DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

APR 13 2020

MEMORANDUM FOR CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF DEFENSE
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
CHIEF OF THE NATIONAL GUARD BUREAU
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF OPERATIONAL TEST AND EVALUATION
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE FOR LEGISLATIVE AFFAIRS
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS
DIRECTOR OF NET ASSESSMENT
UNITED STATES CYBER COMMAND
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF DOD FIELD ACTIVITIES

SUBJECT: Authorized Telework Capabilities and Guidance

References: (a) "Temporary Authorization to Use Impact Level (IL) 2 Cloud Environment for Certain Basic Controlled Unclassified Information (CUI)," March 26, 2020
(b) "Treatment of PII within IL 2 Commercial Cloud,) August 7, 2019
(c) DoD Chief Information Officer memorandum, "COVID-19 Response: Remote Work Capability," March 19, 2020
(d) DoD Chief Information Officer memorandum, "Authorizations to Operate Extensions and Cybersecurity Function Prioritization Guidance," April 3, 2020

Department of Defense Chief Information Officer (DoD CIO) has engaged in a number of initiatives to enhance the telework capabilities of the Department. We continue to field questions from components and have identified a number of areas where clarification is needed.

In support of expanded telework requirements, DoD Components should first look to leverage approved DoD Enterprise Collaboration Capabilities, which are already approved for use by all DoD users. If these capabilities do not meet the Component needs, components are authorized to approve use of commercial cloud services which have been issued a DoD Provisional Authorization. Components must continue to abide by all DoD policies regarding telework capabilities and the use of cloud services, reinforce Operations Security (OPSEC) and

ensure compliance with the level of sensitivity of data approved for these services. If neither of these options are sufficient, Components must submit requirements for approval by DoD CIO and USCYBERCOM. These requirements should be submitted to Joint Forces Headquarters - Department of Defense Information Network (JFHQ-DODIN) at https://intelshare.intelink.gov/sites/jfhq-dodin. The current list of enterprise and provisionally authorized capabilities is provided in Appendix A, and an updated list will be maintained at https://cyber.mil/covid19. Also posted on the site are additional guidelines for initiating teleconferences.

In support of dramatically expanded telework requirements, DoD CIO has approved the use of a Commercial Virtual Remote (CVR) environment as a temporary capability that will be available to supplement existing collaboration tools and enhance remote telework capabilities during the National Emergency. This capability is authorized for use by all DoD users. The CVR Environment is a DoD-contracted Microsoft Office 365 (O365) Teams capability, implemented with DoD specific security controls, which provides video, voice, and text communication, as well as document sharing tools for Basic Controlled Unclassified Information (CUI) as outlined in Reference (a). CVR is accessible from the Internet or DoD networks via both Government Furnished Equipment and personal devices. DoD Components will be incrementally on-boarded by Components in accordance with the prioritization established by the COVID-19 task force. Additional CVR information is available at https://www.cloud.mil/CVR. For all other CVR questions, please contact the DoD CIO team at OSD.COVID19.RemoteWorkTeam@mail.mil.

DoD is aware that several components have expressed pursing unauthorized cloud and collaboration capabilities. These capabilities place DoD information at risk and are not authorized to conduct internal DoD business. Components should not initiate communications using unapproved commercial collaboration capabilities, but may participate in sessions if initiated by outside partners for public, unclassified purposes. The use of cloud services must be formally authorized by a component Authorizing Official (AO) and comply with requirements in the DoD Cloud Computing Security Requirements Guide, found at https://dl.cyber.mil/cloud/pdf/Cloud_Computing_SRG_v1r3.pdf.

Components should not engage in unilateral agreements or accept offers of free solutions from vendors without appropriate consultation and appropriate contracting actions. Engagements with vendors in this context should be coordinated through the DoD CIO team at OSD.COVID19.RemoteWorkTeam@mail.mil. We continue to assess additional telework capabilities that may supplement the existing suite on a temporary basis during the current crisis based on mission need.

Telework has provided the Department with the flexibility to continue operations. However, telework may present significant risks to the Department. To minimize this risk we are providing teleworking guidance to components (Appendix B) and individuals (Appendix C). CIO will continue to update this guidance as needed.

All are reminded that adherence to all standing cyberspace policies and guidance is as important while teleworking as it is while working on-site. Questions for any aspects of this memo should be directed to OSD.COVID19.RemoteWorkTeam@mail.mil.

