair Bulk (PBD) is a new platform in Amazon Web Services US East/West to provide bulk download of Public PAIR bibliographic data in a secure manner without impacting USPTO internal users.

Corporate Administrative Office System (CAOS): is an information system that supports the Human Resources business functions within the USPTO. CAOS supports all activities associated with the recruitment and management of USPTO personnel.

Integrated Workplace Management System (IWMS): manages all aspects of USPTO facilities—from space and lease management to capital improvement tracking to ensuring timely maintenance.

Compute Historical Analytics and Reporting Tools (CHART): Compute Historical Analytics and Reporting Tools. CHART-C 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).

Case Management System (CMS): provide a Cloud based system designed to assist the Office of Civil Rights staff in processing background investigations, employee relations and equal employment cases and requests for reasonable accommodation by collecting and maintaining data.

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 AWS cloud.

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.

Performance Monitoring Tools Amazon Cloud Services (PMTACS): Performance Monitoring Tools in Amazon Cloud Services

Performance Monitoring Tools (PMT): maintains the 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.

Enterprise Software Services (ESS): provides the USPTO with a collection of programs that use common business applications and tools for modeling how the entire organization works. ESS provides a centralized solution for assisting developers in building applications unique to the USPTO.

Enterprise Unix Services (EUS): is an infrastructure operating system that provides a UNIX base hosting platform to support other systems at USPTO.

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 7 and Windows 10 operating system (OS).

Enterprise Virtual Event Services (EVES): is an information system that enables business units to share knowledge through collaboration capabilities that incorporate data, voice, and video communication technologies.

USPTO CoSo Cloud Adobe Connect Solution (UCCACS): instance of CoSo Cloud Adobe Connect solution, is a web communication solution that enables USPTO to provide online computer-based training to internal audiences. The purpose of this system is to enable USPTO business units to share vital knowledge with USPTO staff.

USPTO Cisco Webex for Government (UCWG): purpose is to allow internal and external customers to send messages, conduct video communications, share files, join meetings, and hold white-boarding sessions in real time.

VBrick Rev Cloud (VRC): enables large organizations to securely and efficiently deliver high quality live and on-demand video to thousands of viewers using the corporate wide area network and Internet. It provides centralized management over video ingest and storage, user access and permissions, video capture and delivery devices, and video publishing and distribution.

Integrated Automations (IA): provides the necessary infrastructure to host the Integrated Automations technology solution in development, test, and production environments.

USPTO AWS Cloud Service (UACS): is a standard infrastructure platform used to support PTO Application Information Systems (AIS) hosted in the AWS East/West environment.

USPTO Google Cloud Services (UGCS): is a standard infrastructure platform used to support the USPTO Patent Search AI system hosted in the Google Cloud Platform (GCP) us-east4, Northern Virginia, environment.

USPTO MS Azure Cloud Service (UMACS): is a cloud infrastructure platform used to support USPTO Application Information Systems hosted in the Azure East/West environment

Contractor Access System (CAS): is an infrastructure information system that provides off-site contractors and selected USPTO employees with limited, monitored, and secured access to PTONet applications, resources, and services. The CAS network provides contractors with access to the USPTO network (PTONet) through the Enterprise Trusted User (ETU) Firewall architecture.

Enterprise Windows Servers (EWS): is an Infrastructure information system that provides a hosting platform for major applications that support the USPTO mission.

Private Branch Exchange-Voice over Internet Protocol (PBX-VOIP): is an infrastructure information system that provides services in support of analog voice, digital voice, collaborative services and data communications for business units across the entire USPTO.

Trilateral Network (TRINET): is an infrastructure information system that provides secure network connectivity for electronic exchange and dissemination of sensitive patent data between authenticated endpoints at the Trilateral Offices and TRINET members. The Trilateral Offices consist of the USPTO, the European Patent Office (EPO), and the Japanese Patent Office (JPO). The TRINET members consist of the World Intellectual Property Office (WIPO), the Canadian Intellectual Property Office (CIPO), and the Korean Intellectual Property Office (KIPO).

Data Storage Management System (DSMS): is a general support system (GSS) that provides a secure environment for archival and storage of data and records vital to USPTO's Business Continuity and Disaster Recovery plan.

Security and Compliance Services (SCS): Provides Security and Compliance Services (SCS) to USPTO.

Service Oriented Infrastructure System (SOI): is an infrastructure information system that provides the underlying platform upon which USPTO applications can be deployed.

Siemens Physical Access Control System (PACS): is an electronic physical

security system, and provides the capability to restrict and/or control physical access to USPTO facilities, equipment and resources.

