Template Version Number: 01-2020

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

Privacy Impact Assessment
for the
USPTO Cisco WebEx for Government (UCWG)

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 1/12/2022

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Cisco WebEx for Government (UCWG)

Unique Project Identifier: PTOC-061-00

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.

USPTO Cisco WebEx for Government (UCWG) enables business units to share vital knowledge through collaboration capabilities that incorporate data, voice, and video communication technologies. The system enables global employees and virtual teams to collaborate in real time from anywhere, anytime, on mobile devices or video systems as though they were working in the same room. The UCWG is a USPTO information system that utilizes the Cisco Systems Inc. - WebEx for Government is a FedRAMP Moderate impact system. The system is deployed and operated by Cisco Systems Inc. as a multi-tenant Software as a Service (SaaS) product. As an enterprise product, UCWG includes the ability to interact and integrate with customer (USPTO) directory services and single sign on capabilities to provide authentication for internal or confidential content. That integration occurs via USPTO's Single Sign-On Okta system.

(a) Whether it is a general support system, major application, or other type of system
UCWG is a FedRamp Software as a service system (SaaS).

(b) System location
The system location is a FedRAMP cloud SaaS hosted by Cisco Systems Inc. All data and accompanying PII is stored in this cloud. There is no physical on-premise location for the UCWG system.

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

UCWG interconnects with the following systems:

1. **ICAM Identity as a Service (ICAM IDaaS)** system provides an enterprise authentication and authorization service to all applications/AIS's

2. **Network and Security Infrastructure (NSI)** system facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO applications.

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

UCWG provides meeting links to meeting participants and hosts. Meeting hosts join the meeting via the meeting links from their computer browser. Meeting participants join meeting via the meeting links using their browser or WebEx mobile app. Meeting content includes video, audio, and data from meeting participants.

(e) How information in the system is retrieved by the user
Name and email address information and meeting content is retrieved by authorized USPTO staff and contractors via web browsers on authorized USPTO computer devices and networks connected to the WebEx for Government as a Service (SaaS) cloud.

Authorized USPTO staff and contractors via web browsers on authorized USPTO computer devices and networks connected to the WebEx for Government as a Service (SaaS) cloud can schedule meetings and manage video recording access.

USPTO staff, contractors, and public users participate in meetings via web browsers using web browsers or WebEx mobile apps.

USPTO staff, Contractors, and Public users can access and view recorded WebEx Meetings that have been approved for and configured for public viewing.

(f) How information is transmitted to and from the system
UCWP connects with USPTO Okta system for SAML 2.0 user authentication to UCWP. During user authentication, UCWG sends a SAML Request to the USPTO's Okta Service using the user's browser HTTP-Redirect Binding. Okta returns a SAML Response to the Okta using the user's browser HTTP-POST Binding.

Information is transmitted to and from the system via the WebEx for Government as a Service (SaaS) cloud. End users connect to UCWG via their Internet Browser or WebEx mobile app.

(g) Any information sharing conducted by the system
Authorized USPTO staff and contractors have access to the data stored on the UCWG System. The public can access the recorded meetings on a case-by-case basis if the host makes the recording available. The recording can be disseminated to attendees including members of the public and the receiver can disseminate the recording without prior approval from the host.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
The citation of the legal authority to collect PII and/or BII is 5 U.S.C 301, 35 U.S.C. 2, and E.O.12862.

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

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

☒ This is a new information system.

☐ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions	☐	d. Significant Merging	☐	g. New Interagency Uses	☐
b. Anonymous to Non-Anonymous	☐	e. New Public Access	☐	h. Internal Flow or Collection	☐
c. Significant System Management Changes	☐	f. Commercial Sources	☐	i. Alteration in Character of Data	☐
j. Other changes that create new privacy risks (specify):					

☐ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

☐ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (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): Geographic Region					

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): A meeting participant's video could transmit distinguishing features via a person's appearance or voice.					

System Administration/Audit Data (SAAD)					
a. User ID	☒	c. Date/Time of Access	☒	e. ID Files Accessed	☒
b. IP Address	☒	d. Queries Run	☒	f. Contents of Files	☒
g. Other system administration/audit data (specify):					

Other Information (specify)
Files uploaded during meetings can be accessed by the hosts and participants.

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 PII in UCWG is secured using appropriate administrative, physical, and technical safeguards in accordance with the FedRAMP Moderate Impact-SaaS Authorization. All access has role-based restrictions via USPTO Role Based Access System via SAML 2.0, 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 a part of verifying the integrity of data.

UCWG provides meeting links to meeting participants and hosts. Meeting hosts join the meeting via the meeting links from their computer browser. Meeting participants join meetings via the meeting links using their browser or WebEx mobile app. Meeting content includes video, audio, and data from meeting participants.

