United States Coast Guard
Authorized Telework Capabilities & Web/Videoconferencing Guidance – COVID-19

Version 1.0

USCG Authorized Telework Capabilities & Web/Videoconferencing Guidance – COVID-19

The Department of Defense Chief Information Officer (DoD CIO) is engaged in a number of initiatives to enhance the telework capabilities for all military services.

In support of expanded telework requirements, DoD Components (including USCG), must first look to leverage approved DoD Enterprise Collaboration Capabilities, which are already approved for use by all DoD users. Capabilities outside of referenced tools mentioned in this document place DoD information at risk and are not authorized to conduct internal DoD/USCG business.

Peripherals Needed for Most Authorized Telework Capabilities

- ✓ Computing Device (e.g. computer, laptop)
- ✓ CAC Reader (ActivClient and middleware required)
- ✓ Internet (WiFi)
- ✓ Camera (built-in or webcam for computers/laptops or approved peripheral)

NOTE: The videoconferencing tools listed in the **Authorized Telework Capabilities List** below may be used on government-owned USCG laptops/workstations, however restrictions do apply. The camera and microphone feature should be enabled as indicated in the green "UNCLASSIFED" banner across the top of the desktop (as shown below) for the use of audio/videoconferencing with CVR Teams.

Dell Latitude 5500, 5570, 5580 and HP ProBook 650 G5 are enabled for webcam use. Other models will be enabled in the near future. Enablement occurs automatically. If your machine did not receive the automatic update for enablement (not indicated in the "UNCLASSIFED" banner), contact your unit ISSO.

Approved external webcams for USCG laptops/workstations are available on ESUIT; Logitech HD Pro Webcam C920 and the Microsoft Lifecam Cinema H5D Web Camera. Click here to access ESUIT https://esuit.uscg.mil/ESUIT-Home/Entry/ProductList2.aspx?search=camera

CAUTION: Cameras and microphones shall be disabled in secure/classified or HIPAA sensitive spaces. NOTIFY YOUR CSO IMMEDIATELY IF FOUND.

Authorized Telework Capabilities List (On and Off the CG Network)

The table below provides authorized collaborative tools (e.g. audio/web/video conferencing) that can used on and off of the CG network.

DoD implemented Commercial Virtual Remote (CVR) Teams in order to support discussion among the workforce and with external partners to facilitate effective teleworking during the COVID-19 emergency or until other platforms for collaboration can be acquired. Therefore, the use of CVR Teams is temporary.

NOTE: Official documents SHALL NOT BE CREATED in CVR Teams. CVR Teams may be used to display, review, and discuss draft presentations or documents. Any final presentations and documents that become official records must be created, stored, and disseminated on the CGOne network. Examples of such documents include, but are not limited, documents that implement policy changes, contracts, and regulatory or adjudicative actions. The Coast Guard's preferred videoconferencing tools are CVR Teams, DoD Defense Collaboration System (DCS), and DHS HSIN (DHS HSIN does offer a free Adobe Connect instance within the HSIN tool.)

Recording video chats and chat messages is strictly prohibited!

CVR Teams is a Microsoft environment, which includes Microsoft Teams, and it is intended for use on a personal computer, laptop or mobile device (tablet/phone), government-owned USCG laptops/workstations, or mobile device (tablet/phone) with or without BlackBerry UEM. CVR Teams is authorized for use on the CGOne network or connected via VPN using the web-based version with the following web browsers; Microsoft Edge or Google Chrome. Use of CVR Teams for audio and video features, on a Coast Guard laptop/workstation, may require technical assistance to enable the camera and microphone features, as previously indicated in this document.

The tools listed in the table below are secure, authorized, and available on the Internet for use on and off of the CGOne network. All tools below require CAC authentication, except for CVR Teams.

Table 1

Collaborative Tools	USCG Issued Laptop/ Workstation	Personal Computer/ Laptop	Government Mobile Device	Personal Mobile Device	USCG to DoD	USCG to DHS Agencies	USCG to Any
Commercial Virtual Remote (CVR) Teams	Chat Voice Video Live Events	Chat Voice Video Live Events	Chat Voice Video Live Events	Chat Voice Video Live Events	Chat Voice Video Live Events	Chat Voice Video Live Events	Chat Voice Video Live Events
Defense Collaboration Service-Unclassified (DCS-U)	Chat Voice Video	Chat Voice Video Live Events			Chat Voice Video Live Events		
milSuite	File Sharing, Video, Post a Wiki, Survey	File Sharing, Video, Post a Wiki, Survey	File Sharing, Video, Post a Wiki, Survey	File Sharing, Video, Post a Wiki, Survey	File Sharing, Video, Post a Wiki, Survey		
Homeland Security Information Network (HSIN)	Chat Voice	Chat Voice Video				Chat Voice Video Large-File Sharing	
DoD SAFE	Large-File Sharing	Large-File Sharing	Large-File Sharing		Large-File Sharing		

