Office of Government Ethics

Cisco Webex
Privacy Impact Assessment

August 2022
Information Technology Division

U.S. Office of Government Ethics (OGE)
Privacy Impact Assessment (PIA) for Cisco Webex

Provide electronic copies of the signed PIA to OGE's Chief Information & Cybersecurity Officer and Privacy Officer.

Name of Project/System: Cisco Webex
Office: Information Technology Division

Executive Summary

Webex by Cisco is a third-party web-based video conference application. OGE uses Webex to enable employees and contractors to communicate and collaborate with each other and with individuals outside of the agency, including agency ethics officials, Congressional staff, and members of the public. In addition to the privacy controls utilized in OGE's implementation of Webex, Cisco has its own security and privacy program that includes security requirements, threat modelling, secure design and coding, static analysis, vulnerability testing, privacy impact assessments, and third-party security assessments. More information on Cisco's security and privacy program is available on its website here. The Cisco online privacy statement is available here.

OGE uses Webex for internal and external video conferences. An internal OGE user will schedule the video conference and participants are emailed a web link and/or call in telephone number to join at the scheduled date and time. The application gives users an option to enter their telephone number and have Webex call them to join the videoconference. During video conferences, participants may chat with the group or privately. It also has a registration tool that allows OGE to register participants for webinars conducted via the application.

This PIA covers OGE's practices regarding the use of Webex for discussions and/or presentations that do not involve sensitive personally identifiable information (PII) as part of their content. It also describes additional restrictions on the use of Webex for discussions that do involve sensitive PII as a part of their content (for instance to discuss disciplinary measures against a specific individual).[1] In order to use Webex for the latter, OGE users should submit a Privacy Threshold Analysis (PTA) prior to that use being implemented and abide by the additional restrictions described below.

[1] These additional restrictions apply only when the Webex system is used for a meeting or conversation where PII is discussed or shared. Participants may avoid these requirements by having an in-person meeting or by conducting the meeting by conference call instead of by Webex.

A. CONTACT INFORMATION:

1) Who is the person completing this document

Jennifer Matis
Associate Counsel
Legal, External Affairs and Performance Branch
Program Counsel Division
jmatis@oge.gov
202-482-9216

2) Who is the system owner:

Ty Cooper
Chief Information & Cybersecurity Officer
Information Technology Division
jtcooper@oge.gov
(202) 482-9226

3) Who is the system manager for this system or application:

Tony Upson
Network Architect
Information Technology Division
tupson@oge.gov
(202) 482-9272

4) Who is the Chief Information Security Officer (CISO) who reviewed this document?

Ty Cooper
Chief Information & Cybersecurity Officer
Information Technology Division
jtcooper@oge.gov
(202) 482-9226

5) Who is the Senior Agency Official for Privacy who reviewed this document?

Diana J. Veilleux
Senior Agency Official for Privacy and
Chief, Legal, External Affairs and Performance Branch
Program Counsel Division
Diana.veilleux@oge.gov
202-482-9203

6) Who is the Reviewing Official?

Ty Cooper
Chief Information & Cybersecurity Officer
Information Technology Division
jtcooper@oge.gov
202-482-9226

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes, it contains information about current OGE employees, contractors, employees of other federal, state, and local agencies and members of the public. Information collected includes the name, organizational affiliation, telephone number, and/or email address of OGE users and internal or external participants. Generally, the telephone numbers and email addresses are official government contact information, but it is possible that personal telephone numbers and email addresses may be used.

Because Webex is a communication system, it is possible for any kind of personally identifiable information about individuals to be communicated through a chat, audio participation, or screen sharing. However, OGE has promulgated a policy prohibiting users from preserving Webex meetings or chat conversations in any manner. Moreover, OGE employees are counseled on what information is appropriate to share via Webex.

If a user needs to record a meeting or preserve a chat conversation, they must first submit a PTA and receive explicit approval to do so. Moreover, as noted above, Webex may not be used to communicate sensitive PII unless the user first submits a PTA and complies with the additional restrictions described below, which include making meetings unlisted or placing restrictions on unauthenticated users attempting to join a meeting.

a. Is this information identifiable to the individual?

Potentially, yes.

b. Is the information about individual members of the public?

Potentially, yes.

c. Is the information about employees?

Potentially, yes.

2) What is the purpose of the system/application?

