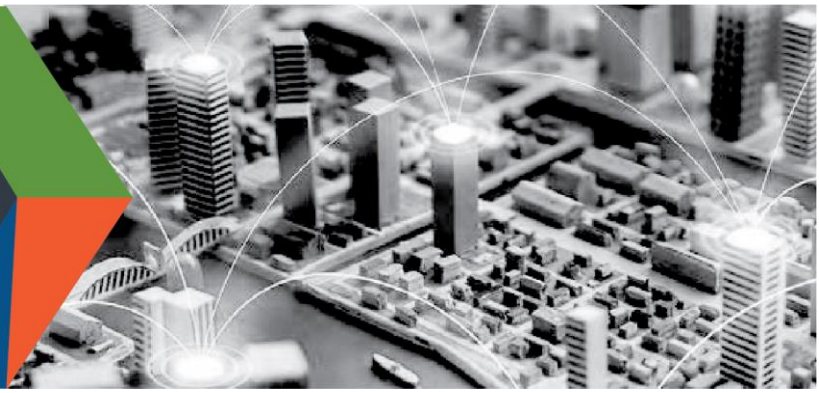
CISA
CYBER+INFRASTRUCTURE
DEFEND TODAY, SECURE TOMORROW



CYBERSECURITY RECOMMENDATIONS FOR CRITICAL INFRASTRUCTURE USING VIDEO CONFERENCING

This videoconferencing product is for executives charged with securing critical infrastructure networks, and for critical infrastructure employees to help them think through related cybersecurity and physical issues.

RAPID INCREASE IN ADOPTION AND DEPLOYMENT OF VIDEO CONFERENCING

American companies and government agencies are increasingly adopting workplace flexibilities such as telework. Advances in information technology, such as the increased availability of video conferencing software and video conferencing capabilities incorporated into other products like collaboration software, facilitate telework. Users are likely to need video conferencing and other collaboration solutions to stay connected as they telework. It is critical that cybersecurity requirements and risk exposure for products be counterbalanced appropriately against remote access product benefits such as convenience, usability, speed, and stability.

The following advisory guidance is intended to support the incorporation of cybersecurity considerations when adopting or expanding the use of video conferencing software and related collaboration tools. The guidance also includes suggestions for individuals using these tools to host and attend meetings—information that is particularly critical as organizations increasingly broadcast sensitive discussions over these platforms.

As the authority for securing telework, the **Cybersecurity and Infrastructure Security Agency (CISA)** established this product line. We plan to continue refining it and consider releasing additional products related to the secure use of online collaboration tools and video conference solutions to further support the ongoing efforts of cybersecurity leaders during this period of maximum telework. Please send your feedback to CyberLiaison@cisa.dhs.gov.

POTENTIAL THREAT VECTORS

Cyber adversaries, from nation-state actors to insiders and criminal organizations, seek to acquire information on research and development, critical infrastructure, and personally identifiable information. Additionally, some actors, seek to disrupt the operations of American institutions and misuse systems for politically motivated causes. Some tactics include cyber actors:

- Actively exploiting unpatched vulnerabilities in client software to gain access to organizational networks and carry out cyber exploitation and cyberattacks;
- Exploiting communication tools to:
    - Take users offline by overloading services, or

  - Eavesdropping on meetings or conference calls;
- Hijacking video-teleconferences by inserting pornographic images, hate images, or threatening language;
- Compromising remote desktop applications (used in some telework solutions to enable remote desktop sharing for collaboration and presentations) to infiltrate other shared applications; and
- Attempting to penetrate sensitive meetings by using social engineering to deceive individuals into divulging information (e.g., meeting links) or by inferring meeting links from other links that use a common structure (e.g., company_name_YYYY_MM_DD).

Some video conferencing products may unintentionally expose information to nefarious cyber actors. For example, some of these products may share or sell customer information to third parties or target users to integrate product use with their personal social media accounts. This data sharing can unintentionally expose employee and organizational information beyond intended recipients.

RECOMMENDED ENTERPRISE SECURITY PRACTICES

1. Assess your organizational needs and determine the appropriate product to use in the enterprise. Also consider the mission need for your organization to collaborate with outside entities. Examine supply chain concerns (e.g., vendor reputation, data center locations) and whether the service under consideration addresses your organization's other security, legal, and privacy requirements.
2. Establish an organizational virtual meeting policy or recirculate the policy if it already exists. Ensure updated guidance is continuously available. Develop a one-page summary of policies applicable to virtual meetings that is easily digestible by end users.
3. Limit and minimize the number of collaboration tools authorized for use in the enterprise to reduce the attack surface and the overall amount of vulnerabilities. Develop a list of approved collaboration and videoconferencing tools for your organization. Review and update security settings continuously. Scan for and remove all unauthorized collaboration tools and associated clients from the enterprise. Centrally manage authorized clients and configuration settings enterprise wide. Maintain the latest version by promptly updating client software and removing all obsolete versions.
4. Prohibit end users from installing client software (including removing local administration rights). When an outside entity initiates a meeting using a collaboration tool not on an approved product list, instruct users to join web (browser) based sessions that do not require installation of client software.
5. Prevent users with administrative privileges from using collaboration tools on the system while logged on with those privileges. Administrators should not perform non-privileged operations on the systems they are administering (e.g., using email, browsing the internet, performing office automation tasks, engaging in recreational use).
6. Prohibit the use of collaboration tools and features that allow remote access and remote administration. While not the main purpose of collaboration tools, some vendors may advertise remote access software as collaboration tools and some collaboration tools may allow remote access and remote administration.
7. Clearly articulate to employees the privacy and document retention implications of your organization's collaboration tools, including any data sharing or utilization of participation or attention tracking features.