Table 1 Functionality Definitions:

- **Chat:** Instant messaging similar to Skype for Business.
- **Voice:** Using application with Internet/Wifi or cellular connection to talk to other party(ies). Also includes web conferencing.
- **Video:** "Videoconferencing" allows users in different locations to hold face-to-face meetings without having to move to a single location together.
- **Live Events:** Broadcast video and meeting content to large online audiences.
- **File Sharing:** Sharing or offering access to digital information or resources, including documents, multimedia (audio/video), graphics, computer programs, images and e-books.
- **Large-File Sharing:** Same as "File Sharing" definition above; for larger files consisting up to an 8GB maximum.

Open the "DoD Telework Capabilities" document below for other DoD authorized capabilities.

DOD Telework Tools.pdf

Third-Party Applications

As of 1 May 2020, all external third-party applications (e.g. Zoom free version) are prohibited for use to conduct Coast Guard business except for telemedicine capabilities (IAW ALCOAST 096/20) or with an approved Special Use Information Technology (SUIT) request for "Zoom for Government" only. However, the Zoom for Government will be the only version authorized for use to conduct Coast Guard business (excludes USCG sensitive information; FOUO, Law Enforcement Sensitive, other Controlled Unclassified Information, all levels of classified information, and OPSEC.) As a reminder, it is **NOT** authorized for use while connected to the CGOne network. Furthermore, Zoom for Government is prohibited for use on a government issued laptop/CG workstation as well. See **Web/Videoconferencing Guidance** section for uses and restrictions.

CVR Teams and Defense Collaboration Service (DCS) are free, available and are a much more secure means to collaborate remotely than third-party applications. If the tools listed in *Table 1* do not meet your videoconferencing needs, then a Special Use Information Technology (SUIT) request is required for Zoom for Government. See the next section; **Special Use Information Technology (SUIT) Request** for further information.

Special Use Information Technology (SUIT) Request

IMPORTANT NOTE: In order to manage risk, NO other Zoom services (free version, Pro, Business etc.) or other third-party commercial solutions are authorized. The requestor will need to coordinate with their local command for registering and purchasing a monthly subscription of Zoom for Government. See the **Zoom for Government** section below for details. USCG Web/Videoconferencing Guidance is found on pages 6-8 of this document.

Please do not submit a CG-2180 form to ITQUESTIONS@uscg.mil. Instead, send an email to ITQUESTIONS@uscg.mil with the following information:

Subject Line: (Example :) Zoom for Government - (Unit Name)

Body of Message: Include the following;

- Business Case (CG mission, support, or business function justification)
- Operational Impact if Denied
- Number of licenses needed (a requesting command must purchase a minimum of 10 licenses for one year. See the **Zoom for Government** section below for details).

The COVID Capabilities Team will review the request, and contact the requestor. If the requestor wishes to continue with a SUIT Request, then the COVID Capabilities Team will provide direction for the SUIT Request process.

Zoom for Government

Zoom is a commercial subscription-based software on a cloud platform offering video and audio conferencing, collaboration, chat, and webinars across mobile devices, desktops, and telephones. "Zoom for Government" is approved under the U.S. Federal Risk and Authorization Management Program (FedRAMP), which provides a higher level of security compared to most of the other Zoom products.

IMPORTANT NOTE: Zoom for Government will be the only version authorized for use to conduct Coast Guard business (excludes USCG sensitive information; FOUO, Law Enforcement Sensitive, other Controlled Unclassified Information, all levels of classified information, and OPSEC.)

*** **CVR Teams and DCS are FREE and a viable and are a much more SECURE means to collaborate remotely than Zoom for Government** ***

The Zoom for Government subscription consists of the following:

- A command must purchase a minimum of 10 licenses with an annual subscription.
- Subscriptions are for a minimum of 1 year. No monthly subscriptions are available.
- Subscription costs are estimated at $280 per license; (10 x $280 = $2,800 at the minimum, for 1 year, per command).
- A minimum of 10 licenses are for intended for "Hosts" (Users). 1 of these will be the "Owner" and can be considered the "Admin" for the command's subscription. The Admin selects the "Users" (hosts) and those "Users" can create and host video and audio conferencing, collaboration, chat, and webinars. When the "User" creates one of these events, they can share the event up to a maximum of 350 invitees. The invitees will receive an email with a link to the event. Invitees are covered within the subscription costs, so no extra costs are associated with invitees. Invitees will have unlimited local Toll & VOIP for all meetings.

NOTE: Requestors submitting a SUIT Request for Zoom for Government are required to read and abide by the Web/Videoconferencing Guidance provided in the **Web/Videoconferencing Guidance** below.