OGE uses Webex to enable employees and contractors to communicate and collaborate with each other and with individuals outside of the agency, including agency ethics officials, Congressional staff, and members of the public. See the Executive Summary above for more information.

3) What legal authority authorizes the purchase or development of this system/application?

The Ethics in Government Act of 1978, as amended, authorizes the Director of OGE to provide overall direction of executive branch policies related to preventing conflicts of interest on the part of officers and employees of any executive agency. See 5 U.S.C. app. § 402. Use of a video conferencing application to communicate internally and with external stakeholders is an essential part of conducting agency business. With regard to use of Webex for training delivery and registration, OGE's responsibilities include supporting agency ethics officials through such training, advice, and counseling as the Director of OGE deems necessary. See 5 C.F.R. § 2638.108(a)(5).

4) What protections are in place to secure communications regarding sensitive PII?

Webex may not be used to communicate sensitive PII unless the user first submits a PTA and complies with the following additional restrictions.

a. When scheduling the meeting, the user should ensure that the meeting is marked as "unlisted" by checking that that the "Listed on public calendar" box is **unchecked**.

b. Do not put any PII in the meeting topic. (For example, do not name the meeting "Discussion about John Doe discipline.")

c. When scheduling the meeting, the user should mark the "Automatic lock" box and select that the system will automatically lock the meeting 0 minutes after the meeting starts. Doing so will require at least one OGE user to log into the system to perform host duties and allow participants into the meeting. The user serving in this role is responsible for ensuring that only invited participants are allowed into the video conference. If no OGE user is available to log into the system and monitor participants, the meeting should be conducted via telephone conference call rather than Webex.

C. <u>DATA in the SYSTEM:</u>

1) What categories of individuals are covered in the system?

- OGE employees and contractors

- Employees of other federal, state, and local agencies
- Members of the public

2) What are the sources of the information in the system?

For OGE employees and contractors the information is collected from a manually typed collection of OGE Employee Name and Email Address Book data via an Excel Spreadsheet, which is then manually imported into each Webex Account and utilized when a video conference is scheduled using the system. For individuals outside of OGE (officials from other government entities or members of the public), the information is provided directly by the individuals.

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

See above.

b. What federal agencies provide data for use in the system?

None.

c. What State and local agencies are providing data for use in the system?

None.

d. From what other third party sources will data be collected?

N/A.

e. What information will be collected from the employee and the public?

The system collects OGE employees' and contractors' names and email addresses when they are participants in a video conference using the system. For participants who are not OGE employees or contractors, the only required information is email addresses. Custom fields such as organizational affiliation can be added to the registration process. Users can also input a telephone number to have the system dial them in to the meeting. The system has the capability to record video and audio and archive chats, but OGE does not use those functions.

3) Accuracy, Timeliness, Reliability, and Completeness

a. How will data collected from sources other than OGE records be verified for accuracy?

The OGE employee and contractor information in the system is maintained by the system manager, who will check it for accuracy and completeness in the course of agency operations. When OGE hires new employees or contractors their name and new OGE email address will be added into the system, and their information will be removed from the system once employees or contractors leave OGE. For non-OGE participants, it is their responsibility to provide OGE with accurate and complete information.

b. How will data be checked for completeness?

See above.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date?

Yes. OGE employee and contractor information in the system is maintained by the system manager, who will check it for accuracy and completeness in the course of agency operations. When OGE hires a new employee or contractor, their name and new OGE email address is added into the system that Webex accesses for scheduling and notification of video conferences. This information will be deleted if an employee or contractor leaves OGE. For non-OGE participants, it is the individual's responsibility to provide OGE with accurate and complete contact information.

d. Are the data elements described in detail and documented?

No. However, the data elements are simple and self-explanatory.

D. ATTRIBUTES OF THE DATA:

1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

No.

3) **Will the new data be placed in the individual's record?**

N/A.

4) **Can the system make determinations about employees/the public that would not be possible without the new data?**

N/A.

5) **How will the new data be verified for relevance and accuracy?**

N/A.

6) **If the data is being aggregated, what controls are in place to protect the data from unauthorized access or use?**

N/A.

7) **If data is being aggregated, are the proper controls remaining in place to protect the data and prevent unauthorized access?**

N/A.

