Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Private Branch Exchange – Voice Over Internet Protocol (PBX-VOIP)

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

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

for Charles Cutshall

TAHIRA MURPHY Digitally signed by TAHIRA MURPHY
Date: 2024.11.29 16:52:13 -05'00' 11/29/2024

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Private Branch Exchange – Voice Over Internet Protocol (PBX-VOIP)

Unique Project Identifier: EIPL-IHSN-03-00

Introduction: System Description

Provide a brief description of the information system.

The Private Branch Exchange – Voice over Internet Protocol (PBX-VOIP) is an infrastructure information system consisting of four sub-systems, Cisco VOIP, Enterprise Call Center (ECC), One Voice Operations Center (OVOC), and the United States Patent and Trademark Office (USPTO) Facsimile (PTOFAX). PBX-VOIP provides the following services in support of analog voice, digital voice, collaborative services and data communications for business units across the entire USPTO:

- Converged and non-converged analog and digital voice communication services;
- Customer Contact Center voice and terminal support;
- Teleworker collaborative computing environment;
- Administration of Microsoft Teams phones;
- Submission of documents, payments; and
- Provide communication services for external and internal community.

Address the following elements:

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

PBX-VOIP is a General Support System (GSS).

(b) System location

PBX-VOIP is located in Alexandria, VA.

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

PBX-VOIP interconnects with the following systems:

- **Enterprise Desktop Platform (EDP):** 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 Windows Services (EWS):** EWS is an infrastructure information system, which provides a hosting platform for major applications that support various USPTO missions.
- **Network and Security Infrastructure System (NSI):** 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.
- **Enterprise UNIX Services (EUS):** EUS System consists of assorted UNIX operating system variants (OS), each of which is comprised of many utilities, along with the master control program, the kernel.
- **Information Dissemination Support System (IDSS):** IDSS is an application information system, and provides the following services or functions in support of the USPTO mission. The purpose of the IDSS system is to support 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 timely search and retrieval of electronic text and images concerning patent applications and patents by USPTO internal and external users.
- **Security and Compliance Services (SCS):** SCS is a system that utilizes its subsystems to connect with all the USPTO systems. This system contains all cybersecurity tools used to assess the security posture of a system and maintains data for after action investigations.
- **Enterprise Software System (ESS):** ESS provides Enterprise Directory Services, Role-Based Access Control System, Email as a Service, and PTO Exchange Services.
- **Storage Infrastructure Managed Service (SIMS):** SIMS provides disk-based storage components, Storage Area Network (SAN), replication, and analysis capabilities. The disk-based storage components are separated into two main areas Block based storage and Network Attached Storage (NAS).

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

PBX-VOIP operates through the following Automated Information Systems (AISs) to achieve its purpose:

Cisco Voice over Internet Protocol (Cisco- VoIP): Provides telephony services to the USPTO Headquarters and Nation-wide Satellite Offices.
Enterprise Contact Center (ECC): Provides technology that allows the public and

USPTO employees the ability to contact USPTO business centers and access interactive and automated information regarding USPTO products, processes, and services. Additionally, ECC features an automated failover capability for system redundancy.

PTO Enterprise Fax System (PTOFAX): The PTOFAX system provides external (non-USPTO) users the ability to send faxes to the USPTO and USPTO personnel the ability to send fax documents to external users from their USPTO Enterprise Desktop Platform (EDP) computers using the PTOFAX client software and via the Enterprise Remote Access (ERA) Secure External Access System (SEAS) by launching the PTOFAX client application through a Citrix client session. The PTOFAX system provides this service by utilizing standard hardware and the commercial off-the-shelf (COTS) product RightFax.

AudioCodes One Voice Operations Center (OVOC): OVOC is a voice network management solution that combines management of voice network devices and quality of experience monitoring into a single, intuitive web- based application.

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

Information in the system is retrieved through webpage access. Secure Shell (SSH) - used for secure logins, file transfers (secure copy protocol, Secure file transfer protocol) and port forwarding. This port is needed for logging into the call managers and for nightly backups for the Cisco- VoIP Cluster. (Call Manager Signaling) credentials are validated via Active Directory.

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

Cisco- VoIP employs cryptographic protections to prevent unauthorized disclosure of information and detect changes during transmission through the implementation of Transport Layer Security (TLS) 1.0 for Uniform Resource Locators (URLs) with Federal Information Processing Standards (FIPS) 140-2 compliant protocols. In addition, Cisco-VoIP implements Hypertext Transfer Protocol Secure (HTTPS) (TLS/SSL) for the WEB administration and the remote command line utilizes SSH.

(g) Any information sharing

The Emergency Notification System connects to the Cisco Call Manager to obtain telephone information for users. In addition, Cisco WebEx Meeting Server utilizes Cisco Call Manager for account information. ECC might share some information with another system for reporting purposes.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting,

maintaining, using, and disseminating the information

5 U.S.C. 301, 35 U.S.C. 2, 44 U.S.C. 3101, and EO 12862

(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):					
*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):					

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)

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.

USPTO implements security and management controls to prevent the inappropriate disclosure of sensitive information. Security controls are employed to ensure information is resistant to tampering, remains confidential as necessary, and is available as intended by the agency and as expected by authorized users. Management controls are utilized to prevent the inappropriate disclosure of sensitive information. In addition, the Perimeter Network (NSI) and Security and Compliance Services (SCS) provide additional automated transmission and monitoring mechanisms to ensure that PII/BII information is protected and not breached by external entities. PII data is received from Office of Human Resources (OHR) and Patent Application Location Monitoring (PALM) and information received is updated via syncing.

