FARM CREDIT ADMINISTRATION
PRIVACY IMPACT ASSESSMENT

SYSTEM, PROGRAM, OR PROJECT NAME

Cisco Webex

SYSTEM TYPE

Information Technology System or Capability

PURPOSE

The Farm Credit Administration uses the Cisco Webex for Government platform for videoconferencing and teleconferencing to enable FCA and Farm Credit System Insurance Corporation (FCSIC) employees and contractors to communicate and collaborate with each other and with individuals outside FCA and FCSIC. These individuals include employees of Farm Credit System (FCS) institutions; employees of other federal, state, and local agencies; and members of the public.

AUTHORITY

12 U.S.C. 2252, 2254

INFORMATION OVERVIEW

Covered Persons	Included
Employees of Farm Credit System (FCS) institutions	☒
Farm Credit institution customers	☐
FCA employees, contractors, interns	☒
Employees of other federal agencies	☒
Members of the public	☒

Personally Identifiable Information (PII)X	Included
Full name	☒
Date of birth	☐
Place of birth	☐
Social Security number (SSN)	☐
Employment status, history, or information	☒
Mother's maiden name	☐
Certificates (e.g., birth, death, naturalization, marriage)	☐
Medical information (medical record numbers, medical notes, or X-rays)	☐
Home address	☐
Phone number(s) (nonwork)	☒
Email address (nonwork)	☒
Employee identification number (EIN)	☐
Financial information	☐
Driver's license/State identification number	☐
Vehicle identifiers (e.g., license plates)	☐

Legal documents, records, or notes (e.g., divorce decree, criminal records)	☐
Education records	☐
Criminal information	☐
Military status or records	☐
Investigative report or database	☐
Biometric identifiers (e.g., fingerprint, voiceprint)	☐
Photographic identifiers (e.g., image, X-ray, video)	☒
Other: System-generated administrative data (audit and use information for FCS, FCA, and FCSIC users, such as meeting duration, participants, or call quality); personal identity verification (PIV) card numbers; and meeting ID information for meeting rooms	☒

LIFE CYCLE NARRATIVE

The Cisco Webex for Government platform is a cloud-based collaboration platform that allows authorized users to hold virtual meetings in real time with audio-only and video participants. Meetings are managed by using an internet browser or desktop application on which a suite of collaboration tools allow participants to share documents, applications, and presentations; to use remote desktop capabilities; and to chat. If meeting recording is enabled, meeting hosts can record the meeting and disseminate the recording a half-hour after the meeting ends. Participants can connect to meetings using their computers or telephones. FCA uses Webex both for internal meetings (staff and contractors only) and for meetings that include nonagency personnel.

As part of a Webex meeting, a variety of PII may be processed. For example, PII related to a specific institution's borrowers may be shared in a meeting between employees of an FCS institution and FCA employees in the Office of Examination. Likewise, other meetings, such as board meetings, which are open to the public and hosted via Webex, may include nonsensitive information or otherwise public information.

PII shared via Webex is not stored on the platform and comes from other IT systems that are subject to their own privacy compliance rules. In addition to information that is shared during a meeting, each participant must supply some PII to participate in a meeting: name, email address, telephone number, and job title or employer information. The platform will also capture images (both photo and video) and voice recordings.

The type of meeting determines what information is collected. In general, nonagency participants enter their names and email addresses or telephone numbers on a web form. In some cases, such as a public FCA board meeting, the names of the participants' employers may also be required. For agency personnel, FCA's IT infrastructure system automatically fills in the user's ID or user name, telephone number, and email address to facilitate authentication of the participant's identity. Employees hosting a meeting may also need to enter a meeting ID or PIN assigned to them for the meeting.

When the system collects information directly from users — both from internal and external users — we provide a Privacy Act statement, which references the applicable system of record notice (SORN) and explains how information collected will be used.