8) **How will the data be retrieved? Does a personal identifier retrieve the data?**

The personal data in the application is primarily for use by the application to notify and identify users and is not retrieved by individuals. To the extent that data is retrieved from the application by users (e.g. when sending materials to webinar participants), retrieval will be by event date or topic--not by personal identifier. If a user needs to retrieve data by personal identifier, they must first submit a PTA and comply with any additional restrictions recommended by the Privacy Officer.

9) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

N/A.

10) **What opportunities do individuals have to decline/refuse to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses)?**

Individuals do not have any opportunity to decline to provide the information or to consent to particular uses of the information.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

N/A.

2) Is the data in the system covered by existing records disposition authority? If yes, what are the retention periods of data in this system?

Yes, the records are covered by DAA-GRS-2013-0007-0012 General Records Schedule 4.2: Information Access and Protection Records (Personally identifiable information extract logs).

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

Timely destruction of federal records is the responsibility of the Agency Records Officer. The reports are temporary and will be destroyed when they are no longer needed by the agency for business use. The procedures are documented in OGE's record's management policies. The system has the capability to record video and audio and archive chats, but OGE does not use those functions.

4) Is the system using technologies in ways that the OGE has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No.

5) How does the use of this technology affect public/employee privacy?

The application has no significant effect on public/employee privacy. The PII collected by the application is not sensitive and is necessary for OGE to conduct its normal business processes. The impact on privacy is justified by the need for the information.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

No.

7) What kinds of information are collected as a function of the monitoring of individuals?

N/A.

8) What controls will be used to prevent unauthorized monitoring?

N/A.

9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.

N/A. None of the information is retrieved by name or other unique identifier. When the application is used for hosting webinars, the information is retrieved by session date or topic, not by individual registrants.

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

N/A.

F. ACCESS TO DATA:

1) Who will have access to the data in the system?

All meeting participants can see the names of other participants while the meeting is live. OGE has both restricted Webex accounts ("restricted account") and accounts open to all internal OGE users ("open accounts"). When meetings or webinars are scheduled with an open account, all OGE employees and contractors will have access to the participant information (name, email address and possibly organization) associated with that event. When meetings or webinars are scheduled with a restricted account, such as *Integrity*.oge, only users with access to that account will have access to the participant information associated with the event.

No one has access to telephone numbers entered into the application, except the individual who entered the number.

2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Access to OGE applications and user accounts is governed by the Account Access Request Form (AARF) process, which authorizes the Information Technology Division (ITD) to create, modify, and disable network accounts, including providing access to OGE applications. AARF requests must be signed by the employee, his/her supervisor, and the Chief Information & Cybersecurity Officer before a request is approved to be implemented by ITD staff. Although anyone with an invitation may participate in an OGE-hosted Webex video conference, the AARF process restricts administrative access to the application and OGE user accounts.

3) Will users have access to all data on the system or will the user's access be restricted? Explain.

See above.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?**

The data is nonsensitive and generally available to all OGE employees and contractors through other authorized means. There is no potential for unauthorized browsing.

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?**

No contractors were involved with the design, development, or maintenance of the application.

6) **Do other systems share data or have access to the data in the system? If yes, explain.**

There is no direct interface with other systems. The application has e-mail address information to send invitations, notifications and calendar items to participants directly from the application. The emails and calendar items do not indicate the other individual participants scheduled to participate.

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

N/A.

8) **Will other agencies share data or have access to the data in this system (Federal, State, or Local)?**

No.

9) **How will the data be used by the other agency?**

N/A.

10) **Who is responsible for assuring proper use of the data?**

Each user is responsible for assuring proper use of the data collected.

See Attached Approval Page

The Following Officials Have Approved the PIA for Cisco Webex:

1) **System Manager**

Initials: TU Date: 8/9/2022

Name: Tony Upson
Title: Network Architect,
Information Technology Division

2) **System Owner**

Initials: TC Date: 8/8/2022

Name: Ty Cooper
Title: Chief Information & Cybersecurity Officer,
Information Technology Division

3) **Chief Information Officer**

Initials: TC Date: 8/8/2022

Name: Ty Cooper
Title: Chief Information & Cybersecurity Officer
Information Technology Division

4) **Senior Agency Official for Privacy**

Initials: DJV Date: 08/03/22

Name: Diana Veilleux
Title: Chief
Legal, External Affairs and Performance Branch
Program Counsel Division