Dana Deasy

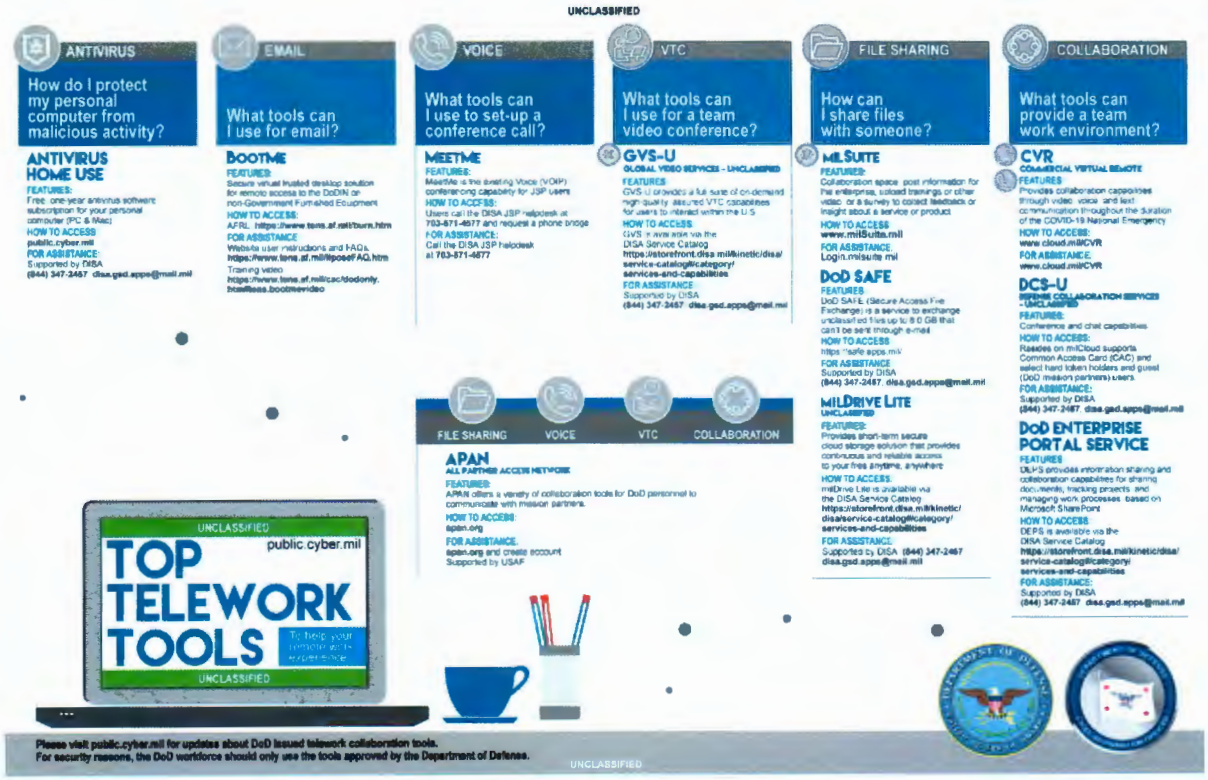
Attachments: As stated

Appendix A

Authorized Enterprise Telework Capabilities

Primary Telework Capabilities

Primary telework capabilities are authorized at the enterprise level and are available for use by all DoD personnel without additional authorizations. In addition, any existing telework capability which has a valid ATO from, and is hosted by a DoD Component remains approved. Components must inform JFHQ-DODIN of these capabilities to ensure a comprehensive understanding of the DoD telework environment is maintained.



Alternative Capabilities

Alternate capabilities are capabilities that have received a DoD Provisional Authorization (PATO). However, these capabilities must still be authorized by the component and meet all applicable DoD cybersecurity policies and standards. Finally, Alternative Capabilities may only process data types consistent with the data impact level of their PATO.

Services with a Provisional Authorization for Sensitive (but non-classified) DoD data

Cloud Service Provider	Title	Data Impact Level	Voice	Video	Chat	File Sharing
BOX	Box Enterprise Cloud Content Collaboration Platform	IL4 with restrictions				X
Cisco Systems, Inc.	Cisco Hosted Collaboration Solution (HCS-D) IL5	IL5	X	X	X	
Microsoft	Microsoft Office 365 vNext IL5	IL5	X	X	X	X

Services with a Provisional Authorization for Public (non-FOUO) DoD data

Cloud Service Provider	Title	Data Impact Level	Voice	Video	Chat	File Sharing
Adobe	Adobe Connect	IL2	X	X	X	
Avaya	Avaya	IL2	X	X	X	
Cisco	Cisco WebEx	IL2	X	X	X	
Cisco	Cisco WebEx Collaboration for US Government	IL2	X	X	X	
Collab9	Collab9: Cloud Unified Communications, Contact Center and Collaboration	IL2	X	X	X	
CoSo Cloud	CoSo Cloud	IL2	X	X	X	X
Google	Google G-Suite:	IL2	X	X	X	X
Huddle	Huddle: Huddle Enterprise Cloud Content Collaboration and File Sharing Portal for Government	IL2				X

Microsoft	Microsoft: Dynamics 365 for Government	IL2	X	X	X	X
Zoom	Zoom for Government	IL2	X	X	X	

Contingency Capabilities

If your mission requires a capability which cannot be met by the current approved enterprise offerings, or by issuing a component ATO for one of the alternate capabilities, contingency capability requirements must be submitted for approval by DoD CIO and USCYBERCOM. These requirements should be submitted to JFHQ-DODIN at https://intelshare.intelink.gov/sites/jfhq-dodin.

