**TELEWORK BEST PRACTICES**

**DO**
- Only use agency-approved collaboration tools, including but not limited to chat and video conferencing platforms.
- Use your agency’s approved methods to share files. Be mindful of distribution and dissemination even when utilizing agency-approved platforms.
- Store work-related content on Government Furnished Equipment (GFE) and agency-approved cloud services only. Do not forward work emails to a personal email account.
- Log off of your remote connection at the end of the work day.
- Always remove your PIV card from your GFE whenever not in active use.
- Study and follow your agency’s acceptable use and telework policy on physical and information security. Ensure telework agreement(s) are current.
- Only connect GFE to a network you are in complete control of (e.g., home network). Do not connect to a network you do not own and control (e.g., public Wi-Fi).
- Use devices owned, managed, and protected by your agency, such as laptops or smart phones whenever possible.

**DON’T**
- Use your GFE or government desktop session for non-work-related activity (e.g., social networking, audio and video streaming, personal shopping).
- Print work-related materials at home, unless explicitly approved by your agency.
- Auto-forward your office phone to a personal number unless explicitly approved by your agency.
- Dial into phone or video conferences unless you were invited. Upon dialing into a phone conference, always announce your name and affiliation.
- Share devices (e.g., with family or other household members) that are used for work.
- Forward work emails to a personal email account.
- Store work-related content on personally owned equipment (including personal mobile devices and personal cloud or file-sharing accounts).
- Leave your computer unlocked when unattended.
- Send unencrypted, sensitive content (e.g., PHI).
- Connect to a network that you do not own and control (e.g., public Wi-Fi).

If you must use a personal device, first ensure use of personal devices is permitted by your department/agency’s policies, then:
- Follow department/agency policy for encrypting and signing emails.
- Require passwords to log into the device, use strong passwords, and change them frequently (including passwords for other accounts accessed from the same device).
- Only use non-privileged profiles for daily activities and only use elevated privileges when administering the device.
- Close all other non-work related windows and applications before and during work-related use of the personal equipment.
- Create a separate user profile with minimal privileges for work-only use.
- Close all work-related windows, applications, files, and documents when not in use.
- Clear browser cache when switching from work to personal use.
- Keep the operating systems and all relevant applications up-to-date and fully patched.
- Turn on automatic patching and run anti-virus software.
- If possible, use separate PIV card readers on personally owned equipment and avoid reconnecting them to GFE.

Adapted from the DoD Cyber Exchange Telework “Network Utilization and Cybersecurity Do’s and Don’t”