Recipients of this notification who discover incorrect information or information that is no longer relevant may be able to directly correct the information in their Webex accounts. In other cases, they can request access to or amendment of their information in accordance with the Privacy Act and FCA's Privacy Act regulations, as outlined in 12 CFR Part 603. Users are also provided a copy of FCA's web privacy policy. In addition, FCA has published this PIA and, where applicable, relies on the SORN to provide notice to individuals whose PII has been collected.

Finally, information in the system may be shared within the agency to facilitate public and internal communications, and externally in accordance with the routine uses identified in the applicable SORN. Any external sharing of information must be within the scope of the agency's authorities and regulations and facilitate a specific FCA business function. In addition, Cisco, which provides the Webex service to FCA, outlines how the system handles information in the Cisco Online Privacy Statement.

COMPLIANCE WITH APPLICABLE STATUTES, REGULATIONS, AND REQUIREMENTS

For each statute or regulatory requirement indicate applicable sections of statutes, regulations, or requirements and provide links to them, or provide a brief description of compliance. If a certain requirement is not applicable to Webex, indicate with N/A.

The Privacy Act of 1974 (As Amended)	
System of records notice(s)	FCA's use of Cisco Webex is covered by the Privacy Act system of records: FCA-8 – FCA Information Technology User Access and Usage Records — FCA, available at 85 FR 51430.
Computer Matching and Privacy Protection Act of 1980	
Notice of computer matching agreement(s)	N/A — FCA does not have any computer matching agreements that pertain to this system.
The Paperwork Reduction Act of 1995	
Office of Management and Budget (OMB) control number(s) or related form(s)	N/A — FCA does not have any OMB control numbers or forms associated with this system.
The Federal Records Act of 1950 (As Amended)	
Record(s) control schedule name(s) and number(s)	Records are maintained in accordance with FCA's comprehensive records schedule and the National Archives and Records Administration's general records schedule.
Other	
N/A	N/A

ADMINISTRATIVE AND TECHNOLOGICAL CONTROLS

☒	All applicable controls for protecting PII as defined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Appendix J, and NIST SP 800-122 have been implemented and are functioning as intended, have compensating controls in place to mitigate residual risk, or have an approved plan of action and milestones.
☒	The system has been reviewed for and assigned a categorization level in accordance with NIST Federal Information Processing Standards (FIPS) Publication 199 and NIST SP 800-60, and the senior agency official for privacy has approved the categorization. FIPS 199 Security Impact Category: ModerateModerate
☒	A security assessment has been conducted for the system, and it has been determined that there are no additional privacy risks.
☒	The information system has been secured in accordance with Federal Information Security Modernization Act requirements. Most recent assessment and authorization type: Authorization to Use (ATU) and date: 8/27/2020 ☐ This is a new system, and the assessment and authorization date is pending.
☒	A comprehensive listing of data elements included in the system has been provided to the privacy officer, reviewed and approved, and included in the agencywide PII inventory.
☐	System users are subject to or have signed confidentiality or nondisclosure agreements, as applicable.
☒	System users are subject to background checks or investigations. FCA employees undergo background checks. Because Webex is a solution authorized by the Federal Risk and Authorization Management Program (FedRAMP), certain personnel at Webex are also subject to background checks.
☒	System access is limited to authorized personnel with a bona fide need to know in support of their duties.
☒	Notice is provided in the form of a Privacy Act statement, privacy notice, privacy policy, or similar, as applicable.
☐	Contracts or agreements (e.g., memorandums of understanding, memorandums of agreement, and information security agreements) establish ownership rights over data, including PII.
☒	Acceptance of liability and responsibilities for exposure of PII are clearly defined in agreements or contracts.
☒	Access to and use of PII are monitored, tracked, and recorded.

☒	Training on PII, confidentiality, and information security policies and practices is provided to system users or those with access to information.

