United States Department of Justice

Privacy Impact Assessment

for the

Webex Meetings

Approved by:

Peter Winn

Chief Privacy and Civil Liberties Officer (Acting)

U.S. Department of Justice

Date approved: August 2, 2022

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

Webex Meetings (Webex) is real-time collaboration software from Cisco Systems (Cisco) that the United States Department of Justice (DOJ or "the Department")[1] uses for video and voice conferencing. In addition to video and voice conferencing, Webex users can share documents, meeting notes, and presentations, and collaborate on content through the whiteboard note-taking feature. When specifically approved, users may record a video conference. Users may connect to Webex online or by telephone. DOJ uses the FedRAMP[2] authorized Cisco Webex for the U.S. Government platform.

DOJ conducted this Privacy Impact Assessment (PIA) because the information collected, maintained, used, or disseminated by the system includes personally identifiable information[3] (PII) about individuals, such as contact information (emails, phone numbers, and names), and video images and voice, which may be recorded when specifically authorized. However, since Webex is hosted by a third-party, DOJ does not maintain this data, except users who maintain recordings when authorized. While only DOJ personnel, including employees, contractors and other individuals assigned to the Department (DOJ users), may schedule meetings using the DOJ iteration of Webex, the system may capture information about other individuals, including other federal employees or members of the public who attend DOJ meetings. Given the free flow of information during a video or voice conference, there is the potential that a significant amount of personally identifiable information, including information related to civil or criminal litigation, may be shared through the use of Webex. This PIA is intended to encompass the use of Webex by Department components in their ordinary course of business.

---

[1] Prior to using Webex, individual DOJ components must certify that they have read this PIA and will utilize Webex in a manner consistent with the activities described herein. DOJ components that wish to use Webex in a manner that is beyond the scope of this PIA must complete a separate PIA, or provide an addendum to this PIA, that the Department, where practicable, will publish on the DOJ PIA webpage: https://www.justice.gov/opcl/dojprivacy-impact-assessments.

[2] The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a "do once, use many times" framework that saves cost, time, and staff required to conduct redundant Agency security assessments. Additional information is available at https://www.fedramp.gov/faqs/.

[3] Personally identifiable information (PII), defined in OMB Memorandum M-07-16 "Safeguarding Against and Responding to the Breach of Personally Identifiable Information"), as information in identifiable form as defined in Section 208(d) of the E-Government Act of 2002 ("the definition of 'identifiable form' means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means."). PII may also include device identifiers, data and telemetry (such as IP or MAC address) when such data is linked or tied to a specific person's device. If Webex links other data with an individual's personal information, Cisco will treat that linked data as personally identifiable information.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

In order for the Department to efficiently execute its mission, DOJ components and its personnel require a reliable, secure way to host video and voice conference events to increase productivity, efficiency, and reduce travel expenses. Webex enables DOJ users (also referred to as "hosts" in this PIA) to conduct meetings and attend conferences or trainings from a desktop, laptop, or mobile device, as permitted by their individual components' policy and licensure.[4] Webex is intended to provide a stable digital conferencing platform for moderate to large group meetings. The Department offers Webex as a shared service to components; however, some components may elect to procure their own Webex license.[5]

Webex users include internal DOJ users, other federal government users, state, tribal, or local government users, or members of the public. To administer Webex, DOJ relies on a role-based system. Webex users are assigned a role as either (1) administrator, (2) host, or (3) attendee. These roles can be further subdivided using various permissions, as deemed appropriate within the component or for a specific meeting's needs. Within DOJ components, each section/office can designate administrators, who assign roles, devices, and services that may be used by hosts and attendees. Administrators may also perform some basic trouble-shooting duties such as resetting passwords and finally escalating troubleshooting issues to Cisco. All DOJ users who are given permission to schedule meetings and invite attendees may serve as hosts. Attendees may include DOJ employees, approved DOJ contractors and external attendees, including members of the public (attendees are also referred to as "guests" in this PIA).

When a host establishes a meeting and invites attendees, an invitation e-mail is sent to attendees, which contains a link to the meeting and a password, which is required to access the meeting. Each component may place limitations on a host's abilities, such as requiring access to the Webex system through their government-issued laptop or mobile device. Attendees will be able to access the meeting from any device with internet access, or by dialing a designated dial-in telephone number.

