Selecting and Safely Using Collaboration Services for Telework

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.

We define collaboration services as those capabilities that allow the workforce to communicate via internet-enabled text, voice, and video, and can include the sharing of files and other mission content. Collaboration can occur between two people or widened to include a large group to support mission needs.

This document provides a snapshot of best practices and criteria based on capabilities available at the time of publication and was coordinated with the Department of Homeland Security (DHS), which is releasing a similar guide: “Cybersecurity Recommendations for Federal Agencies When Using Video Conferencing Solutions.” This NSA publication is designed to provide simple, actionable, considerations for individual government users. The intent of this document is not meant to be exhaustive or based on formal testing, but rather be responsive to a growing demand amongst the federal government to allow its workforce to operate remotely using personal devices when deemed to be in the best interests of the health and welfare of its workforce and the nation.

Recommendations in this document are likely to change as collaboration services evolve and also address known vulnerabilities and threats. Users should be aware that even the most secure collaboration service cannot defend against a compromised user device.

Scope

This document provides security assessment guidance about commercially available collaboration services. It does not cover USG services designed specifically for secure communications, such as Defense Collaboration Services, Intelink Services, and others. NSA strongly recommends use of these dedicated government services, when possible, before any of the commercial services detailed below.

Assessment of individual services for this document focused on those which support multiple operating systems and platforms (e.g., both mobile and desktop).

Audience

The primary audience for this guidance are U.S. Government employees and military service members engaging in telework, especially telework employing personally owned devices such as smartphones and home computers. Teleworkers may not be able to access collaboration services on their respective government enterprise networks, and therefore turn to commercial services for collaboration on vital mission work. These 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

The criteria below identifies risks and features to consider when choosing collaboration services to support your mission. All criteria should be strongly considered but may not be fully supported based on your own operating environment and constraints. The criteria is intended to align with related USG guidance to include NIST SP 800-171r2 – *Protecting Controlled Unclassified Information in Non-Federal Systems and Organizations* (Feb 2020) and NIST SP 800-46r2 *Guide to Enterprise Telework, Remote Access and BYOD Security* (Apr 2016).

1. Does the service implement end-to-end encryption?

End-to-end (E2E) encryption means that content (text, voice, video, data, etc.) is encrypted all the way from sender to recipient(s) without being intelligible to servers or other services along the way. Some apps further support encryption while data is at rest, both on endpoints (e.g. your mobile device or workstation) and while residing on remote storage (e.g. servers, cloud storage). Only the originator of the message and the intended recipients should be able to see the unencrypted content. Strong end-to-end encryption is dependent on keys being distributed carefully. Some services such as large-scale group video chat are not designed with end-to-end encryption for performance reasons.

2. Are strong, well-known, testable encryption standards used?

Even in the absence of end-to-end encryption, NSA recommends the use of strong encryption standards, preferably NIST-approved algorithms and current IETF secure protocol standards. Many collaboration services protect data-in-transit between clients and servers via the Transport Layer Security (TLS) version 1.2 (or later) secure protocol, which is commonly used for sensitive but unclassified information. Use of published protocol standards, such as TLS and DTLS-SRTP, is preferred. If the product vendor has created its own encryption scheme or protocol, it should undergo an independent evaluation by an accredited lab. This includes not just cryptographic protocols, but also key generation.

3. Is multi-factor authentication (MFA) used to validate users' identities?

Without MFA, weak or stolen passwords can be used to access legitimate users' accounts and possibly impersonate them during use of the collaboration service. Multi-factor authentication requires that a second form of identification (code, token, out-of-band challenge, etc.) be provided to allow access to an existing account.

4. Can users see and control who connects to collaboration sessions?

The collaboration service should allow organizers to limit access to collaboration sessions to only those who are invited. This can be implemented through such features as session login passwords or waiting rooms, but preferably would support reasonably strong authentication. Users should also be able to see when participants join through unencrypted/unauthenticated means such as telephone calls.

5. Does the service privacy policy allow the vendor to share data with third parties or affiliates?

While collaboration services must often collect certain basic information needed to operate, they should protect sensitive data such as contact details and content. Collaboration information and conversations should not be shared with third parties. This could include metadata associated with user identities, device information, collaboration session history, or various other information that may put your organization at risk. Information sharing should be spelled out clearly in the privacy policy.

