171st ARW Teleworking Guide

Revision 1.3: 3 September 2020

1. **Message from Communications Flight Commander:** This document is our attempt to corral the volumes of loose Comm related material into one usable reference. The information listed in this condensed document is supported by installation guides, how-to's and troubleshooting steps that are currently published on the CFP SharePoint page. We will do our best to keep this document current and relevant as new information comes to light. We welcome your feedback and insights as to how we can better present the information you will need to do your job.
- Lt Daniel Fairbanks
2. **Communications Flight Contact Information**
    a. **Hours of Operation:** We will continue to follow the normal Compressed Work Schedule hours of operation 0630-1630 Mon-Fri or Tue-Fri as appropriate with the exception of 0630-1530 on early Friday.
    b. **The BEST WAY TO REACH US:** Please email the CFP Org Box at 171.ARW.CS.Helpdesk-CFP.Org@us.af.mil as this is monitored by multiple personnel and will give us a record of your request in the event we are unable to take your call.
    c. If you are trying to get **immediate assistance** you may still contact the CFP at 412-776-7333.
3. **Equipment Sign-out:** Any ANG assets that will be taken off base need to be properly accounted for between you and your equipment custodian. That information can be documented on an AF Form 1297 or kept on a sign out log. Some examples of equipment that you may need in order to support teleworking is a laptop, a CAC reader (or keyboard with CAC), and even a monitor if necessary. The most important thing to remember is that no equipment will leave base unaccounted for. All of the equipment must be signed out of Comm by your respective equipment custodian.
4. **The PAPERWORK**
    a. **To TELEWORK**:
        i. We require an email from your commander authorizing your VPN request
        ii. You will need to take the Employee (or Manager, as appropriate) **Telework Fundamentals Training** and provide the **Final CERT** to your manager.
            1. Employee - https://www.telework.gov/training-resources/telework-training/virtual-telework-fundamentals-training-courses/employee-course/index.htm
            2. Manager - https://www.telework.gov/training-resources/telework-training/virtual-telework-fundamentals-training-courses/managers-course/index.htm
        iii. You are required to fill out and submit the **DD2946 - Telework Agreement** to your manager.
    b. **Equipment Sign-out**: AF Form 1297 or sign-out sheet, whatever your equipment custodian requires.
5. **How To Access Base Voicemail from Off Base**
    a. Dial 412-776-8011
    b. Enter your base phone 7 digit extension number and #
    c. Enter your PIN and #

6. **Virtual Private Network (VPN) Access:** There are three different methods that offer various levels of access to AF, ANG, and Base resources. The one you use will depend on the equipment you are using (laptop, home computer) and which VPN you are able to utilize.
   VPN Training: You can access VPN training for mobile devices at https://cyber.mil/cyber-training/training-catalog/
   a. **Base Laptop:** Each base laptop has the Cisco AnyConnect client and the USAF VPN Client loaded.
      i. **Cisco AnyConnect** is utilized by the ANG and will give you access to the base network, Outlook, base share drives, etc., as if you were in the office. This VPN is not available until Comm completes the required pre-configuration and account establishment. Also, as previously stated in the PAPERWORK section, you will need commander's approval to use this VPN.
         1. **In the Cortana Search** (bottom Left of screen): Type AnyConnect and run the Cisco AnyConnect App. All pre-approved personnel are authorized to use:
            a. VPN 1, 2 or 3.
            b. One of the five Joint Regional Security Stack (JRSS). These options are installed with the newest version of Cisco AnyConnect (4.8.03036). JRSS options vastly increase the number of concurrent users.
      ii. **AF VPN** is the Air Force remote access service and can be used by ANG personnel. You can use it to conduct all normal business.
         1. The AF VPN client is pre-loaded on base machines. The ICON is on your desktop.
   b. **Home PC/Laptop:** NOTE: You will require a CAC reader to be installed on your home machine.
      i. **Desktop Anywhere** is available to use on your home machine. It requires you to follow the Desktop Anywhere Win10 or MAC Installation Guide which is available on the CFP SharePoint page.
      ii. **AF Portal** is also a great way to access many of the tools you use every day when you set up the hotlink. From the Portal you can access OWA email by hovering over the pull down arrow, top right next to your profile, and select email. To access your CHES email from commercial internet use the OWA external link: https://owa.us.af.mil/owa. To access OneDrive from a commercial internet/PC use: https://usaf-my.dps.mil/ .
7. **Team Collaboration Tools**
   a. **Conference Bridges:** There are two Conference Bridges available for you to reserve. To check availability, or to reserve a time, please go to the Wing SharePoint page and scroll to the bottom where you will see a calendar. Find the date you are looking for and click in the bottom right hand side. There you will see an add button, click that to add your information. Please make sure you enter a start time, end time, and in the description block, POC information for the conference. If you do not have edit privileges, your commander likely does, or contact Comm and we will either edit your privileges or make the reservation for you.