Webex provides the option to record a meeting. However, pursuant to Department policy, recordings are only permitted if prior authorization has been obtained.[6] Webex automatically provides notice to attendees if a Webex meeting will be recorded. Absent prior authorization and notice to all participants, a meeting will not be recorded. Those authorized to use the recording function may store such recordings on their government approved devices. If the note taking whiteboard feature is

---

[4] Each component may establish their own user procedures within the parameters established by this PIA. These procedures may include designating specific DOJ users as administrators, the number of Webex events permitted per component, event type, functionality and accessibility limitations, such as permitting digital recordings of an event or transcription.

[5] Components may choose to utilize a third-party vendor to obtain their Webex license. These vendors do not have access to Webex data.

[6] Each component will determine the requirements for granting recording authorization.

activated, the host may download the collaborative content at the conclusion of the meeting to their computer.[7] Cisco does not maintain any copies of the recordings or collaborative content.
Cisco manages the system for the Department, thus log data is collected and maintained by Cisco. Cisco generates statistical reports for DOJ that may be stored by the DOJ administrators on the DOJ network for no longer than 90 days.[8] Cisco may log attendee names, contact information including email addresses or telephone numbers, if used, and user roles as required to facilitate meetings and issue meeting invitations. Cisco regularly provides DOJ with usage and trending reports which do not contain PII.[9] The Department uses a third-party vendor to facilitate billing with Cisco who collects the name(s) and contact information of DOJ Contracting Officers and Contracting Officers' representatives.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority		**Citation/Reference**
X	Statute	• Federal laws that authorize the Attorney General to create and maintain federal records of agency activities, including but not limited to 5 U.S.C. § 301 and 44 U.S.C. § 3101 • Federal Records Act, 44 U.S.C. § 3301
	Executive Order	
	Federal Regulation	
	Agreement, memorandum of understanding, or other documented arrangement	
X	Other (summarize and provide copy of relevant portion)	• DOJ Electronic Messaging Records Retention Instruction 0801.04.02 • Presidential Memorandum—Building a 21st Century Digital Government, May 23, 2012 • Memorandum on Transparency and Open Government, January 21, 2009

[7] The meeting host must enable this note-taking feature for use during a specific meeting. The whiteboard may be a blank document or a template that the host provides for the attendees to write upon and annotate. At the conclusion of the meeting, the host may save the notes of attendees or the collaborative content displayed during the meeting to their computer. If not saved at the conclusion of the meeting, the notes will be erased. Webex does not save any notes or collaborative documents. Only participants who join the meeting from video system or video conferencing applications will be able to see or annotate any shared content such as the whiteboard function.
[8] DOJ administrators use a meeting control hub which serves as a control panel to run reports on certain general usage data/statistics, monitor number of active users based on limited licenses. The hosts' usage information is kept for ninety days by Cisco.
[9] Usage/trend reports include data such as inactivity, number of meetings hosted, whether the meetings are audio- or web-based, and the number of Webex meetings held in a month.

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

While Cisco offers a comprehensive suite of features for Webex users,[10] DOJ only uses the Webex functions needed to conduct virtual meetings, events and trainings.[11] The table below depicts both the possible data that may be captured by DOJ during the use of Webex and the types of data Cisco collects on behalf of DOJ.[12] Due to the varied nature of the Department's work, recordings of video or voice conferences could potentially include almost any type of unclassified PII. It is not possible to list with certainty every type of information that may be collected, maintained, or disseminated by the Department through the use of Webex.

[10] For non-DOJ clients that may use more of the features of Webex, a comprehensive list of all the data being collected, maintained and used by Cisco can be found in Cisco Privacy Data Sheet, available at https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/cisco-webex-meetings-privacy-data-sheet.html#1OverviewofCiscoWebexMeetingsCapabilities.

[11] DOJ uses Cisco Webex Meetings Suite, Cisco Webex Events, and Cisco Webex Training portion of the Cisco for U.S. Government platform.

