Selecting and Safely Using Collaboration Services for Telework - UPDATE

Summary

During a global pandemic or other crisis contingency scenarios, many United States Government (USG) personnel must operate from home while continuing to perform critical national functions and support continuity of government services. With limited access to government furnished equipment (GFE) such as laptops and secure smartphones, the use of (not typically approved) commercial collaboration services on personal devices for limited government official use becomes necessary and unavoidable.

Audience

The primary audience for this guidance is U.S. Government employees and military service members engaging in telework, especially telework employing personally owned devices such as smartphones and home computers. Collaboration services vary widely in the cybersecurity functionality and assurance that they offer. By using the objective criteria detailed below, government employees and organizations can make more informed decisions about which collaboration services meet their particular needs. By following the practical guidelines, users can draw down their risk exposure and become harder targets for malicious threat actors.

Note that individual departments and agencies may provide specific services or issue specific direction for their teleworkers. This document **does not** override or supersede any official guidance provided by your organization. Consult your department or agency IT support or CIO organization for further guidance.

Criteria to Consider When Selecting a Collaboration Service

1. Does the service implement end-to-end encryption (E2EE)?
2. Are strong, well-known, testable encryption standards used?
3. Is multi-factor authentication (MFA) used to validate users' identities?
4. Can users see and control who connects to collaboration sessions?
5. Does the service privacy policy allow the vendor to share data with third parties or affiliates?
6. Do users have the ability to securely delete data from the service and its repositories as needed?
7. Has the collaboration service's source code been shared publicly (e.g. open source)?
8. Has the service and/or app been reviewed or certified for use by a security-focused nationally recognized or government body?
9. Is the service developed and/or hosted under the jurisdiction of a government with laws that could jeopardize USG official use?

Using Collaboration Services Securely

- If possible, use government furnished equipment (GFE) that is managed and intended for government use only, and utilize secure services designed for government use.
- If you download a collaboration service app, be sure you know where it came from.
- Ensure that encryption is enabled when initiating a collaboration session.
- Use the most secure means possible for meeting invitations.
- Verify that only intended invitees are participating before beginning, and throughout, each session.
- Ensure that any information shared is appropriate for the participants.
- Ensure that your physical environment does not provide unintentional access to voice, video, or data during collaboration sessions.

Table of Assessments against Criteria

Service	1 – End-to-End Encryption[5]					2 – Testable Encryption	3 – MFA	4 – Invitation Controls	5 – Minimal 3rd Party Sharing	6 – Secure Deletion	7 – Public Source Code Shared	8 – Certified Service (FedRAMP / NIAP)
	Text Chat	Voice Calls	Video Calls	File Sharing	Screen Sharing							
Adobe Connect™[i]	N	N	N	N	N	Y	Y	Y	Y	Client – Y Server – Y	N	FedRAMP
Amazon Chime™[ii]	N	N	N	N	N	Y	Y	Y	N	Client – Y Server – Y	N	FedRAMP In Progress
Cisco Webex®[iii]	Y[1]	Y[1]	Y[1]	Y[1]	Y[1]	Y	Y[1, 2]	Y[1]	Y	Client – Y Server – N[3]	N	FedRAMP
Dust	Y	N/A	N/A	N/A	N/A	N[3]	N	Y	N	Client – Y Server – Y	N	None
Google G Suite™[iv]	N	N	N	N	N	Y	Y[1]	Y[1, 4]	Y	Client – Y Server – Y[2]	N	FedRAMP
GoToMeeting®[v]	Y[1]	Y[1]	Y[1]	N/A	N/A	Y	N	Y[1]	Y	Client – Y Server – N[3]	N	None
Jitsi Meet®[vi]	Y[1]	Y[1]	Y[1]	Y[1]	Y[1]	Y	N	Y	N	Client – N[3] Server – N[3]	Y	None
Mattermost™[vii]	N	N	N	N/A	N	Y	Y[2]	Y[4]	N	Client – Y Server – N	Y	None
Microsoft Teams®[viii]	N	N	N	N	N	Y	Y	Y	Y	Client – Y[1] Server – Y[1]	N	FedRAMP
Signal®[ix]	Y	Y	N/A	Y	N/A	Y	Y	Y	Y	Client – Y Server – Y	Y	None
Skype for Business™[x]	N	N	N	N	N	Y	Y	Y	Y	Client – Y[1] Server – Y[1]	N	FedRAMP
Slack®[xi]	N	N	N	N	N	Y	Y	Y	Y[1]	Client – Y[1] Server – Y[1]	N	FedRAMP
SMS Text	N	N/A	N/A	N	N/A	N	N	N	N	Client – Y Server – N	N	None
WhatsApp®[xii]	Y	N/A	Y	Y	N/A	Y	Y	Y	Y	Client – Y Server – Y	N	None
Wickr®[xiii]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Client – Y Server – Y	Y	None
Wire	Y	Y	Y	Y	Y	Y	Y	Y	Y	Client – Y Server – Y	Y	FedRAMP In Progress
Zoom®[xiv]	Y[1]	N	N	Y[1]	N	Y	Y[1]	Y	Y	Client – Y Server – N[3]	N	FedRAMP