Cardinal Intellectual Property (CIP) Patent Cooperation Treaty Search Recordation System (PCTSRS): The Patent Cooperation Treaty Search Recordation System (PCTSRS) is designed to support the United States Patent and Trademark Office's (USPTO) international application or Patent Cooperation Treaty (PCT) application process. The PCT provides a unified procedure for filing patent applications to protect inventions in each of its Contracting States. PCTSRS facilitates PCT searches and enables CIP employees to submit an accompanying written opinion regarding the patentability of the invention in question.

VASTEC Data Conversion System (DCS): The purpose of the system is to transform electronic Tagged Image File Format (TIFF) images of patent application documents to Extensible Markup Language (XML) documents based on a predefined XML schema. The files in the new XML format allow patent examiners to search, manage, and manipulate different document types, using examination tools under development.

Digital Media System (DMS): is an information system that 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.

Landon IP Information System (LIPIS): is an infrastructure information system that is designed to support the USPTO international application or PCT application process.

Ex-Libris Alma Primo: Alma is a cloud-based Low Impact Software-as-a-Service (LI-SaaS) unified library services platform. It provides managing print, electronic, and digital materials in a single interface. Alma provides patrons (tenant organizations) with a cost-effective library management solution that consists of the following components: Alma (library) and Primo (discovery services).

Patent Administrative Center (PAC): system will provide 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 Public Search: is a custom developed application information system provided by USPTO to replace legacy public search systems with a unified search system.

Patent Search Artificial Intelligence: 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).

Patent Business Content Management Services (PBCMS): purpose is to migrate current legacy services to the new cloud-based services that leverage cloud native capabilities and technologies to reduce infrastructure and operational maintenance cost to the USPTO.

Patent Capture and Application Processing System – Examination Support (PCAPS-ES): purpose is to process, transmit, and store data and images to support the data-capture and conversion requirements of the USPTO to support the USPTO patent application process.

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

Patent End to End (PE2E): provides examination tools for Central examination unit to track and manage the cases in this group and view documents in text format.

Patent Exam Center (PEC): allow 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).

Patent Search System - Specialized Search and Retrieval (PSS-SS): is a Master system that supports the Patent Cost Center. It is considered a mission critical “system”. PSS-SS provides access to highly specialized data.

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 Next Generation (TMNG): is a Major Application that provides support for the automated processing of trademark applications for the USPTO.

Trademark Processing System (External System) (TPS-ES): is Major Application information system that provides customer support for processing Trademark applications for USPTO.

Trademark Processing System (Internal Systems) (TPS-IS): is an information system that provides support for the automated processing of trademark applications for the USPTO. TPS-IS includes eleven applications that are used to support USPTO staff through the trademark review process. TPS-IS features the ability to interface with related systems within USPTO.

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

Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP), and Internet Protocol Address Management (IPAM) (DDI): The Infoblox infrastructure is a highly-available and secure solution for providing DNS/ DHCP/IPAM (DDI) services to USPTO enterprise computer network.

Enterprise Access Infrastructure System (EAIS): EAIS is a combination of specialized systems designed to support file transfer services to USPTO information systems. These systems are established in the Axway Secure Transport environment. The routers, switches, firewalls, Lightweight Directory Access Protocol (LDAP) servers, and ACE/SecurID authentication servers that are needed for end-to-end support are not related to EAIS. The EAIS servers are located internally and the Axway Edge appliances are in the demilitarized zone (DMZ) for external users.

Network Access Control (NAC): The Cisco Identity Services Engine (ISE) is a next-generation identity and access control policy platform that enables the USPTO to enforce authentication, authorization, and accounting on users and devices accessing the USPTO network through either wired or wireless connections.

The Cisco ISE allows the USPTO to gather real-time contextual information from networks, users, and devices, tying identity to network elements such as access switches, wireless Local Area Network (LAN) controllers, Virtual Private Networks (VPN) gateways, and data center switches. With this contextual information, the USPTO can make governance decisions about network access.

Office of Human Resources/Office of Financial Disbursement Network (OHR/OFDNet): The OHRNet project provides an integrated, maintainable, and cost-effective system for the continued support of the Patent and Trademark T&A transmission process. The project provides an infrastructure change to the existing architecture but does not replace the existing T&A program used by the USPTO timekeepers. OHRNet establishes secure communications for transmission of T&A data across the USPTO Local Area Network (PTONet) and to the U.S. Department of Agriculture - National Finance Center (NFC).

OFDNet provides reliable data communications between the USPTO and the four financial processing centers located throughout the U.S.:

- U.S. Treasury primary Regional Operating Center (ROC)
- U.S. Treasury ROC disaster recovery site
- USDA's Digital Infrastructure Services Center
- NFC Federal Processing Center

OFDNET allows the USPTO Momentum financial application software to send and receive disbursement and payroll data in a secure environment on behalf of the USPTO Office of Finance (OF).