[12] DOJ has access to the information stored by Cisco upon request or DOJ Webex admins can directly access the Cisco Control Hub to run usage reports. DOJ only maintains usage data and statistics, much of which come from Cisco-generated usage reports that do not link to a specific user.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C, and D	Cisco collects names and usernames of site administrators, hosts, and attendees, which may include members of the public. Additionally, recordings may capture virtually any type of unclassified PII.
Physical address	X	A, B, C, and D	Cisco may collect this information. Mailing addresses may be added by the user into their profile but is not a requirement to use a Webex account. Additionally, recordings may capture virtually any type of unclassified PII.
Business email address	X	A, B, C, and D	Cisco collects business email addresses from attendees participating in Webex meetings. Additionally, recordings may capture virtually any type of unclassified PII.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Business phone number	X	A, B, C, and D	Recordings may capture virtually any type of unclassified PII.
Date of birth or age	X	A, B, C, and D	Recordings may capture virtually any type of unclassified PII.
Place of birth			
Gender	X	A, B, C, and D	Recordings may capture virtually any type of unclassified PII.
Race, ethnicity or citizenship	X	A, B, C, and D	Recordings may capture virtually any type of unclassified PII.
Religion	X	A, B, C, and D	Recordings may capture virtually any type of unclassified PII.
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	A, B, C, and D	Cisco may collect this information. Physical mailing addresses may be added by the user into their profile but is not a requirement to use a Webex account. Additionally, recordings may capture virtually any type of unclassified PII.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Personal e-mail address	X	A, B, C, and D	Cisco collects personal email addresses from attendees participating in Webex meetings. Additionally, recordings may capture virtually any type of unclassified PII.
Personal phone number	X	A, B, C, and D	Recordings may capture virtually any type of unclassified PII.
Medical records number			
Medical notes or other medical or health information	X	A, B, C, and D	Recordings may capture virtually any type of unclassified PII.
Financial account information			
Applicant information	X	A, B, C, and D	Recordings may capture virtually any type of unclassified PII.
Education records	X	A, B, C, and D	Recordings may capture virtually any type of unclassified PII.
Military status or other information	X	A, B, C, and D	Recordings may capture virtually any type of unclassified PII.
Employment status, history, or similar information	X	A, B, C, and D	Recordings may capture virtually any type of unclassified PII.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C, and D	Recordings may capture virtually any type of unclassified PII.
Certificates			
Legal documents	X	A, B, C, and D	Recordings may capture virtually any type of unclassified PII.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Device identifiers, e.g., mobile devices	X	A, B, C, and D	Cisco collects host and attendee device identifiers, IP addresses, browser type (whether the user accessed the meeting though mobile app or web-based browser). Cisco's data analytics can only determine which users are DOJ users versus guests. It cannot trace the IP address to a specific individual. Additionally, recordings may capture virtually any type of unclassified PII.
Web uniform resource locator(s)	X	A	Cisco collects unique meeting URLs linked to the meeting ID and user when creating an IT Service Desk ticket for service.
Foreign activities	X	A, B, C, and D	Recordings may capture virtually any type of unclassified PII.
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, and D	Recordings may capture virtually any type of unclassified PII.
Juvenile criminal records information	X	A, B, C, and D	Recordings may capture virtually any type of unclassified PII.
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C, and D	Recordings may capture virtually any type of unclassified PII.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Whistleblower, e.g., tip, complaint or referral	X	A, B, C, and D	Recordings may capture virtually any type of unclassified PII.
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C, and D	Recordings may capture virtually any type of unclassified PII.
Procurement/contracting records			
Proprietary or business information	X	A, B, C, and D	Recordings may capture virtually any type of unclassified PII.
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C, and D	Cisco may collect this information. Hosts may upload photographs for their Webex user profiles but is not a requirement to use a Webex account. Additionally, recordings may capture virtually any type of unclassified PII.
- **Video containing biometric data**	X	A, B, C, and D	Video recordings are likely to capture facial images.
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**	X	A, B, C, and D	Video recordings will capture voice.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
- **Scars, marks, tattoos**	X	A, B, C, and D	Recordings may capture virtually any type of unclassified PII.
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:	X	A	Both Cisco and DOJ capture a record of the authorized users with admin capabilities.
- **User ID**	X	A, B, C, D	Cisco collects this information.
- **User passwords/codes**	X	A, B, C, D	Cisco collects this information.
- **IP address**	X	A, B, C, D	Cisco collects this information.
- **Date/time of access**	X	A, B, C, D	Cisco collects this information.
- **Queries run**	X	A	Cisco collects this information.
- **Content of files accessed/reviewed**	X	A	Cisco collects this information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
- **Contents of files**	X	A, B, C, and D	DOJ may retain video recordings and other collaborative content depending on the usage options enabled by the component. The recording metadata collected could include meeting/event date, time subject, names of all attendees, case project file name/number (if appropriate), recording save location (url or file path, if appropriate)

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Other (please list the type of info and describe as completely as possible):	X	A, B, C, and D	WebEx is an online collaboration tool that may collect, host, and/or disclose significant quantities of information relating to work at DOJ. Because of the varied nature of DOJ's work and because WebEx could conceivably include almost any type of unclassified PII, it is not possible to list with certainty every item of information that will be collected, maintained, or disseminated by the system.