6. Do users have the ability to securely delete data from the service and its repositories as needed?

While no services are likely to support full secure overwrite/deletion capabilities, users should be given the opportunity to delete content (e.g. shared files, chat sessions, saved video sessions) and permanently remove accounts that are no longer used.

7. Has the collaboration service's source code been shared publicly (e.g. open source)?

Open source development can provide accountability that code is written to secure programming best practices and isn't likely to introduce vulnerabilities or weaknesses that could put users and data at risk.

8. Has the service and/or app been reviewed or certified for use by a security-focused nationally recognized or government body?

NSA recommends that cloud services (which collaboration apps rely on) be evaluated under the Office of Management and Budget (OMB) FEDRAMP program. NSA also recommends that collaboration apps be evaluated by independent testing labs under the National Information Assurance Partnership (NIAP) against the Application Software Protection Profile (PP) [1]. NSA has worked with the DHS S&T Mobile Security R&D Program to develop excellent semi-automatable testing criteria for app vetting based on the application PP [2]. These criteria include tests of how apps interact with platform resources, how they defend themselves from exploitation, the crypto libraries they use, what permissions they request, and many others.

9. Is the service developed and/or hosted under the jurisdiction of a government with laws that could jeopardize USG official use?

Since it is well documented that some countries require that communications be provided to law enforcement and intelligence services, it may not be wise for certain USG missions to be performed on services hosted or developed under certain foreign legal jurisdictions. Users should be aware that the country of origin where products were developed is not always public knowledge. This criterion was not assessed in the table on page 5.

Using Collaboration Services Securely

If possible, use government furnished equipment (GFE) that is managed and intended for government use only and secure services designed for government use.

No collaboration service can defend against a compromised device. Personal devices are often exposed to considerable risk of compromise due to failure to apply patches in a timely fashion and the installation of applications that users fail to recognize as being malicious (spyware). Resulting malware infections can access files, keystrokes, contacts, call histories, GPS locations, room audio or camera video (even when not on a call), and most any other information the device observes. Even the most secure collaboration service provides no protection against a compromised device.

Carefully managed GFE devices are often more secure than personal devices unless configuration control policies delay the deployment of critical patches. If GFE is available, it should be used. If GFE cannot be used, NSA recommends using a temporary secure operating system such as the Air Force's Trusted End Node Security (TENS) solution to create a "virtual GFE." If neither is practical, users should ensure all user accounts do not have administrator rights (which are only for managing the system) and if possible create a separate user account with low privileges for only work use. Consider using NSA's "Best Practices for Keeping Your Home Network Secure" guide to protect your personal devices.

If you download a collaboration service app, be sure you know where it came from.

Beware of potentially unwanted programs posing as legitimate collaboration apps. Many collaboration services require users to install specialized client software on their systems. If possible, install the correct client directly using the official app store. This helps ensure it is signed and legitimate. If you must download a client from a website, ensure it is from the properly signed secure (e.g. HTTPS) official website. Do not run or install clients from unexpected downloads, especially from links in email or other messaging that may have come from malicious senders. Some services allow users to avoid installing custom apps by using a web interface.

Ensure that encryption is enabled when initiating a collaboration session.

Most collaboration apps do not have specific settings to enable or disable encryption, but where they do, NSA

recommends enabling encryption. When using browser-based services, users should validate that HTTPS is enabled and check the website certificate to ensure it was issued by a trusted certificate authority.

Use the most secure means possible for meeting invitations.

Send meeting invites through other encrypted and authenticated collaboration services if possible. Do not post meeting invites in publicly accessible forums or sites. If invitations must be sent in the clear, organizers should send passwords or PINs by a separate method (e.g. email and SMS or email and phone call).

Verify that only intended invitees are participating before beginning, and throughout, each session.

Ensure that someone is in charge of verifying participants and checking if unknown participants have entered. If participants are not authenticated by the service, at least ensure that their voice or appearance is recognized. Use meeting waiting rooms if possible to allow access to be controlled.

Ensure that any information shared is appropriate for the participants.