PTO Network (PTONet): The function of PTONet is to manage and maintain the flow of the core business data system and internetworking equipment implemented within the USPTO. PTONet is the foundation for all USPTO users to communicate, search for information, and support business processes. PTONet also includes Authentication Services (AS) and Network Time System (NTS) components. AS: Cisco Access Control Center (ACS) Server is an access policy control platform that enables network administrators to use their RSA devices (or fobs) or PTONet Windows' user accounts to log onto PTONet network devices. This Cisco product functions as a central login agent for all network devices. The Cisco ACS Server supports Remote Access Dial-In Services (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+)-capable network devices. Authorization levels on network devices are determined by the user's assigned Cisco ACS Server user group. Cisco ACS Server maintains logs of log-in activity and configuration activity on TACACS+-capable network devices.

Perimeter Network (PN)

The Perimeter Network 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. The Perimeter Network also provides secure public and trusted users access to USPTO resources and applications.

The Perimeter Network 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.

The Perimeter Network is the preferred connection point for Wide Area Network (WAN) access, both to trusted USPTO sites and to untrusted or semi-trusted WAN sites such as contractors. By bringing in all external connections to one point of demarcation, it is clear where security and routing controls must be applied in the PTONet network. It also allows simple use of default routing in the Core, keeping the details of external routing prefixes out of the Core network.

Remote Access-Virtual Private Network (RA VPN)
The RA VPN system enables authorized USPTO personnel and contractors to telecommute by providing multiple ways to connect. The first method allows USPTO's UL, which is a managed asset, to connect using the Cisco AnyConnect VPN client. Another method allows a typical non-USPTO managed-asset and uses a combination of Cisco AnyConnect VPN client and client-less (browsers).

EMP-SL1
The Enterprise Management Platform - ScienceLogic One system is a group of distributed appliances managed as a single unified system from two central Database appliances. The Database appliances hold and maintain the central databases of the platform. It pushes configurations and updates out to platform members, synchronizes changes and schedules platform operations.

The EMP-SL1 platform has two sub-components, an observability system for network devices, servers and cloud infrastructure, and the USPTO Log-In/Log-Out (LILO) time reporting tool for USPTO employees.

Public Enterprise Wireless Local Area Network (PEWLAN)
Public Enterprise Wireless Local Area Network (PEWLAN) is a productivity enhancer for the mobile staff, guests, and contractors. A smoothly implemented wireless LAN facilitates secure 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.

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

USPTO authenticates and authorizes users through secured wired, wireless, and VPN networks. Users cannot retrieve information from the system.

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

NSI is an Infrastructure information system, and provides an aggregate of subsystems that facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO IT applications. NSI is made up of network servers and devices that are connected with all other internal USPTO systems.

(g) Any information sharing

NSI facilitates the sharing of information within USPTO, with other agencies and other systems. The information shared is determined by the systems listed within the interconnections.

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

The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information for NSI is 5 U.S.C. 301, 35 U.S.C. 2, and 44 U.S.C. 3101.

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

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): The NSI system is a network that facilitates the transfer of information between information systems. Please refer to the PIA, for the interconnections listed in Section C of the introduction.					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: NSI facilitates the transfer of information between information systems, some of which collect and transmit SSN over NSI. Please refer to the PIA, for the interconnections listed in section C of the introduction.					

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): The NSI system is a network that facilitates the transfer of information between information systems. Please refer to the PIA, for the interconnections listed in Section C of the introduction.					

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):
The NSI system is a network that facilitates the transfer of information between information systems. Please refer to the PIA, for the interconnections listed in Section C of the introduction.

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):
The NSI system is a network that facilitates the transfer of information between information systems. Please refer to the PIA, for the interconnections listed in Section C of the introduction.

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): NSI has the capability and function to collect some audit data.

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	☐	Hard Copy: Mail/Fax	☐	Online	☐
Telephone	☐	Email	☐		

Other (specify): The NSI system is a network that facilitates the transfer of information between information systems. Please refer to the PIA, for the interconnections listed in Section C of the introduction.

Government Sources					
Within the Bureau	☒	Other DOC Bureaus	☐	Other Federal Agencies	☒
State, Local, Tribal	☐	Foreign	☐		

Other (specify): The NSI system is a network that facilitates the transfer of information between information systems. Please refer to the PIA, for the interconnections listed in Section C of the introduction.

Non-government Sources					
Public Organizations	☐	Private Sector	☐	Commercial Data Brokers	☐
Third Party Website or Application			☐		
Other (specify): The NSI system is a network that facilitates the transfer of information between information systems. Please refer to the PIA, for the interconnections listed in Section C of the introduction.					

2.3 Describe how the accuracy of the information in the system is ensured.

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. 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): NSI purpose is to facilitate the transfer of information between systems.			