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person	X	Hard copy: mail/fax		Online	X
Phone	X	Email	X		
Other (specify): Information may be received from an individual via tablet, computer, smartphone or telephone.					

Government sources:					
Within the Component	X	Other DOJ Components	X	Online	X
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented	X		

Government sources:					
		arrangement related to the transfer): Foreign government participants may share their information under the same terms as any other participant. This sharing is entirely voluntary and not pursuant to any international agreement.			
Other (specify):					

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	X
Commercial data brokers					
Other (specify):					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X			Information collected by DOJ, primarily recordings, will only be shared on a case-by-case basis as needed.
DOJ Components	X			Information collected by DOJ, primarily recordings, will be shared on a case-by-case basis as needed.
Federal entities	X			Information collected by DOJ, primarily recordings, will be shared on a case-by-case basis as needed.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
State, local, tribal gov't entities	X			Information collected by DOJ, primarily recordings, will be shared on a case-by-case basis as needed.
Public	X			Information collected by DOJ, primarily recordings, will be shared on a case-by-case basis as needed.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Information collected by DOJ, primarily recordings, will be shared on a case-by-case basis as needed.
Private sector	X			Information collected by DOJ, primarily recordings, will be shared on a case-by-case basis as needed.
Foreign governments	X			Information collected by DOJ, primarily recordings, will be shared on a case-by-case basis as needed.
Foreign entities	X			Information collected by DOJ, primarily recordings, will be shared on a case-by-case basis as needed.
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

No information will be released from Webex for Open Data purposes.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

DOJ provides individuals with generalized notice about its collection, use, and sharing of PII through a variety of Systems of Records Notices (SORNS), and, in some instances, individualized notice pursuant to Section 552a(e)(3) of the Privacy Act.[13] For meetings that will be recorded, participants are given explicit notice prior to the start of the meeting that the event will be recorded. The types of information potentially collected, used and shared through the use of Webex is covered under several applicable SORNS.

- Individuals have been notified that account information, audit logs, and user records maintained by the Department to plan and manage system services are covered under JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full 86 Fed. Reg. 1352 (Jul. 14, 2021).
- Webex information such as shared/sent meeting invites are covered by JUSTICE/DOJ-003 Correspondence Management Systems (CMS) for the Department of Justice, 66 Fed. Reg. 29992 (Jun. 4, 2001), 66 Fed. Reg. 34743 (Jun. 29, 2001), 67 Fed. Reg. 65598 (Oct. 25, 2002), and 82 Fed. Reg. 24147 (May 25, 2017).
- DOJ employee records maintained in this system are covered by JUSTICE/DOJ-014, Department of Justice Employee Directory Systems, last published in full at 74 Fed. Reg. 57194 (Nov. 4, 2009) and modified at 82 Fed. Reg. 24151, 153 (May 25, 2017).

In addition to the limited information that may be collected, used, and/or shared by the Department, Cisco collects the information that Webex users provide, in accordance with their terms of service and privacy policies.[14]

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

Individuals outside of DOJ voluntarily provide information to participate in Webex meetings. For individuals within DOJ, the information technology section creates user profiles based on information pulled from DOJ's Active Directory such as name and email.[15] Opportunities exist for users to provide additional information to associate with their profile when signing up for a Webex account but is not required.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

---

[13] Additional information about the Department's use of third-party websites and applications, can be found at https://www.justice.gov/doj/privacy-policy#website.
[14] Cisco's Webex privacy policy is available at https://www.cisco.com/c/en/us/about/legal/privacy-full.html.
[15] Components may use Active Directory services to support a single sign-on solution for active user accounts. This provides identity management to allow accessibility of users to services and resources within DOJ. Once users have cleared this verification process, they do not need to sign-on again to access DOJ resources and systems. Active directory requires users to submit a unique password and undergo multi-factor authentication in a single sign-on process before gaining access to all DOJ resources.