Plan beforehand the topics to be covered and consider the implications if the conversation or materials are compromised so that you understand the risks. Be aware of screen-sharing features so that you only share your screen to display content salient to the collaboration session. If content is sensitive, ensure that it is appropriate to share with all participants. Be mindful of the affiliations of those with whom you connect.

Ensure that your physical environment does not provide unintentional access to voice, video, or data during collaboration sessions.

Be aware of your surroundings including any other communications going on (e.g. family members on phone calls or video chats, location hints if working from a sensitive location). Disable unnecessary app permissions (e.g. location services). Ensure there is no other software on your device that is actively sharing microphone data back to a remote server. Note that less-trusted devices, to include Internet of Things (IoT), often have microphones or cameras, so it may be wise to leave personal cell phones or computers in a different room if they are not being used for work.

Service	Basic Functionality	1 – E2E Encryption	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)
Cisco Webex®[9]	a, b, c, d, e	Y[1]	Y	Y[12]	Y[1]	Y	Client – Y Server – N[3]	N	FedRAMP
Dust	a	Y	N[3]	N	Y	N	Client – Y Server – Y	N	None
Google G Suite™[10]	a, b, c, d	N	Y	Y[1]	Y[1]	Y	Client – Y Server – Y[2]	N	FedRAMP
GoToMeeting®[11]	a, b, c	Y[1]	Y	N	Y[1]	Y	Client – Y Server – N[3]	N	None
Mattermost™[12]	a, b, c, e	Y	Y	Y[2]	Y	N	Client – Y Server – N	Y	FedRAMP
Microsoft Teams®[13]	a, c, d, e	N	Y	Y	Y	Y	Client – Y[1] Server – Y[1]	N	FedRAMP
Signal®[14]	a, b, d	Y	Y	Y	Y	Y	Client – Y Server – Y	Y	None
Skype for Business™[15]	a, c, d, e	Y[4]	Y[4]	Y	Y	N	Client – Y Server – N[3]	N	None
Slack®[16]	a, c, d, e	N	Y	Y	Y	N[3]	Client – N Server – N	N	FedRAMP
SMS Text	a, d	N	N	N	N	N	Client – Y Server – N	N	None
WhatsApp®[17]	a, c, d	Y	Y	Y	Y	Y	Client – Y Server – Y	N	None
Wickr®[18]	a, c, d, e	Y	Y	Y	Y	Y	Client – Y Server – Y	Y	None
Zoom®[19]	a, b, c, e	Y[14]	Y	N	Y	Y	Client – Y Server – N[3]	N	FedRAMP

Table of Assessments against Criteria

Legend: Y = Yes, N = No; (a) text chat, (b) voice conferencing, (c) video conferencing, (d) file sharing, (e) screen sharing.

[1] Configurable

[2] Free Version - N

[3] No Published Details

[4] Partial

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 an input for government employees and organizations. Users of these services must exercise judgment when choosing a service for their particular mission telework needs.

Works Cited

[1] NIAP (Mar. 1, 2019) Application Software Protection Profile, [Online] Available at https://www.niap-ccevs.org/Profile/Info.cfm?PPID=429&id=429 [Accessed Apr. 20,2020]
[2] NSA (Sep. 18, 2018) Guide "Best Practices for keeping Your Home Network Secure" [Online] Available at https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-best-practices-for-keeping-home-network-secure.pdf [Accessed Apr. 20, 2020]

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 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: 443-634-0721, MediaRelations@nsa.gov

[9] Cisco Webex is a registered trademark of Cisco Systems, Inc.
[10] Google G Suite is a trademark of Google, LLC
[11] GoToMeeting is a registered trademark of LogMein, Inc.
[12] Mattermost is a trademark of Mattermost, Inc.
[13] Microsoft Teams is a registered trademark of Microsoft Corporation
[14] Signal is a registered trademark of Signal Technology Foundation
[15] Skype for Business is a trademark of Microsoft Corporation
[16] Slack is a registered trademark of Slack Technologies, Inc.
[17] WhatsApp is a registered trademark of WhatsApp, Inc.
[18] Wickr is a registered trademark of Wickr, Inc.
[19] Zoom is a registered trademark of Zoom Video Communications, Inc.