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).

NSI facilitates the transmission of information between systems. These systems may choose to change the PII they are transmitting via NSI at any time as they are the owners of their PII. To see the PII collected by these systems, please refer to the PIA for the interconnections listed in section c. Please note that some of these systems are not USPTO owned or operated system but operated by other agencies.

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 stored within the system could be exposed. To avoid a breach, the system has certain security controls in place to ensure the information is handled, retained, and disposed of appropriately. 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. These audit trails are based on application server out-of-the-box logging reports reviewed by the Information System Security Officer (ISSO) and System Auditor and any suspicious indicators such as browsing will be immediately investigated and appropriate action taken. Also, system users undergo annual mandatory training regarding appropriate handling of information. 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.

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): NSI facilitates the transmission of information between systems. These systems may choose to change the PII they are transmitting via NSI at any time as they are the owners of their PII. To see the PII collected by these systems, please refer to the PIA for the interconnections listed in section c. Please note that some of these systems are not USPTO owned or operated system but operated by other agencies.	☒	☒	☐

☐	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: All interconnections listed in introduction section c. 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): Guest access – Guests will utilize a separate SSID and will require authentication prior to being allowed access to the guest network. The ISE guest portal will provide credentialed access to the guest network. [Public & Enterprise Wireless Local Area Network (PEWLAN)] Guests are not allowed to connect to the wired network.			

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:	
☒	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: NSI only facilitates the transmission of information between systems. These systems would be responsible for determining if individuals have an opportunity to decline to provide PII/BII within their system. Please refer to the PIA for the interconnections listed in section c of the introduction.

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: NSI only facilitates the transmission of information between systems. These systems would be responsible for determining if individuals have an opportunity to consent to particular uses of their PII/BII within their system. Please refer to the PIA for the interconnections listed in section c of the introduction.

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:
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: NSI only facilitates the transmission of information between systems. These systems would be responsible for determining if individuals have an opportunity to review or update the PII/BII pertaining to them. Please refer to the PIA for the interconnections listed in section c of the introduction.

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: Audit Logs
☒	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): 5/1/2025 ☐ 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).*

PII within the system is secured using appropriate management, operational, and technical safeguards in accordance with NIST requirements. Such management controls include a review process to ensure that management controls are in place and documented in the System Security Privacy Plan (SSPP). The SSPP specifically addresses the management, operational, and technical controls that are in place and planned during the operation of the system. Operational safeguards include restricting access to PII/BII data to a small subset of users. All access has role-based restrictions and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. The system maintains an audit trail and the appropriate personnel is alerted when there is suspicious activity. Data is encrypted in transit and at rest.

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)*:
☐	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. Provide the name of the record control schedule:
☒	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: NSI only facilitates the transmission of information between systems. Those systems are responsible for their record control schedules. NSI does not monitor nor store records on behalf of these systems. Please refer to the PIA for the interconnections listed in section c of the introduction.
☐	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): NSI only facilitates the transmission of information between systems. Those systems are responsible for their disposing of the data. NSI does not store the PII/BII, it only passes through NSI. Please refer to the PIA for the interconnections listed in section c of the introduction.			

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: NSI only facilitates the transmission of information between systems. Those systems are responsible for determining the confidentiality impact level. NSI does not monitor nor store records on behalf of these systems. Please refer to the PIA for the interconnections listed in section c of the introduction.
☒	Quantity of PII	Provide explanation: NSI facilitates the transmission of large quantities of data that may contain PII.
☒	Data Field Sensitivity	Provide explanation: The data transmitted via NSI includes patent related data, HR data and other data that may contain PII.
☒	Context of Use	Provide explanation: NSI only facilitates the transmission of information between systems.
☒	Obligation to Protect Confidentiality	Provide explanation: NSI employs approved cryptographic mechanism, including AES, IPSec, SSHv2, SSL/TLS, HTTPS WPA2 etc., to protect the confidentiality and integrity of information in transit. All inbound and outbound communications within the NSI network are encrypted to prevent unauthorized access, interception or disclosure
☒	Access to and Location of PII	Provide explanation: There is no direct access to PII through the NSI system. NSI facilitates the secure transmission of PII, which is encrypted in transit to protect confidentiality and prevent unauthorized disclosure.
☒	Other:	Provide explanation: NSI only facilitates the transmission of information between systems. Those systems are responsible for determining the confidentiality impact level. NSI does not monitor nor store records on behalf of these systems. Please refer to the PIA for the interconnections listed in section c of the introduction.

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.)

The PII in this system poses a risk if 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 cloud and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved and authorized accounts. USPTO monitors, in real-time, all activities and events within the servers storing the potential PII data and personnel review audit logs received on a regular bases and alert 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.