INDUSTRY CUI TELEWORK
DOs AND DON'Ts

Consistent with contractual requirements, and in accordance with ISOO CUI Memo 2020-03-30, CUI must be safeguarded at all times, including when handling the information in a telework environment. This guidance is not intended to replace an organization's telework policy and training requirements, but rather to remind individuals of their continuing responsibility to protect information and information systems.

The methods used to safeguard CUI, personally identifiable information (PII), and protected health information (PHI) may change with the environment but meeting the relevant cybersecurity and physical security safeguarding requirements required to prevent unauthorized disclosure of the CUI is crucial.

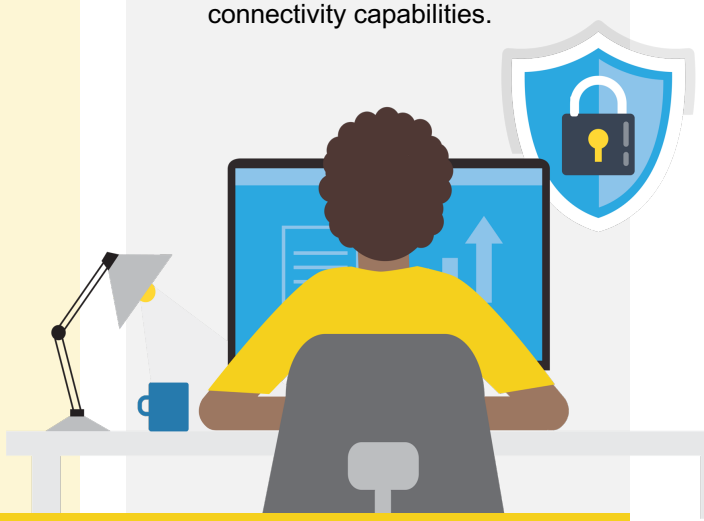
To better assist Industry, some examples of telework best practices when handling CUI include:

✓ DO:

- Study and follow the Acceptable Use Policy for your company or government systems if using government-furnished equipment (GFE).
- Cover any cameras on toys, laptops, and monitoring devices when not in use.
- Ensure GFE software is updated and connected to the organization's VPN gateway (for user authentication, secure communications, access control, etc.).
- Ensure that devices and computer equipment used at home (i.e., home routers, modems, and all connected devices) are up-to-date with the latest security patches and updates.
- Use a combination of security software (i.e., antivirus software, personal firewalls, spam and content filtering, popup blocking, etc.).
- Use organization's approved file sharing service/capabilities (e.g., DoD SAFE).
- Use a multi-factor authentication process for remote access (randomized numbers and letters, different passwords for each application, token-based authentication, network-based authentication, domain authentication, etc.).
- Use GFE for mission-essential activity only.
- Print CUI, PII, or PHI only when necessary.
- Enable encryption and establish strong passwords for home Wi-Fi.
- Secure CUI, PII, and PHI in a trusted location (e.g., locked file cabinet or safe).
- Log off the VPN connection, disconnect from the internet, and turn off the computer system at the end of the workday.

✗ DO NOT:

- Leave your GFE unlocked when not in use.
- Open suspicious emails or links.
- Send or forward unencrypted CUI, PII, or PHI.
- Leave CUI, PII, or PHI out in the open or unattended.
- Store CUI, PII, or PHI on personal systems.
- Work in public locations where others can "shoulder surf".
- Leave video collaboration tools connected when not in use.
- Converse about CUI or CUI-related matters near baby monitors, audio recordable toys, digital assistants, or devices with Internet-connectivity capabilities.



For additional information, please visit DCSA ESO Website (https://www.dcsa.mil/mc/isd/cui/) for additional information regarding CUI and teleworking with CUI.

August 29, 2022