Template Version Number: 01-2020

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

Privacy Impact Assessment
for the
Enterprise Virtual Event Services (EVES)

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

Jennifer Goode 09/09/2021

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Enterprise Virtual Event Services

Unique Project Identifier: (PTOI-025-00)

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

Enterprise Virtual Event Services (EVES) enables business units to share vital knowledge through collaboration capabilities that incorporate data, voice, and video communication technologies. Business units will gain efficiency and effectiveness by communicating and sharing vital business knowledge with internal and external customers.

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

(b) System location
The system location is in 600 Dulany Street, Alexandria, Virginia**.**

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
EVES has the following interconnections:

Cisco Call Manager: The Cisco Call Manager provides registration, call control, and routing for Cisco Telepresence Endpoints.

VBrick REV: The VBrick REV uses three VBrick Distributed Media Engines (DME) to provide an on campus content delivery network for on demand video distribution and two VBrick Active Directory servers for account provisioning.

Enterprise Monitoring and Security Operations (EMS): The Enterprise Management System (EMS) provides automated, proactive system management, and service-level management for network devices and application and database servers.

Enterprise Windows System (EWS): The EWS is an Infrastructure information system, and provides a hosting platform for major applications that support various USPTO missions. The USPTO facilities are leased by the General Services Administration (GSA) from LCOR, Incorporated.

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

Network and Security Infrastructure (NSI): The 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 Software Services (ESS): The ESS system provides the USPTO organization with a collection of programs that utilize common business applications and tools for modeling how the entire organization works.

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

Agency Administrative Support System (AASS): The AASS is an Application information system that works to: Consolidate imaging document systems within the Corporate System Division (CSD). It enables USPTO to manage and track automated hardware and software assets from the time of their acquisition to retirement.

Service Oriented Infrastructure (SOI): The SOI provides a feature-rich and stable platform upon which USPTO applications can be deployed. SOI includes web servers running Apache and HTTP servers.

Enterprise Desktop Platform (EDP): The EDP is an infrastructure information system which provides a standard enterprise-wide environment that manages desktops and laptops running on the Windows 10 operating system (OS), providing United States Government Configuration Baseline (USGCB) compliant workstations.

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

The system achieves this through internal Email meeting invites, web browsers, desktop clients, and telephone connections.

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

Authorized users join meetings via web URLs and SIP addresses. Users approved for administrative access view audit log records via a browser interface.

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

All information is encrypted Transmitted to and from using via TLS 1.2 encryption.

(g) Any information sharing conducted by the system.
The system provides VBrick REV with enterprise directory information to perform account provisioning.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
35 U.S.C. 2, 115, 117, 118, 122, 184, 261, 371; 5 U.S.C. 301; 37 C.F.R. 1.14

(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 (version 01-2015 or 01-2017).
☐ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later).

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. Physical Characteristics	☐
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): EVES does not record audio and video but may maintain and store it for other systems.					

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.

The non-sensitive Personally Identifiable Information in EVES 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): EVES does not record audio and video but may maintain and store it for other systems.			

☒	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): FOIA			

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).

EVES is primarily a transport mechanism, the information provided by virtual meeting participants is restricted to meeting hosts and authorized system administrators.

Federal Employee, USPTO Employees and Contractors: Name and email address are collected and maintained in audit logs, and that information is only used to capture the meeting participants. This information helps to document meeting attendance, improve Federal services online, and as a way to measure employee satisfaction with the service. Call detail information is used to document system usage.

Members of the Public: Display Name, email address, and IP address are collected and maintained in audit logs, and that information is only used to capture the total number of meeting participants. The total number of connections helps to improve Federal services online and as a way to measure the public's satisfaction with the service. Call detail information is used to document system usage.

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.)

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. Training is also provided to handle insider threats. The risks to the system are insider threats and adversarial entities. EVES implements NIST security and management controls to prevent the inappropriate disclosure of sensitive information. Automated mechanisms are in place to ensure the security of all data collected. Security controls are employed to ensure information is resistant to tampering (Physical and Access Controls), the confidentiality of data in transit (Encryption), and that data is available for authorized users only (Access Control). Management controls are utilized to prevent the inappropriate disclosure of sensitive information. In addition, the Perimeter Network (NSI) and EMSO systems provide additional automated transmission and monitoring mechanisms to ensure that PII is protected and not breached by any outside entities or insider threats. In the event of disposal, EVES uses degaussing to permanently remove data according to government mandate and security policy.

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: VBrick REV: The VBrick REV uses three VBrick Distributed Media Engines (DME) to provide an on campus content delivery network for on demand video distribution and two VBrick Active Directory servers for account provisioning. Security and Compliance Services (SCS): SCS provides automated, proactive system management, and service-level management for network devices and application and database servers. EVES connects with Enterprise Software Services to provide account provisioning and authorization services using enterprise directory information. Enterprise Software Services (ESS): The ESS system provides the USPTO organization with a collection