ADMINISTRATIVE AND TECHNOLOGICAL CONTROLS NARRATIVE

Webex is a solution authorized by FedRAMP for use at the moderate level, and FCA's chief information officer (CIO) and authorizing official has granted the system an Authorization to Use. The agency secures information in the system by a variety of means, including the following:

- Physical security controls of FCA facilities and data centers that house system components
- Use of transport layer security connections and multifactor authentication
- Access controls and application of the principle of least privilege (i.e., users have only the information access and system permissions required to do their jobs)
- Application, network, server, and database activity logs, which are reviewed when abnormalities arise or when requested by the CIO or chief information security officer (CISO)
- Security policies, procedures, and end-user guidance for secure use of Webex and other videoconferencing solutions

FCA has implemented a baseline set of security measures, in accordance with Cisco guidance, to ensure Webex is adequately secured from improper access. These measures include the following:

- Requiring the use of strong passwords for meetings
- Making meetings unlisted (i.e., the topic and other details of the meeting are not made public)
- Placing restrictions on unauthenticated users attempting to join a meeting

Also, FCA has disabled access to users' meeting-recording capabilities. Only Webex users with Webex "events" accounts may record meetings, and only with the CIO's explicit permission.

FCA policy limits staff's access to Webex. The platform can be used only for FCA business purposes (i.e., no personal use), and generally only FCA employees may have accounts. A contracting officer may request an account for a contractor with valid business needs in support of his or her work at FCA.

All FCA users receive annual IT security and privacy awareness training and are responsible for reviewing and attesting to the requirements described in FCA IT security and personal use policies, including the agency's Rules of Behavior. Finally, FCA has made guidance available to all employees on appropriate use of Webex and other videoconferencing capabilities, including best practices for ensuring the security of sensitive information discussed or exchanged on these platforms.

PRIVACY RISK ANALYSIS

The following overview of the primary risks associated with FCA's use of Webex includes a description of mitigations the agency has put in place for each.

Data minimization: To minimize the risk of unnecessary or inadvertent data collection or access caused by user error or misuse (specifically, collection of video and audio and collection of information related to nonagency users such as phone numbers and email address), FCA has the following safeguards in place:

- Restricting the use of the recording capability to users granted access and authorization by the CIO
- Standardizing the information participants from outside FCA must provide to participate in an FCA-sponsored Webex videoconference
- Informing end users that FCA Webex accounts are not for personal use

Data confidentiality, including access or use by unauthorized users: There is a risk that sensitive PII could be compromised during a Webex meeting either through sharing on the platform during a meeting or through a video or

audio recording. As previously described, FCA has implemented the security controls and best practices Cisco recommends to reduce the risk that external parties could access FCA Webex videoconferences. Also, as noted above, we limit who can record meetings. Further, the agency has issued guidance on securely using videoconferencing capabilities, such as Webex.

Transparency: There is a risk that participants in an FCA Webex meeting who are not FCA staff may be unaware that Webex collects or accesses their PII and, in some cases, their likeness (if the meeting is being recorded). We have mitigated this risk by publishing this PIA, restricting recording capabilities in Webex, and providing disclosures and notices to participants in recorded meetings. FCA also has published a SORN, FCA-8, to provide additional notice of the collection and use of PII for Webex meetings.

Overall risk: Overall, FCA's use of Webex presents limited privacy risk. Though the system facilitates the sharing of potentially sensitive PII related to FCA activities, the system's primary collection, use, and storage of PII is limited to less sensitive information that participants provide voluntarily, such as names and contact information, limited employment information (associated with contact information), audio, video, and photos. The agency has implemented a variety of technological and administrative controls to reduce the risk of unnecessary collection of PII and unauthorized access to or use of PII. The agency also has provided training and awareness materials to users on securing meetings and information shared in meetings. Finally, the agency has published this PIA and the associated SORN, FCA-8, to inform individuals of the collection and use of PII through Webex.

DOCUMENT CONTROL

Approval

/s/_____ Wesley Fravel, FCA privacy officer	/s/_____ Jeannie Shaffer, CISO
/s/_____ Ruth Surface, associate director, infrastructure division	/s/_____ Jerry Golley, CIO and senior agency official for privacy

Change Control and Approval History

Version	Date	Change Summary
V 1.0	2/8/2021	Initial Version