i. **Base Bridge** is hosted on base, has only enough ports for 16 callers, and can be called local, DSN or Commercial. It is intended to be used primarily by callers from on base extensions as too many off base callers can seriously degrade call capacity into/out of the base.
    1. From On Base Dial 776-8080
        a. At the prompt enter 001## (disregard PIN prompts)
        b. You will be joined to the conference
    2. From Off Base Dial 412-776-8080 (or DSN 294-8080)
        a. At the prompt enter 001## (disregard PIN prompts)
        b. You will be joined to the conference

ii. **DISA Bridges** are hosted by DISA, we have 3 bridges, and each has enough ports for up to 40 callers, and can be called DSN or Commercial.
    1. Bridge 1: From On or Off base Dial 301-909-7350 (DSN 723-7350):
        a. At the prompt enter: 247311300#
        b. One person has to be the chairperson – please contact Comm for the Chairperson PIN.
    2. Bridge 2: From On or Off base Dial 301-909-7357 (DSN 434-7357):
        a. At the prompt enter: 24734983#
        b. One person has to be the chairperson – please contact Comm for the Chairperson PIN.
    3. Bridge 3: From On or Off base Dial 301-909-7357 (DSN 434-7357):
        a. At the prompt enter: 247311301#
        b. One person has to be the chairperson – please contact Comm for the Chairperson PIN.

b. **Skype** is a chat-based tool for keeping in contact with personnel from base. The status option lets you tell other members when you are Available, Busy, Away, etc. This tool on a base laptop allows Comm to see what you see and better assist you with issues you may be having at home.

c. **TEAMS (CVR/CHES)** Microsoft Teams is also a chat-based workspace application meant to facilitate ongoing collaboration and communication occurring among any team, project, organization or group of people. Teams provides single-point access to conversations, files and more. Teams also has audio and/or video calls if your machine is properly equipped.

8. **Guides and Troubleshooting Info:** Take note of the attached GFE Do's and Don'ts. Please follow the link to the CFP SharePoint page where you will find all of the installation guides, how-to's, and troubleshooting steps for known VPN issues. We will continue to update this location as new information becomes available:
https://org2.eis.af.mil/sites/34158/MSG/CF/CFP/_layouts/15/start.aspx#/

    a. **CVR Teams Self-Help Portal:** All CVR accounts and users are able to reactivate disabled accounts until 15 Dec 2020. Through the self-help portal, you will be able to initiate a new password reset, reset authentication for a new device, and unlock your account.
    CVR Self-Help Portal: https://disa.deps.mil/ext/cop/gsd/cvr/index.html#/

GOVERNMENT LAPTOP (GFE) DO'S & DON'TS

Basic guidelines all users have signed and must follow:

- I understand that I will not connect this device to other computing equipment, including personal laptops (e.g., tethering or wireless personal area network [WPAN], air card use, and device synchronization [hot-synch]) without prior Designated Accrediting Authority (DAA) approval.
- I will also observe device-specific stipulations prior to any connections. I will not exceed my authorized user access and enable unauthorized functionality of this device.
- I will follow any local Wireless Remote Access connection policies and approval procedures prior to use.
- I will not configure wireless devices to download, install, or use unauthorized applications, software updates, or personal e-mail accounts (e.g., AOL, Yahoo, Gmail, etc.) unless authorized by the DAA.
- I acknowledge that only authorized wireless peripherals and Bluetooth devices (including CAC readers, and headsets/hands free devices) will be used/synchronized to this wireless device and I must contact the Service Desk and/or my organizational IAO for a list of approved devices.
- I understand locally created operating instructions on use of wireless devices may accompany this user agreement.

DO'S

☐ Personnel with GFE's can receive updates via VPN. All users with GFE's should either have access to Cisco AnyConnect or USAF VPN Client. **Do log in once a week for a while to allow your computer to grab updates and check in with the network.**

☐ **Do practice good OPSEC.** When connected to your at-home WiFi please keep in mind what you are accessing and surfing. You will not have Air Force Filters to restrict you, please act like you still do.

☐ **Do be responsible for protecting GFE and information from theft, damage, and improper use.**

☐ DoDI 1035.01 highly recommends use of a firewall with personal PCs, **please use the McAfee Home Use Program.** Extraction of information to removable media, via email or to personal printers should not be allowed.