For public users, a display name and email address is collected, used, and maintained. However, the display name and email address is not used to authenticate the public users (no authentication is required). The display name and email address that the public user enters is also not verified and it can be anything the user choses; such as:
Display name: Fake Person
Email address: fakeaddress@makebelieve.com
In this context, the display name and email address are considered to be a form of User ID.

For authorized USPTO internal users, name and email address is collected, maintained, and used by the system. However, authentication occurs via Single-Sign-On and only once the user is already authenticated to their PTONet account and only after the user acknowledges the USPTO warning banner. UCWG does not use internal users' email addresses for authentication. In this context, the email address is considered to be a form of User ID.

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):			

☐	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): Make improvements to the Service; Provide user support; To authenticate and authorize account user access; Diagnose technical issues; Respond to Customer support requests.			

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).

UCWG collects PII from government employees, contractors, and members of the public. UCWG is used for administrative matters by facilitating meetings with others. UCWG promotes information sharing initiatives through collaboration capabilities that incorporate data, voice, and video communication technologies. UCWG improves online federal services as well as employee and customer satisfaction by enabling global employees and virtual teams to collaborate in real time from anywhere, anytime, on mobile devices or video systems as though they were working in the same room. The UCWG team also provides user support via remote desktop support and troubleshooting using UCWG.

5.2 Describe any potential threats to privacy 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.)

Foreign and adversarial entities, insider threats, and computer failure are adverse risk events that could potentially expose PII data about USPTO employees or contractors stored within the system. To mitigate the risk of these adverse events, the servers storing the potential PII are located in a highly sensitive zone within the USPTO internal network and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved and authorized accounts. Physical access to servers is restricted to only a few authorized individuals. All systems are subject to monitoring that is consistent with applicable regulations, agency policies, procedures, and guidelines. UCWG is continually monitored to provide "near real-time" risk reporting and mitigation activities. Additionally, users undergo annual mandatory training regarding appropriate handling of information.

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/BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: ICAM-OKTA NSI The security safeguards for the UCWG meet the NIST SP 80-53 (Rev. 4) requirements set forth System Security Plan (SSP) and in the USPTO Cybersecurity Baseline Policy. The Security Plan specifically addresses the management, operational, and technical controls that are in place and planned during the operation of the enhanced system. All systems are subject to monitoring that is consistent with applicable regulations, agency policies, procedures, and guidelines. The system is implemented with encryption (SSL). Authorized users have role-based permissions. UCWG is continually monitored to provide "near real-time" risk reporting and mitigation activities. PII in UCWG is secured using appropriate administrative, physical and technical safeguards in accordance with the applicable federal laws, Executive Orders, directives, policies, 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 and changes as part of verifying the integrity of data. Information is protected through a layered security approach which incorporates the use of secure authentication, access control, mandatory configuration settings, firewalls, Virtual Private Network (VPN), and encryption, where required. Internally within USPTO, data transmission confidentiality controls are provided by PTONet.
☐	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: Authorized WebEx users have access to information as disclosed in their privacy policy accessible at https://www.cisco.com/c/en/us/about/legal/privacy.html	
☒	Yes, notice is provided by other means.	Specify how: Prior to joining WebEx meeting, users must accept a warning banner. Cisco provides a link to system privacy statement in meeting help about window. See Appendix A: Warning Banner
☐	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

☒	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: For members of the public, they can chose 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 UCWG via the USPTO computer used to access content.

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	Specify why not: USPTO Employees and Contractors consent to providing information for the primary purpose of acquiring

	uses of their PII/BII.	access to applications and network during on boarding when they accept their USPTO PTONet credentials. Public users agree to UCWG Warning Banner before joining a meeting.

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: USPTO account holders may login to uspto.WebEx.com and update their PII held in their account profile and preferences. 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 a UCWG SaaS database. That PII is monitored and tracked by USPTO on an as-needed basis.
☒	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): ☒ 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 supporting 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 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).*

The security safeguards for the UCWG meet the NIST SP 80-53 (Rev. 4) requirements set forth System Security Plan (SSP) and in the USPTO Cybersecurity Baseline Policy. The Security Plan specifically addresses the management, operational, and technical controls that are in place and planned during the operation of the enhanced system. All systems are subject to monitoring that is consistent with applicable regulations, agency policies, procedures, and guidelines. The system is implemented with encryption (SSL). Authorized users have role-based permissions. UCWG is continually monitored to provide "near real-time" risk reporting and mitigation activities.

Management Controls:

a) The USPTO uses the Life Cycle review process to ensure that management controls are in place for EDMS-C. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the Security Plan. The Security Plans specifically address the management, operational and technical controls that are in place, and planned, during the operation of the enhanced system. Additional management controls include performing national agency checks on all personnel, including contractor staff.

b) The USPTO uses the Personally Identifiable Data Extracts Policy. This means no extracts of sensitive data may be copied on to portable media without a waiver approved by the DOC CIO.

