



 USAG Ansbach

Smart Telework Practices

18 March 2020

Purpose

- To provide USAG Ansbach staff a reminder on Information Security (INFOSEC) responsibilities when using DoD information systems as they Telework and Contribute to both their Organization efforts, and the continuing mission of the Department of Defense
- DoD Telework Policy Guidance – See: <https://www.dcpas.osd.mil/OD/Telework>

Why Telework

- The Telework expectation...
 - Telework is an effective strategy for mission accomplishment, ensuring continuity of operations in a crisis, facilitating your organization's ability to recruit and retain valued talent.

A new “Normal”

- As the ramifications, impacts and reality of the COVID-19 virus takes effect, many USAG Ansbach staff members may find themselves forced to practice social distancing while continuing to contribute through Telework.
- If you have that capability, as the Garrison Security Manager, I wanted to take a few moments to offer as a reminder the INFOSEC responsibilities you have while using your issued DoD tools (Laptops with remote VPN capability, or Organization i-Phones), and your OWA E-mail -- if your home computer is connected with a plug-in CAC reader.

Remember OPSEC Always

- -- **OPSEC Rules of the Road** --
 - Do not disseminate any information that reveals: vulnerabilities, shortfalls, ongoing operations, budgets, personal actions or morale.
 - Ask yourself, "Could this information be used against us?" before hitting Send.
 - Don't send Controlled Unclassified Information (CUI), Personally Identifiable Information (PII) or For Official Use Only (FOUO) emails or documents unencrypted, and limit distribution.
 - NEVER process or discuss Classified operations on NIPRNET.
 - Don't discuss government business in the presence of visitors and those who don't have a need to know.
 - Avoid sending or discussing critical or sensitive information without encryption or secure communications.
 - Don't try and talk around critical or sensitive information.
 - Don't download CUI / PII to personal networks.
 - Brief family members on basic OPSEC responsibilities.
 - Secure and destroy CUI, memos, notes or documents when not needed.
 - Log off and remove CAC card when not working.
 - Report OPSEC violations to a supervisor and the group's identified OPSEC Officer.

Turn on your e-mail Encryption

- No e-mails sent during Telework (or remotely via Outlook Web Access (OWA)) should be sent unencrypted.
- Turn on your automatic e-mail Encryption, or reach out to your S-6 representative for assistance in making this happen.

iPhone Usage and online Apps

- A number of online Apps feature bots which work in the background pulling user information in an effort to enhance the Apps efficiency.
- Unfortunately, these Apps can easily be re-tooled to monitor (and report back) the processes of other applications running on the phone, as well as the actions and activities of the user.
- Follow your S-6 representatives guidance. If they tell you that an application you find online is safe, then it is safe to upload -- otherwise Resist the Temptation...

Something New, DoD-SAFE

- DoD Safe is designed for transferring information from point "A" to point "B" in a secure manner using a Secure DoD Server.
- What does this mean? Well, if you are working or collaborating at home with Sensitive information --(Never Classified), but more on par with Controlled Unclassified Information (CUI) or For Official Use Only (FOUO) data-- and need to securely share this work-product with your colleagues, you can either use your Encrypted e-mail, or 'DoD Safe' as your means of bridging the points together.
- The benefit of DoD Safe is that, should the need arise, you can transmit up to 8GB of data securely, and doing so will not overwhelm and capsize the e-mail boxes of your team.

Something New, DoD-SAFE

How to send
personally identifiable
information
(PII)



OPTION
1



ENCRYPT
and you're good to go!

OPTION
2



DoD SAFE!
it's convenient
and everyone has access!

<https://safe.apps.mil/>

OPTION
3



OR...
BE BLOCKED!
make sure your message
gets there...
It's all about PII Security!

Using Telework Time Wisely

- While telework normally implies a contribution to mission, it also means time that you can avail yourself to online training.
- Both AKO and JKO offer a number of online training venues which meet AR 350-1 requirements, and
- Civilian Education System (CES) offers workforce development training. The CES courses are targeted at grade level. GS-01 through GS-09 employees are eligible to attend the CES Basic Course; GS-11 through GS-12 employees are eligible to attend the CES Intermediate Course; and GS-13 through GS-15 employees are eligible to attend the CES Advance Course. Other courses available for consideration include: The Supervisory Development Course (SDC); Managers Development Course (MDC); and the Action Officer's Development Course (AODC). To access this training, log on to CHRTAS (<https://www.atrrs.army.mil/channels/chrtas/student>) and look for the CES Hot Links.
- National Incident Management System (NIMS) online training -- this training is largely designated for Emergency Operation Center (EOC) and Crisis Management Action Team (CMAT) personnel; Provost Marshal's Directorate of Emergency Services (DES); First Responders, and Emergency Essential Personnel
- The Center For Development of Security Excellence (CDSE) training Platform is also available

Reminders from S6

- It is against regulation to forward gov't phone numbers to a personal phone.
- It is against regulation to discuss gov't information on personal phones.
- You can use personal earbuds or headsets, but they must be the 3.5mm audio jack version -- but Do NOT use wireless or Bluetooth speakers / headphones / earbuds
- We are NOT supposed to use USB headphones/earbuds - It is considered a policy violation if you connect an unauthorized device to your gov't systems.
- If you do have computer related issues, first contact ' 119 ' – the commercial number for ESD is: **0611-143-523-1000**. If the problem cannot be fixed remotely, depending on staff availability, you may need to come in and get it fixed.

Reminders from S6...cont'd

- Finally -- McAfee has announced a "Work from Home (WFH)" program that provides free access to their Total Protection solution for 60-days. Under McAfee WFH, anyone can download their premier anti-virus and secure virtual private networking solutions to better protect their systems in response to the heightened mission need to support telework requirements.

<https://www.mcafee.com/consumer/en-us/landing-page/direct/aff/wfh-60dayfree>

Comms Systems Continuity

- **VPN**
- DSN Phones;
- Unclassified / Secure VOIP;
- JABBER Video
- **Issued iPhones**
- Internet (Unclassified / Secure)
- **OWA – CAC Readers: Issued; On Hand, or Available?**
- **Issued Laptops**
- Tandberg (IP)
- Projectors
- CII – KSV-21 Cards