DON'TS

- ☐ Don't introduce personally owned software or connect personally owned media or peripheral devices with volatile or non-volatile memory. This means please **do not connect any USB devices to the laptop that was not issued by the base or install any software.**
- ☐ **Don't connect wireless accessories** such as Bluetooth devices.
- ☐ **Don't charge phones off the laptops.**
- ☐ **Don't take classified documents (hard copy or electronic) home or to alternative worksites.** If classified telework is authorized at an approved alternative secure location, teleworkers shall comply with the procedures established by the DoD Component regarding such work.
- ☐ **Don't use of personal e-mail accounts for PII transmission**. PII may only be e-mailed between Government email accounts and must be encrypted and digitally signed.
- ☐ GFE shall be used for official use and authorized purposes only. **Family members and friends are not authorized to use GFE's and materials.**

Changes

Change 1 – 29 April 20

ii. **DISA Bridge** is hosted by DISA, has enough ports for up to 40 callers, and can be called DSN or Commercial.

1. From On or Off base Dial 301-909-7350 (DSN 723-7350):
    a. At the prompt enter: 24734983#

2. **Virtual Private Network (VPN) Access:** There are three different methods that offer various levels of access to AF, ANG, and Base resources. The one you use will depend on the equipment you are using (laptop, home computer) and which VPN you are able to utilize.

b. **Base Laptop:** Each base laptop has the Cisco AnyConnect client and the USAF VPN Client loaded.

i. **Cisco AnyConnect** is utilized by the ANG and will give you access to the base network, Outlook, base share drives, etc., as if you were in the office. This VPN is not available until Comm completes the required pre-configuration and account establishment. Also, as previously stated in the PAPERWORK section, you will need commander's approval to use this VPN.

1. **In the Cortana Search** (bottom Left of screen): Type AnyConnect and run the Cisco AnyConnect App. All pre-approved personnel are authorized to use:
    a. VPN 1, 2 or 3.
    b. One of the five Joint Regional Security Stack (JRSS). These options are installed with the newest version of Cisco AnyConnect (4.8.03036). JRSS options vastly increase the number of concurrent users.

ii. **AF VPN** is the Air Force remote access service and can be used by ANG personnel. You can use it to conduct all normal business.

Change 2 – 25 August 20

b. **Home PC/Laptop:** NOTE: You will require a CAC reader to be installed on your home machine.

i. **Desktop Anywhere** is available to use on your home machine. It requires you to follow the Desktop Anywhere Win10 or MAC Installation Guide which is available on the CFP SharePoint page.

ii. **AF Portal** is also a great way to access many of the tools you use every day when you set up the hotlink. From the Portal you can access OWA email by hovering over the pull down arrow, top right next to your profile, and select email. To access your CHES email from commercial internet use the OWA external link: https://owa.us.af.mil/owa. To access OneDrive from a commercial internet/PC use: https://usaf-my.dps.mil/ .

Change 3 – 3 September 20

7. **Virtual Private Network (VPN) Access:** There are three different methods that offer various levels of access to AF, ANG, and Base resources. The one you use will depend on the equipment you are using (laptop, home computer) and which VPN you are able to utilize.
VPN Training: You can access VPN training for mobile devices at https://cyber.mil/cyber-training/training-catalog/ located on the right hand side of the page.

ii. **DISA Bridge** is hosted by DISA, we have 3 bridges, and each has enough ports for up to 40 callers, and can be called DSN or Commercial.
    1. Bridge 1: From On or Off base Dial 301-909-7350 (DSN 723-7350):
        a. At the prompt enter: 247311300#
        b. One person has to be the chairperson – please contact Comm for the Chairperson PIN.
    2. Bridge 2: From On or Off base Dial 301-909-7357 (DSN 434-7357):
        a. At the prompt enter: 24734983#
        b. One person has to be the chairperson – please contact Comm for the Chairperson PIN.
    3. Bridge 3: From On or Off base Dial 301-909-7357 (DSN 434-7357):
        a. At the prompt enter: 247311301#
        b. One person has to be the chairperson – please contact Comm for the Chairperson PIN.

b. Skype is a chat-based tool for keeping in contact with personnel from base. The status option lets you tell other members when you are Available, Busy, Away, etc. This tool on a base laptop allows Comm to see what you see and better assist you with issues you may be having at home.

c. TEAMS (CVR/CHES) Microsoft Teams is also a chat-based workspace application meant to facilitate ongoing collaboration and communication occurring among any team, project, organization or group of people. Teams provides single-point access to conversations, files and more. Teams also has audio and/or video calls if your machine is properly equipped.

a. **CVR Teams Self-Help Portal:** All CVR accounts and users are able to reactivate disabled accounts until 15 Dec 2020. Through the self-help portal, you will be able to initiate a new password reset, reset authentication for a new device, and unlock your account. We recommend using Edge and your authentication certificate to access the portal.
CVR Self-Help Portal: https://disa.deps.mil/ext/cop/gsd/cvr/index.html#/