Operational Controls:

a) Access to all PII/BII data is for users on PTONet who have verified access to EDMS-C. Additionally, access to PII/BII data is restricted to a small subset of EDMS-C users.

b) Manual procedures are followed for handling extracted data containing sensitive PII which is physically transported outside of the USPTO premises. In order to remove data extracts containing sensitive PII from USPTO premises, users must:

    1. Maintain a centralized office log for extracted datasets that contain sensitive PII. This log must include the date the data was extracted and removed from the facilities, a description of the data extracted, the purpose of the extract, the expected date of disposal or return, and the actual date of return or deletion.
    2. Ensure that any extract which is no longer needed is returned to USPTO premises or securely erased and that this activity is recorded on the log.
    3. Obtain management concurrence in the log, if an extract aged over 90 days is still required.
    4. Store all PII data extracts maintained on a USPTO laptop in the encrypted My Documents directory. This includes any sensitive PII data extracts downloaded via the USPTO Virtual Private network (VPN).
    5. Encrypt and password-protect all sensitive PII data extracts maintained on a portable storage device (such as CD, memory key, flash drive, etc.). Exceptions due to technical limitations must have the approval of the Office Director and alternative protective measures must be in place prior to removal from USPTO premises.

USPTO is using the following compensating controls to protect PII data:

a) No extracts of sensitive data may be copied on to portable media without a waiver approved by the DOC CIO. The request for a waiver must include specifics as to how the data and device are protected, how long the data will be maintained, and how the data on the device will be deleted when no longer required.

All laptop computers allowed to store sensitive data must have full disk encryption.

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 and number *(list all that apply)*: COMMERCE/DEPT-23 Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs. COMMERCE/PAT-TM-19: Dissemination Events and Registrations COMMERCE/DEPT-18: Employees Personnel Files Not Covered by Notices of Other Agencies. COMMERCE/DEPT-20: Biographical Files and Social Networks.
☐	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 5.1, item 020: Non-recordkeeping copies of electronic records • GRS 5.2, item 020: Intermediary 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 Levels

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 levels. *(Check all that apply.)*

☒	Identifiability	Provide explanation: UCWG collects, maintains, or disseminates PII about DOC employees, contractors, and members of the public. The types of information collected, maintained, used or disseminated by the system may include Name, user id, and work email, etc. which are personal identifiers. When combined, this data set can be used to identify a particular individual.
☒	Quantity of PII	Provide explanation: USPTO has 400 accounts that can host online meetings. Each meeting captures name and email address of meeting attendees, etc. Meetings content can be recorded.
☒	Data Field Sensitivity	Provide explanation: Data fields may include name, login id, phone number, and email address for USPTO employees and contractors who are account holders, which alone or in combination have little relevance outside the context. For non-account holders, data fields may include name and email address which alone or in combination have little relevance outside the context.

☒	Context of Use	Provide explanation: UCWG is primarily a transport mechanism, the information provided by virtual meeting participants is restricted to meeting hosts and authorized system administrators. Enterprise User Id is used to identify and authorize USPTO system account holders. For Federal and Public users, name and email address may be 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. System use and General Personal Data are used to make improvements to the service, provide user support, diagnose technical issues, and respond to Customer support requests. Video, audio, and shared data are used to facilitate performing "face to face" communication in a virtual environment. Meeting Content information provided through the use of the Services, such as meeting recordings (i.e., video and audio), files, your votes, chat logs and transcripts, and any other information uploaded while using the Services is collected and maintained are used to capture meeting experience for on demand access via online service portal. Name, Login ID and email address are collected and maintained in audit logs and that information is used to capture system usage.
☒	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. In accordance with the Privacy Act of 1974, PII must be protected.
☒	Access to and Location of PII	Provide explanation: PII is secured using appropriate administrative, physical and technical safeguards in accordance with the FedRAMP Moderate Impact SaaS Authorization. Authorized USPTO staff and contractors have access to the data stored on the UCWG System. UCWG does not disseminate PII information to any other systems.
☐	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. 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. In addition to insider threats, activity which may raise privacy concerns include the collection, maintenance, and dissemination of PII in the form of name and personal and work name, telephone number and email address as well as user ID and date/time access. 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.