Appendix B

Telework Best Practices for Organizations

DUTIES AND RESPONSIBILITIES.

1) The organization will provide the overall direction for the individual telework program and ensure employee teleworking activities are consistent with records management policy and mission requirements
2) Organizations must enable security measures with the assumption the public network between the teleworking individual and the organization cannot be trusted
3) Organizations will review operational processes to maintain telework and remote access security
4) Organizations will review usage restrictions, configuration requirements, connection requirements
5) Administrative rights will not be granted to users on Government Furnished Equipment (GFE) or equipment furnished to employees of a contracted company
6) The organization will monitor and log all GFE device activity of individuals engaged in telework
7) Multi-factor authentication will be required when accessing a GFE or contractor furnished device
8) Hosts and devices must use random number values and public/private key pairs for all cryptographic functions
9) The organization will provide telework training and ensure any individual engaged in telework has completed the training
10) The organization will have a plan for allowing teleworkers to be able to successfully and securely telework, and to recover records into the Component's record keeping environment
11) The organization will develop system threat models for any resource that is accessed remotely
12) Organizations must assume that there is a potential for a device being used for teleworking to fall into the hands of malicious actors

Appendix C

Telework Best Practices for Users

GUIDANCE. Achieving a secure teleworking environment can be best accomplished by adhering to the following guidelines:

1) Technical Tasks To Complete
    a. Ensure patches and updates to hardware, software, and operating systems are applied as soon as they are available.
    b. Change the default password on home Wi-Fi networks and enable encryption
    c. Reboot the machine prior to establishing a new VPN session
    d. Disable the VPN connection upon completion of daily activities
    e. Enable security software such as anti-virus, anti-phishing, and anti-malware
    f. Disable webcams and microphones on laptops/desktops when not in use
    g. Ensure multi-factor authorization is enabled on GFE's and contractor devices
    h. Ensure that your personally owned routing device supports basic firewall capabilities
    i. Implement Wi-Fi Protected Access 2 (WPA2) with a strong passphrase of 20 or more characters, including numbers and special characters
    j. Change the SSID to something unique, but do not hide the SSID as this can cause compatibility issues and offers no additional security
    k. Disable the ability to perform remote administration on the routing device

2) Allowable Actions for Government Furnished Equipment
    a. You may connect peripherals such as a personal keyboard or mouse (not printers) to Government Furnished Equipment (GFE). External monitors may be connected if using a VGA, HDMI, or DisplayPort connection (USB connections are not allowed)
    b. You may connect to a home network that you are in complete control of
        i. You should not connect to a network that you do not own and control

3) Unallowable Actions
    a. Do not send unencrypted PHI or PII, or auto-forward or forward PHI or PII to a personal email account or store on a personally owned computer
    b. Do not use GFE or contractor supplied equipment to browse social media or streaming services for personal audio or video communication
    c. Do not use GFE or contractor supplied equipment for any other non-essential activity
    d. Do not take classified material to a personal place of residence
    e. Do not leave your GFE or contractor supplied device unattended while logged in

f. Do not allow video conferencing applications to continue running while not in use
g. Do not use personal email accounts for official business or forward email from an official email account to a personal account
h. Do not use personal hard drives, USB/thumb drives, external hard drives, or commercial cloud/file sharing services for official business

4) Best Practices
   a. Use approved file-sharing applications to share files with one another
   b. Work offline when possible in order to free up bandwidth
   c. Do not install unknown or unnecessary browser extensions
   d. Ensure passwords and challenge responses are properly protected
   e. On personal devices, do not use administrator accounts for daily activities such as web browsing, email access, and file creating/editing
   f. Do not open emails from senders you do not recognize, and never click on an attachment or a link in an email from an unrecognizable source
   g. Avoid using the out-of-office message unless necessary
   h. Avoid posting information such as address, phone number, place of employment, and other personal information that can be used to target or harass you

5) User Responsibilities
   a. Users will be held accountable for the security of government hardware, software and information
   b. Users will guard against phishing and social engineering attempts including shoulder surfing
   c. Users will be able to recognize unusual activity on their device and know how to respond
   d. Users will read and be familiar with all applicable acceptable use policies provided by the organization