All users may access or amend their Webex profile data at any time. Access or amendment requests for user records that are maintained by DOJ can be requested in accordance with DOJ regulations, and in accordance with JUSTICE/DOJ-002, "Department of Justice Information Technology, Information System, and Network Activity and Access Records," last published in full 86 Fed. Reg. 1352 (Jul. 14, 2021). Recordings of meetings document what occurred in the video conference, e.g., what was said by whom, and cannot be amended.

Individuals seeking to gain further access to information within Webex that is maintained by DOJ may request amendment or correction of their respective information, may do so by making a FOIA and/or Privacy Act request by following the provisions of those statutes and DOJ regulations on those statutes. Further instructions on how to submit a request are provided at Part 16 of Title 28, Code of Federal Regulations.[16]

Cisco has detailed the procedures for individuals to request access, rectification, suspension of processing or deletion of personal data in the Privacy Data Sheet, available at https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/cisco-webex-meetings-privacy-data-sheet.html#11Howtoexerciseyourdatasubjectrights.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including the development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** Each DOJ component must have their own ATO. Accordingly, the date of the most recent ATO will vary, depending on the individual component. **If an ATO has not been completed, but is underway, provide status or expected completion date:** JMD ATO—To be updated when the transition to the provider is complete. CRM ATO—November 17, 2022 **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:**

[16] The Electronic Code of Federal Regulations is accessible here: https://www.ecfr.gov.

	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** Webex Collaboration Security Operations manages and maintains compliance of configuration changes required for Webex maintenance, vulnerability management, and all continuous monitoring aspects of the system. They will also perform configuration changes to improve the Webex Collaboration System security posture when necessary. These activities include updating vendor products, updating configuration baselines to remediate vulnerabilities, applying all security patches, and editing of continuous monitoring profiles to increase auditing capabilities. At DOJ there are assigned Information System Security Officers (ISSOs) to ensure that all security controls are in place and relevant information is uploaded in Cyber Security Assessment and Management (CSAM) System, the Department's system inventory application. Webex system is reviewed annually, as required for a FISMA system that has been designated as "moderate" under FIPS 199.[17] Component information technology teams will ensure all necessary cybersecurity controls are in place and that all FISMA/FedRamp compliance documentation is completed before the use of the system.[18]
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** Webex follows the Audit and Accountability (AU) controls outlined by NIST 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations.[19] Auditing provides visibility into important security events via log files and suspicious events are forwarded to the Department's Splunk[20] for correlation, reporting, and archiving on a regular basis. Webex audit and accountability procedures are reviewed annually, and audit and accountability policies are reviewed every three years.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**. Contractors are responsible for complying with the applicable policies and procedures in accordance with the security posture established by Cisco senior management and with applicable contracts with DOJ. Cisco requires basic security awareness training for

[17] FIPS 199 stands for Federal Information Processing Standards Publication 199. For more information see https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.
[18] For safeguarding information and dealing with cybersecurity issues Cisco's Security and Trust Organization coordinates the Data Incident Response Process and manages the enterprise-wide response to data-centric incidents.
[19] See https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.
[20] The Department's iteration of Splunk captures, indexes, and correlates "real-time" event data in a searchable repository from which IT and information security staff can generate graphs, reports, alerts, dashboards, and visualizations of various events. The Splunk solution provides insight into operational, security, and functional aspects of the environment. Splunk is covered under separate privacy documentation.

	employees and contractors that support the operation of the contractor system. Those who have additional access will have information security technical training for them to understand their information system security roles.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** No additional training is necessary for Webex users. However, prior to accessing Webex, and subsequently on an annual basis, all DOJ users must complete computer security awareness training, as well as review and agree to comply with DOJ information technology Rules of Behavior. System administrators will complete additional professional training, including security training and the Role-Based IT Professional Training-Security Awareness for Privileged Users. System administrators will complete additional professional training, including security training and the Role-Based IT Professional Training-Security Awareness for Privileged Users.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

The following access and security controls have been utilized to protect privacy by reducing the risk of unauthorized access and disclosure:

- Webex has a security categorization of FISMA moderate as described in NIST Special Publication 800-53.[21] DOJ uses the FedRAMP government certified version.[22] As a result, the system has assessed and implemented applicable security controls to ensure protections commensurate with the impact to the Department from unauthorized access or disclosure of information.