Legend: Y = Yes, N = No; N/A = Not Applicable

[1] Configurable

[2] Free Version - N

[3] No Published Details

[4] Partial

[5] End-to-end Encryption (E2EE) may be limited by app, browser, number of participants, or capabilities of other clients. Even without E2EE, all services (other than SMS) utilize link encryption between clients and servers whenever possible.

Assessment of Common Collaboration Services Against the Criteria

The above table presents an initial assessment of how available commercial collaboration services satisfy our security criteria. The selection of services for this initial assessment was driven by inquiries and usage from across NSA's national security customer base; this is not a comprehensive list of services or possible criteria.

NSA analysts gathered factual material from published company literature and product specifications, supplemented by other openly published analyses and basic hands-on technical observation. No formal testing was performed on products or services for this analysis. These assessment findings are meant to serve as input for government employees and organizations. Users of these services must exercise judgment when choosing a service for their particular mission telework needs.

Disclaimers

Note that this does not constitute a Qualified Products List, within the meaning of the definition of Federal Acquisition Regulation (FAR) 2.101 or a Qualified Manufacturers List under FAR subpart 9.2—Qualification Requirements. The government has not undertaken any testing or evaluation of the products listed under this analysis, but has only reviewed the published attributes of the products. The list is not all-inclusive. This list may be amended and supplemented from time to time as market research discloses other items or as new products become available. The descriptions and procedures explained in this document do not constitute or imply an endorsement by NSA/CSS, DoD, or USG of the products in question. It is intended solely for the non-commercial use of USG personnel for purpose of explaining and giving operating instructions for the use of the particular product in question. Any further use for other purposes is prohibited.

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Contact

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media inquiries / Press Desk: Media Relations, 443-634-0721, MediaRelations@nsa.gov

---

[i] Adobe Connect is a trademark of Adobe Systems, Inc.
[ii] Amazon Chime is a trademark of amazon.com, Inc.
[iii] Cisco Webex is a registered trademark of Cisco Systems, Inc.
[iv] Google G Suite is a trademark of Google, LLC
[v] GoToMeeting is a registered trademark of LogMein, Inc.
[vi] Jitsi Meet is a registered trademark of BlueJimp, SARL
[vii] Mattermost is a trademark of Mattermost, Inc.
[viii] Microsoft Teams is a registered trademark of Microsoft Corporation
[ix] Signal is a registered trademark of Signal Technology Foundation
[x] Skype for Business is a trademark of Microsoft Corporation
[xi] Slack is a registered trademark of Slack Technologies, Inc.
[xii] WhatsApp is a registered trademark of WhatsApp, Inc.
[xiii] Wickr is a registered trademark of Wickr, Inc.
[xiv] Zoom is a registered trademark of Zoom Video Communications, Inc.