8. Ensure that your organization's telework policy or guide addresses requirements for physical and information security. Verify that users have updated telework agreements. Consider whether organizational information technology priorities need to be adjusted given the different contexts of largescale telework.

BEST PRACTICES FOR END-USERS

1. Only use organization-approved software and tools for business, including company-provided or -approved video conferencing and collaboration tools to host/initiate and schedule meetings.
2. Tailor security precautions to be appropriate for the intended audience and content of a meeting. Do not make meetings "public" unless they are intended to be open to anybody. For meetings that will be broadly attended, ensure you have the capability to mute all attendees and limit the ability of attendees to share screens.
3. Particularly when conducting meetings with a large audience, have a preestablished plan that details:
    a. The circumstances in which a meeting will be terminated if it is disrupted,
    b. Who has the authority to make that decision, and
    c. How the meeting termination will be executed.
4. For private meetings, require a meeting password and use features such as a waiting room to control the admittance of guests. For enhanced security, use randomly generated meeting codes and strong passwords and do not reuse them. Do not share a link to a teleconference on an unrestricted, publicly available social media post. If possible, disable the ability of participants to join a meeting before the host and automatically mute participants upon entry.
5. Provide the link to the meeting directly to specific people and share passwords in a separate email. If possible, require unique participant credentials, monitor meeting members as they join, and lock an event once all desired members have joined. Use features to permit removal of any meeting guest during the course of the meeting.
6. Manage screensharing, recording, and file sharing options. Consider saving locally versus to the cloud based on the specific circumstances (e.g., need to share the recording with a wide audience or the public, using company-issued equipment versus personal equipment). Change default file names when saving recordings. Make sure to consult with your organization's counsel about laws applicable to recording videoconferences and sharing materials through them. Set participant expectations on session recording, screen recording, and screen shots.
7. Consider sensitivity of data before exposing it (via screen share or upload) to video conference and collaboration platforms. When sharing a screen, ensure only information that needs to be shared is visible; close or minimize all other windows. If displaying content from organizational intranet sites in public meetings, hide the address bar from participants before displaying the content. Use common sense—do not discuss content you would not discuss over regular telephone lines. When having sensitive discussions, use all available security measures (e.g., waiting rooms and strong passwords), ensure all attendees of the meeting have a need to know, and make attendees aware of expectations for session security. Examples of information that may be unsuited to discussing via video teleconferencing software include: National Security Information, Sensitive Law Enforcement Information, Critical Infrastructure System Operations or Vulnerabilities, Continuity of Operations Plans, Personally Identifiable Information, Advanced Research and Development Projects, and

Proprietary Business Information.

8. When joining meetings initiated by third parties that use collaboration tools not approved by your organization, do not attempt to install software—join web (browser) based session instead. Do not use work email addresses to sign up for unauthorized/free tools.
9. If logging into a collaboration tool via a web browser, be careful to accurately type the domain name of the website. Be wary of links sent by unfamiliar addresses, and never click on a link to a meeting sent by a suspicious sender. Verify that meeting links sent via email are valid.
10. Ensure that your visual and audio surroundings are secure and do not reveal any unwanted information (e.g., confirm that whiteboards and other items on the wall are cleared of sensitive or personal information; confirm that roommates or family members are not within earshot of sensitive conversations). If available, make use of background replacement or blurring options in the collaboration tool.
11. Move, mute, or disable virtual assistants and home security cameras to avoid inadvertently recording sensitive information. Do not have sensitive discussions with potential eavesdroppers in your workspace or in a public area. Consider using headphones.
12. Check and update your home network. Change default settings and use complex passwords for your broadband router and Wi-Fi network and only share this information with people you trust. Choose a generic name for your home Wi-Fi network to avoid identifying who it belongs to or the equipment manufacturer. Update router software and ensure your Wi-Fi is encrypted with current protocols (such as WPA2 or WPA3), and confirm that legacy protocols such as WEP and WPA are disabled.

REPORTING

To report a cyber incident, call CISA at 1-888-282-0870 or visit www.cisa.gov.