- Webex restricts access to log data only to individuals designated as system administrators with a specific need to review that data. Only system administrators are granted access to search and retrieve the meeting data within the administrator's component. Host users may only access their own account and meeting data. Attendees have an even more limited role within Webex; they do not have access to any of the data beyond their individual profile within the meeting.

- Webex is protected by multiple firewalls, an intrusion prevention system, real-time continuous monitoring using malicious code detection and protection, encryption, and other technical controls in accordance with applicable security standards.

[21] *See* https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.
[22] This system's FIPS 199 categorization is set at moderate for confidentiality and integrity, while the availability is set at low.

- Profile photos and mailing addresses are not required to use Webex.

- Webex makes it clear to users, through visual indicators, when a meeting contains participants that are not part of their organization. Webex meetings can be moderated such that moderators have exclusive control of the room's participants.

- Webex encrypts all passwords and user-generated information. Web-based information transmitted during customer connections are encrypted using the highest level of encryption supported, consistent with applicable standards. Only FIPS-compliant algorithms are used by Webex.

- Data collected from Webex meetings are stored for ninety days for Cisco to run back-end performance reports.

- For DOJ users authorized to record meetings, Webex clearly displays to participants via video that recording is in progress.[23] The DOJ Webex host must immediately save the recording following the meeting or it will be erased. Cisco does not retain copies of recorded meetings. Recordings are only permitted for hosts who have received prior authorization from their component.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

Cisco maintains data collected from Webex for ninety days for the purposes of providing back-end analytics to the Department.

Information stored within the Department is to be retained and disposed of in accordance with the General Records Schedule retention schedule applicable to such information.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. __X___ Yes.

[23] When an individual calls into a Webex meeting and is unable to see the visual notification that the meeting is being recorded, there will be an audio notification that recording is in process when the host activates the recording feature. Users who have dialed into a Webex meeting via the telephone after the recording has been initiated may not know that recording is in progress. After the initial audio announcement, the host will need to announce that the feature has been activated. For users joining via video, they will receive a pop-up notification that the meeting is being recorded and must click an affirmative response prior to joining the meeting. The meeting will be clearly marked as being recorded.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

- JUSTICE/DOJ-002 Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full 86 Fed. Reg. 37188 (Jul. 14, 2021).

- JUSTICE/DOJ-003 Correspondence Management Systems (CMS) for the Department of Justice, 66 Fed. Reg. 29992 (Jun. 4, 2001), 66 Fed. Reg. 34743 (Jun. 29, 2001), 67 Fed. Reg. 65598 (Oct. 25, 2002), and 82 Fed. Reg. 24147 (May 25, 2017).

- JUSTICE/DOJ-014, Department of Justice Employee Directory Systems, last published in full at 74 Fed. Reg. 57194 (Nov. 4, 2009) and modified at 82 Fed. Reg. 24151, 153 (May 25, 2017).

- Other SORNs may also apply for specific DOJ components, depending on component use of the system and matters discussed in WebEx sessions.

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical and physical controls over the information.***

The primary privacy risks associated with the Department's use of Webex are unauthorized access or misuse of PII. Risks to individual privacy exist any time PII is made available to the Department. Individuals who interact with the Department using Webex may submit additional information to the Department when participating in virtual meetings. When an individual interacts with the Department through this communication system, they may post PII in comments or share PII with the Department through direct messaging or during verbal discussions. These interactions may expose the Department to the user's PII. To mitigate this risk, the Department has administrators who may limit the capabilities available during the meeting, for example turning off the comment function or limiting occasions during which attendees may speak freely. Further, the host acts as the gatekeeper for those authorized to attend. Meeting invites sent by DOJ employees or administrators are directed to specified individuals, inviting them to attend a specific meeting.

During DOJ hosted meetings, users outside of DOJ may participate as attendees. Both groups of users (internal to DOJ and outside of DOJ) have same user capabilities: attend meetings, use the white board feature, if activated, and the ability to share their screen, change their user name, raise their hand, and type in the chat during a meeting. Users can also take screenshots of the meeting at any time via their own device. The DOJ host(s) have more control during a meeting. They can record a meeting, if authorized, share documents which may be downloaded by attendees, override all volume controls, enable waiting rooms, lock meetings and enable passwords for their meetings for access control purposes.

