Template Version Number: 01-2020

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

Privacy Threshold Analysis
for the
Enterprise Virtual Event Services (EVES)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Enterprise Virtual Event Services (EVES)

Unique Project Identifier: PTOI-025-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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, VA 22314

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 purpose that the system is designed to serve:***

EVES enables USPTO 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.

e) ***The way the system operates to achieve the purpose:***
The system achieves this through internal Email meeting invites, web browsers, desktop clients, and telephone connections.

f) ***A general description of the type of information collected, maintained, used, or disseminated by the system:***
The system disseminates real-time video, audio, and presentation to and from video conference participants and users watching recorded videos on demand.

The system uses LDAP Synchronization to copy USPTO Active Directory user information to USPTO's VBrick REV Cloud instance.

The system collects call detail record information about each call, time, duration, calling party.

The system collects meeting detail record information about each meeting, time, duration, display name, and email address.

g) ***Identify individuals who have access to information on the system:***
System administrators have access to audit logs that contain the call and meeting detail records.

Meeting participants have access to the video, audio, and presentation screens disseminated during a meeting.

h) ***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.

i) ***How information is transmitted to and from the system:***
All information is encrypted Transmitted to and from using via TLS 1.2 encryption.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

☐ This is a new information system. *Continue to answer questions and complete certification.*

☐ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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. *Continue to answer questions and complete certification.*

☐ 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). *Continue to answer questions and complete certification.*

☐ 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). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

☐ Yes. This is a new information system.

☐ Yes. This is an existing information system for which an amended contract is needed.

☐ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

☒ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

☐ Yes. *(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.			

☒ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

☐ Yes, the IT system collects, maintains, or disseminates BII.

☒ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

☒ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

☒ DOC employees
☒ Contractors working on behalf of DOC
☐ Other Federal Government personnel
☒ Members of the public

☐ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

☐ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

☒ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

☒ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

☐ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

☐ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

☒ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

☒ I certify the criteria implied by one or more of the questions above **apply** to the Enterprise Virtual Event Services (EVES) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

☐ I certify the criteria implied by the questions above **do not apply** to the Enterprise Virtual Event Services (EVES) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Randy Hill Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-8983 Email: Randy.Hill@uspto.gov Signature: Users, Hill, Randy Digitally signed by Users, Hill, Randy Date: 2021.08.10 13:07:36 -04'00' ________________ Date signed: ________________	**Chief Information Security Officer** Name: Don Watson Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-8130 Email: Don.Watson@uspto.gov Signature: DON R Watson Digitally signed by DON R Watson Date: 2021.08.11 10:33:29 -04'00' ________________ Date signed: ________________
Privacy Act Officer Name: John Heaton Office: Office of General Law (O/GL) Phone: (571) 270-7420 Email: Ricou.Heaton@upsto.gov Signature: Users, Heaton, John (Ricou) Digitally signed by Users, Heaton, John (Ricou) Date: 2021.08.09 16:34:11 -04'00' ________________ Date signed: ________________	**Bureau Chief Privacy Officer and Authorizing Official** Name: Henry J. Holcombe Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-9400 Email: Jamie.Holcombe@uspto.gov Signature: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2021.08.11 13:48:53 -04'00' ________________ Date signed: ________________
Co-Authorizing Official Name: N/A Office: N/A Phone: N/A Email: N/A Signature: ________________ Date signed: ________________	