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): Call detail records, Caller ID information (including first and last name), Voicemail messages			

☐	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): System Performance, Usage, and Quality. Phone system stores records of phone calls and records are also forwarded to Avotus for report generation for Freedom of Information Act (FOIA), Human Resources (HR), and Office of Security request.			

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).

Call detail records, caller ID information (including first and last name), and voicemail messages are collected, maintained, and disseminated for DOC employees, Contractors working on behalf of DOC, Other Federal Government personnel, and Members of the public.

The system automatically collects the details of a call as to date, time, parties, length, and devices. Call detail records are copied to a storage space for long-term storage. Cisco-VoIP maintenance personnel have access to this information and provide reports upon request/schedule to other USPTO Business Units.

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 addition to insider threats, activity which may raise privacy concerns include the collection, maintenance and dissemination of PII in the form of call detail records, caller ID information (including first and last name), and voicemail messages. USPTO mitigates such threats through mandatory training for system users regarding appropriate handling of information and automatic purging of information in accordance with the retention schedule.

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):	☐	☐	☐

☐	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: IDSS SCS ESS SIMS NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is

	accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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

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

Section 7: Notice and Consent

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

☒	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
☒	Yes, notice is provided by 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:
☒	No, notice is not provided.	Specify why not: Detail Record information is requested from other business units within USPTO for in office processes like FOIA requests and for investigative actions by Office of human resources and security, etc.

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 do not have the ability to decline to provide PII/BII since there is no mechanism in place preventing the collection of call detail information on a per user basis for telephone calls. Collection of Call Detail Records can be completely turned off if directed but will have an impact to

		the system maintenance/usage as well as providing reports to other USPTO Business units (BU) and FOIA requests.

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: Users do not have the ability to consent to particular uses of their PII/BII since there is no mechanism in place preventing the collection of call detail information on a per user basis for telephone calls. Even if there was, non-USPTO callers to a USPTO issued phone cannot request this. Collection of Call Detail Records can be completely turned off if directed but will have an impact to the system maintenance/usage as well as providing reports to other USPTO BUs and FOIA requests.

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: Individuals can call the service desk to have their information updated.
☐	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

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): 11/27/2023 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
☒	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
☒	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 5 recommended security controls

	for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
☒	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☐	Contracts with customers establish DOC ownership rights over data including PII/BII.
☐	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
☐	Other (specify):

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

Information in USPTO information systems is protected with operational, management, and technical controls that are documented in the PBX-VOIP System Security Plan. A Security Categorization compliant with the FIPS 199 and NIST SP 800-60 requirements was conducted for PBX-VOIP. The overall FIPS 199 security impact level for PBX-VOIP was determined to be Moderate. This categorization influences the level of effort needed to protect the information managed and transmitted by the system.

Operational controls include securing all hardware associated with the PBX-VOIP in the USPTO Data Center. The Data Center is controlled by access card entry and is manned by a uniformed guard service to restrict access to the servers, their operating systems, and databases.

PBX-VOIP is secured by various USPTO infrastructure components, including the Network and Security Infrastructure (NSI) system and other OCIO established technical controls including passwords.
Windows and Linux servers within PBX-VOIP are regularly updated with the latest security patches by the Windows and Unix System Support Groups.

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)*: COMMERCE/DEPT-18, Employee Personnel Files Not Covered by Notices of Other Agencies COMMERCE/DEPT-25, Access Control and Identity Management System. COMMERCE/PAT-TM-20, Customer Call Center, Assistance and Satisfaction Survey Records.
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☐	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

General Records Schedules (GRS) | National Archives

☒	There is an approved record control schedule. Provide the name of the record control schedule: GRS 5.1; 020: Non-recordkeeping copies of electronic records. GRS 5.5; 010: Mail, printing, and telecommunication services administrative and operational records. GRS 5.5; 020: Mail, printing, and telecommunication services control records. GRS 5.8; 010: Technical and administrative help desk operational records. GRS 6.5; 010: Public customer service operations records
☐	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: Caller ID (Name, Telephone Number), and voicemail messages are non-sensitive identifiers.
☒	Quantity of PII	Provide explanation: The quantity of data is collected is large but the number of data items collected are the details of a call relating to date, time, parties, length, and devices.
☒	Data Field Sensitivity	Provide explanation: The data includes limited personal data that does not increase the sensitivity of the data.
☒	Context of Use	Provide explanation: System automatically collects the details of a call as to date, time, parties, length, and devices. Call Detail Records are copied to a storage space for long-term storage. Cisco-VoIP maintenance personnel have access to this information and provide reports upon request for FOIA and other USPTO Business Units like HR and Office of Security.
☒	Obligation to Protect Confidentiality	Provide explanation: USPTO Privacy Policy requires the PII information collected within the system to be protected accordance to NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information.
☒	Access to and Location of PII	Provide explanation: Access is limited only to the identified and authenticated users.
☐	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 addition to insider threats, activity which may raise privacy concerns include the collection, maintenance and dissemination of PII in the form of call detail records, caller ID information (including first and last name), and voicemail messages. USPTO mitigates such threats through mandatory training for system users regarding appropriate handling of information and automatic purging of information in accordance with the retention schedule.

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.