DOJ has taken additional efforts to limit recordings. The issuance of DOJ Policy Memorandum, *Recording Department Meeting/Event Platforms*, in February of 2022 established DOJ policy for the use and maintenance of content captured, created, or shared using recording capabilities in Webex.[24] The policy specifically states that the recording capability must only be used in limited circumstances where the recording is necessary and permitted by law. Recordings should not be used to replace traditional meeting minutes or notes. Components should establish written component-level policy that identifies appropriate uses for recording capabilities based on component mission and function requirements. The Policy states that recordings must not remain on individual drives, such as OneDrive, but rather, should be moved to the appropriate recordkeeping repository as necessary. The Webex host who made the recording must ensure the safe storage and handling of any recordings with sensitive information. A recording may be shared with non-participants only after analyzing the associated privacy risks, including whether PII has been protected appropriately and whether sufficient notice was provided to the participants in the recording. In the event that a recorded training is shared for later viewing, the sharing process should minimize the duplication of the files so that viewing permissions are provided for the file rather than transmitting a copy of the file.

Next, the risk of collecting erroneous or inaccurate information from individuals is mitigated by only collecting what is necessary. While Cisco may offer facial recognition features, capabilities for automated assistant to hold simultaneous rooms and meetings, some level of artificial intelligence to provide a more personalized user experience for other clients, DOJ's usage of Cisco does not include these additional features.[25] Webex is not designated as an official record-keeping system for substantive information. Substantive information is to be retained within the Department and disposed of by the components themselves, in accordance with the retention schedule applicable to such information. Attendees have access to their own profile and may correct that information at any time. Recordings of meetings are unable to be altered.

To mitigate the risk that Webex may inadvertently contain information from another DOJ system, Webex does not connect to any DOJ major or minor system. DOJ users must be verified by DOJ's Active Directory and be admitted onto the DOJ network before they are eligible to use Webex on their web and mobile devices. Cisco manages Webex, not DOJ.

---

[24] DOJ recordkeeping policies follow 44 U.S.C. §§ 3101 *et seq;* 5 U.S.C. § 301and DOJ Order 0801 Records and Information Management.

[25] For more information, see the four addendums in the Cisco Privacy Data Sheet https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/cisco-webex-meetings-privacy-data-sheet.html#AddendumOnePeopleInsightsfeatureforCiscoWebex.

As mentioned, Cisco has implemented a number of privacy mitigation strategies including not selling personal data, not tracking user usage data for advertising purposes, and not interfering with meeting traffic or content. Cisco offers technical security measures to Webex users such as encrypting data in transit.[26] In the event of a breach, Cisco's Security and Trust Organization coordinates the Data Incident Response Process on an enterprise-wide level by having a breach and incident notification process in place.

Furthermore, Cisco has created a variety of online resources for Webex users to mitigate the misuse of PII. Cisco's Webex Help Center provides best practices for hosts with tips for scheduling meetings, security during meetings,[27] and suggestions to either delete or password protect recordings stored by the Department post-meeting. Additionally, Cisco provides best practices for site administrators and their use of the meeting control hub, where administrators have the ability to manage the number of active users, the number of licenses and run statistical analysis reports.[28]

According to Cisco's data retention plan, user information will be kept as long as the user maintains an active subscription. For users whose accounts are terminated, they immediately lose access to Webex, but their name and user ID are maintained for ninety days from date of termination. The hosts' usage information is kept for ninety days while billing information may be maintained for seven years. DOJ maintains user data for no more than ninety days as set by DOJ administrators.

---

[26] Host and usage information is only encrypted in transit but not at rest. Cisco has stated that any data not encrypted at rest is protected by highly secure data center protection mechanisms and operational procedures. *See* https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/cisco-webex-meetings-privacy-data-sheet.html#7Personaldatasecurity.

[27] To enhance security during a meeting, Cisco suggests that users restrict access to the meeting, validate the identity of all participants, remove a participant when necessary, control who can share their screens, and end the meeting rather than just leaving a meeting.

[28] DOJ uses the FedRAMP-certified Webex offered by Cisco. Not all features are authorized or needed for DOJ to conduct day to day business. DOJ administrators' meeting control hub simply consists of ability to run reports on certain general usage data/statistics, monitor number of active users based on limited licenses.