# OPSEC AND TELEWORK SMART CARD

## Implementing Effective OPSEC While Teleworking

The DoD Telework Program, DoDI 1035.01, was created to foster workforce efficiency, emergency preparedness, and quality of life. When authorized, the employee being afforded an opportunity to telework has a responsibility to continue to protect controlled unclassified information (CUI) including Privacy Act or For Official Use Only data. The employee should also be familiar with the information identified on your organization's Critical Information and Indicators List (CIIL).

The first step for any employee or service member who is eligible to telework is to accomplish training on telework procedures to include information technology and data security. This OPSEC smart card is not designed to replace your organization's telework training requirements but is intended to remind employees of their continuing responsibility to protect information and information systems.

## Teleworking DOs

- DO coordinate with your organization's OPSEC point of contact for additional local guidance
- DO check out government furnished equipment with two-factor logon authentication enabled
- DO update antivirus software and operating system patches in accordance with organization guidance
- DO make sure you are aware of the organization's critical information and you have access to your unit's CIIL
- DO encrypt e-mails containing CUI (i.e., such as FOUO and Privacy Act) data or critical information
- DO use authorized data transfer tools when NIPRNet e-mail encryption is unavailable
- DO understand and implement local organization's telework security policy and procedures
- DO examine your surroundings when teleworking; not everyone nearby has a valid need to know
- DO bring all materials generated at home to the office to shred using authorized destruction methods
- DO remember our adversaries continue to exploit critical information during national emergencies

## Teleworking DON'Ts

- DON'T use workarounds to make telework security "easier" or "faster"
- DON'T use social media chat messaging tools to discuss sensitive operational activities or details
- DON'T use personal cellular or land line communications devices to talk about sensitive operational activities
- DON'T use personal e-mail accounts or providers to transmit sensitive operational activity information
- DON'T use non-government personal digital assistant devices to process sensitive operational activity info

## Additional Resources

The following additional resources are provided to enhance your understanding of how to protect information while teleworking. Remember, it is your responsibility to continue to protect controlled unclassified information.

- DoD Instruction 1035.1, Telework Policy - https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/103501p.pdf

- Federal Telework Program website - https://www .telework.gov

- Air Force Instruction 36-816, Civilian Telework Program - https://static.e-publishing.af.mil/production/1/af_a1/publication/dodi1035.01_afi36816/dodi103501_afi36-816.pdf

- AF OST generated smart cards - https://www.facebook.com/pg/AirForceOST/photos/?tab=album&album_id=2523387624580345

Air Force OPSEC Support Team (AF OST)
Joint Base San Antonio – Lackland AFB
DSN 945-2667
Commercial 210-925-2667
AF.OST@us.af.mil
https://www.facebook.com/AirForceOST/

Dated 23 March 2020, Version 1.0