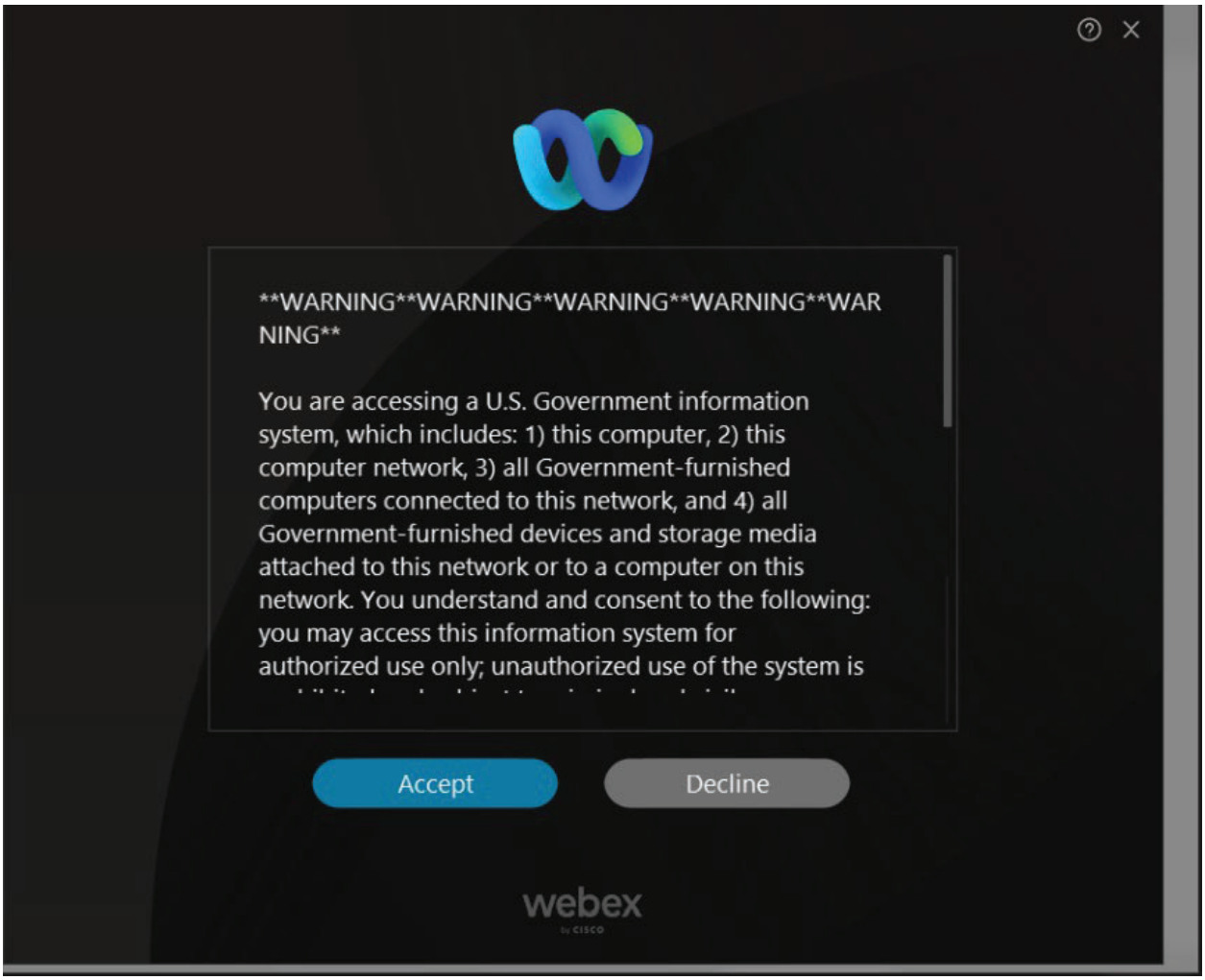
12.2 Indicate whether the conduct of this PIA results in any required business process changes.

☐	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.

Appendix A: Warning Banner



USPTO Points of Contact and Signatures

System Owner
Name: Randy Hill
Office: Collaborative Services Division
Phone: (571) 272-8983
Email: Randy.Hill@uspto.gov

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

Signature: Users, Hill, Randy Digitally signed by Users, Hill, Randy Date: 2021.10.27 11:09:11 -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

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

Signature: DON R Watson Digitally signed by DON R Watson Date: 2021.11.02 09:40:53 -04'00'

Date signed: _____

Privacy Act Officer
Name: John (Ricou) Heaton
Office: General Law Office (GLO)
Phone: (571) 270-7420
Email: Ricou.Heaton@uspto.gov

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

Signature: Users, Heaton, John (Ricou) Digitally signed by Users, Heaton, John (Ricou) Date: 2021.10.21 09:22:58 -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

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

Signature: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2021.11.02 10:55:41 -04'00'

Date signed: _____

Co-Authorizing Official (if applicable)

Name: N/A
Office: N/A
Phone: N/A
Email: N/A

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

Signature: _____

Date signed: _____

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