Zoom for Government users seeking technical support must contact the vendor directly. The Coast Guard Centralized Service Desk (CSD) does not provide technical assistance for Zoom.

Web/Videoconferencing Guidance

This Web/Videoconferencing Guide will help you create a workflow using technology more efficiently for yourself as well as for the Coast Guard as a whole. Please refer to the most recent ALCOAST regarding teleworking options, categories, and information at https://www.uscg.mil/Coronavirus/

WEB/VIDEOCONFERENCING EXCEPTIONS: If the DoD-approved web/videoconferencing and collaboration solutions do not provide the necessary capabilities to a unit commander, then third-party applications (apps), such as Zoom for Government can be installed ONLY on personal computer/laptop or mobile device (tablet/phone), or government furnished mobile device (tablet/phone) with and without BlackBerry UEM and are limited to "off network" use.

Third-party teleconferencing, videoconferencing, and collaboration apps are NOT authorized on CG Government Furnished Equipment (GFE) Standard Workstation Laptops. Zoom for Government offers the capability for collaborating remotely while also not using and preserving Coast Guard's CGOne bandwidth. However, Zoom for Government should be used as a last resort. See the "Helpful Links" at the end of this document for further details.
CGCYBER will continue to evaluate risks and put out information to advise users, while working with CG-6 to provide more secure collaboration alternatives that will allow us to migrate away from unsafe applications and ensure the protection of CG information and data.

Uses for Zoom for Government

Zoom for Government is a commercial video/web conferencing application that can be utilized to discuss publicly releasable information, and to assist communications within the USCG community during the COVID-19 pandemic. There are several instances that Zoom for Government would be appropriate for use during this crisis:

- ✓ Conducting briefs on COVID-related activities or assistance where the information is unclassified and not Controlled Unclassified Information
- ✓ Conducting contingency communications between commands and personnel
- ✓ Communicating with personnel that is not specifically mission-focused
- ✓ As noted in ALCOAST 096/20, telehealth use is authorized

Mobile Devices

Zoom for Government may ONLY be downloaded on personal computer/laptop or mobile device (tablet/phone), or government furnished mobile device (tablet/phone) with and without BlackBerry UEM.

IMPORTANT NOTES:
The Centralized Support Desk (CSD) (CGFIXIT) does not provide support for Zoom for Government or CVR Teams. Contact the service providers directly for support.

Keep Privacy, Operational (OPSEC), and Cybersecurity in mind at all times!

CONDITIONS OF USE:

1. If Zoom for Government is procured using USCG funds, the Opt-Out Requirement must be checked (Mandatory for USCG-funded accounts).
2. Users are required to opt out of the "sale" of personal data to prevent Zoom for Government from sharing PII with third-parties (namely advertising programs such as Google Ads and Google Analytics). Opting out is accomplished by clicking on the "Do Not 'Sell' My Personal Information" link or restricting cookie collection.

*******If Zoom for Government does not allow users to opt out of using personal data then its use is <u>prohibited</u>.*******

PROHIBITED USE:

- Use of screen shots, capturing video or audio, or recording any audio or video content (including the functions within Zoom for Government during use is strictly prohibited.
- Users of Zoom for Government are not authorized, and are strictly prohibited, from displaying or discussing the following:
- Conversations discussing or sharing USCG sensitive information (FOUO, Law Enforcement Sensitive, other Controlled Unclassified Information, and all levels of classified information);
- Operational Security (OPSEC);
- Personally Identifiable Information (PII), Sensitive PII, and Protected Health Information (PHI);
- Health Insurance Portability and Accountability Act (HIPAA) related disclosures, except as allowed by ALCOAST 096/20 https://content.govdelivery.com/accounts/USDHSCG/bulletins/2825e73

Funding

Funding of Zoom for Government is at the discretion, and is the responsibility, of the requesting Command. Zoom for Government is not an approved enterprise application, so a Special Use Information Technology (SUIT) request must be submitted for tracking purposes.

Helpful Links:

Please check https://www.dcms.uscg.mil/Telework/ for the most updated list of programs and processes to obtain authorization for use.

IMPORTANT NOTE: Examples of prohibited commercial third-party applications on CGOne network for Coast Guard official business include Google Hangouts, Zoom, WhatsApp, Skype, and FaceTime Messenger. This is NOT an all-inclusive list. This excludes the approved Zoom for the medical community outlined in ALCOAST 096-20. Refer to https://www.dcms.uscg.mil/Telework/ for the most updated list.

1. Working from Home – includes links for VDI and VPN
2. Telework Program – includes Commandant Instruction for Telework
3. CG-6 Public Telework web page
4. USCG COVID page –FAQs for telework
5. FBI Warning on third-party apps page - risks & information using third-Party apps

Reference: U.S. Coast Guard Cybersecurity Manual, COMDTINST M5500.13F

End of Document