Working Remotely - The Basics

- The use of Government Furnished Equipment is ALWAYS the preferred method for connecting to DoD Resources.
- Adhere to your organization-specific Telework User Guidance.
- Use your organization's official connection services while conducting official business (e.g., VPN, MobiKEY, Vmware View, Desktop Anyware, etc.)
- While connected to the NIPRNet, use of streaming video/audio and internet access is not authorized except for official business.
- Users are responsible for following existing Acceptable Use Policies.

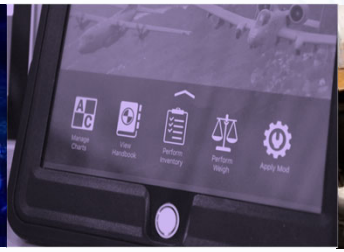
Cybersecurity Fundamentals

- Don't use open/untrusted Wi-Fi.
- Users are responsible for the security of government information and equipment in any environment.
- Be aware of possible Phishing attempts. https://dl.dod.cyber.mil/wp-content/uploads/trn/products/brochures/unclass-phishing_brochure.pdf
- Don't forward content from your official email account to a personal email account.
- Ensure personal devices/systems have updated anti-virus software in use.
- Understand the difference between FOUO/CUI/UNCLASSIFIED information.
- Always encrypt PII/PHI/CUI data.
- For any questions/concerns about sensitive information, please contact your local security representative.

Telework Using Government Furnished Equipment (GFE)

- GFE is for official government use only.
- GFE to be used only by authorized users. Remind family members the computer is for your work only and not to be used for other purposes (Utilize good practices such as locking and removing your CAC)
- Teleworkers are responsible for the physical security of their GFE.
- No use of streaming video/audio and internet access except for official business.






Version 12/162150MAR20

Personal Device Access to DoD Resources (Outlook Web Access, milDrive, milSuite, etc.)

- Use DoD provided bootable media for access if available. (e.g., Trusted End Node Security (TENS).
- If unavailable, follow instructions on https://public.cyber.mil/pki-pke/end-users/getting-started/ to properly configure your device to support the use of a DOD PKI certificate. Use of a compatible CAC reader is required for access.
- Don't use personal email accounts for official business.
- Don't use personal hard drives, USB/thumb drives, external hard drives, or commercial cloud/file sharing services for official business; use only government approved storage devices or solutions.
- NEVER store or process PII or PHI on non-government computers!

Additional Resources

- DoD Cyber Exchange: https://public.cyber.mil/
- DoD Cyber Awareness Challenge: https://public.cyber.mil/training/cyber-awareness-challenge/
- DoD Phishing Awareness Training: https://public.cyber.mil/training/phishing-awareness/
- Bootable Media Online Training: https://cyber.mil/training/bootable-media/
- Trusted End Node Security (TENS): http://www.spi.dod.mil/
- US CERT COVID 19 Cyber Scams: https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams

Working Remotely

Maintaining a Cyber Mindset!