	of programs that utilize common business applications and tools for modeling how the entire organization works. Agency Administrative Support System (AASS). The AASS is an Application information system that works to: Consolidate imaging document systems within the Corporate System Division (CSD). It enables USPTO to manage and track automated hardware and software assets from the time of their acquisition to retirement. All data transmissions are encrypted and require credential verification. All data transmissions not done through dedicated lines require security certificates. Inbound transmissions as well as outbound transmissions pass through a DMZ before being sent to endpoint servers. Access controls, auditing and encryption are leveraged to prevent PII/BII leakage. In accordance with the USPTO Privacy Policy guidelines, all systems that process PII and have interconnections are designed and administered to ensure the confidentiality of PII provided to and by EVES. Specific safeguards that are employed by the systems: • The systems and its facility are physically secured and closely monitored. Only individuals authorized by USPTO are granted logical access to the system. • Technical, operational, and management security controls are in place and are verified regularly. • Periodic security testing are conducted on the systems to help detect new security vulnerabilities on time. • All personnel are trained to securely handle PII information and to understand their responsibilities for protecting PII.
☐	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:	
☒	Yes, notice is provided by other means.	Specify how: Pop-up/Banner Warning – See Appendix A

☒	No, notice is not provided.	Specify why not: The vendor (Cisco) does not provide an option to add a link to the USPTO privacy policy on the webpage where the PII is entered. The Cisco system is at end-of-life and will be decommissioned by December 2021. This issue only pertains to members of the public that are using a forwarded link to attend the meeting. PTO employees and contractors have a privacy statement see Appendix A.

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: For members of the public, they can choose to enter any name or email address (whether valid or not) into the system. Their name and email address are not verified or used for authentication.
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: For USPTO employees, the authorization process automatically passes the users name and USPTO email address to EVES via the USPTO computer used to access content during onboarding

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: The information provided by the public is voluntary and is not validated. USPTO Employees and Contractors consent to providing information for the primary purpose of acquiring access to applications and network during on boarding when they accept their USPTO PTONet credentials
☐	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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: Employees have the opportunity to update their PII through active directory. Public users have an opportunity to review/update PII before submitting the information.
☐	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: The PII (from both members of the public and USPTO employees and contractors) is recorded and stored in system databases. That PII is monitored and tracked by USPTO on an as-needed basis through 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): __3/10/2021_____ ☐ 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).*

Personally Identifiable Information (PII) in EVES is secured using appropriate administrative, physical, and technical safeguards in accordance with the applicable federal laws, executive orders, directives, policies, regulations, and standards.

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 USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access.

Additionally, EVES is secured by various USPTO infrastructure components, including the Network and Security Infrastructure (NSI) system and other OCIO established technical controls to include password authentication at the server and database levels.

All sensitive-PII at-rest and in-transit is protected in accordance with NIST recommended encryption. The information transmitted between the systems is protected within USPTO's secure perimeter through the Network and Security Infrastructure (NSI) and the Enterprise Monitoring and Security Operations (EMSO) systems. All data transmissions are encrypted and require credential verification. All data transmissions not done through dedicated lines require security certificates and pass through a DMZ before being sent to endpoint servers.

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/PAT-TM-17, USPTO Security Access Control and Certificate Systems COMMERCE/DEPT-23 Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs. COMMERCE/DEPT-25 Access Control and Identity Management System
☐	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: GRS 3.2:010 Information Systems Security Records Systems and data security 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: Name, telephone number, email address, work email and work telephone number can be personal identifiers. Video and audio recordings can also be used to identify individuals.
☒	Quantity of PII	Provide explanation: EVES system personnel consider the quantity of PII (name and email address for USPTO employees and contractors; potential real name and email address [unverified] for members of the public) to be limited.
☒	Data Field Sensitivity	Provide explanation: The combination of name and email address for USPTO employees and contractors; potential real name and email address [unverified] for members of the public all have low sensitivity. Video and audio recordings can also be used to identify individuals.
☒	Context of Use	Provide explanation: Federal Employees: Name and email address are collected and maintained in audit logs, and that information is only used to capture the meeting participants. This information helps to document meeting attendance, improve Federal services online, and as a way to measure employee satisfaction with the service. Call detail information is used to document system usage. Members of the Public: Display Name, email address, and IP address are collected and maintained in audit logs, and that information is only used to capture the total number of meeting participants. The total number of connections helps to improve Federal services online and as a way to measure the public's satisfaction with the service. Call detail information is used to document system usage. Video and audio recordings can be used to identify individuals

		and affect privacy.
☒	Obligation to Protect Confidentiality	Provide explanation: In accordance with NIST 800-53 Rev. 4, EVES implements both AR-2 (Privacy Impact and Risk Assessment) and AR-7 (Privacy-Enhanced System Design and Development) security controls to ensure all stakeholder's confidentiality is protected.
☒	Access to and Location of PII	Provide explanation: The non-sensitive Personally Identifiable Information in EVES is secured using appropriate administrative, physical and technical safeguards in accordance with the NIST 800-53 Rev. 4. Authorized USPTO staff and contractors have access to the data stored on the EVES System.
☐	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.)

USPTO has identified and evaluated potential threats to PII such as loss of confidentiality and integrity of information. Also insider threats and outside entities can be threats to Privacy. Based upon USPTO's threat assessment, the Agency has implemented a baseline of security controls to mitigate the risk to sensitive information to an acceptable level. All information is encrypted Transmitted to and from using via TLS 1.2 encryption. Only the system administrators have access to audit logs that contain the call and meeting detail records.

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 – Privacy Notice