TELECOMMUTING FAQS | THE DO'S AND DON'TS OF WORKING FROM HOME

1. **Can I connect my personal _____ to my INL laptop when telecommuting from home?**
   a. Monitor: Yes, if it is not a smart or blue tooth capable device.
   b. Wired keyboard and mouse: Yes
   c. Bluetooth keyboard and mouse: This is acceptable for a keyboard, mouse, and headsets. Understand there is a small risk of key stroke interception, but the likelihood is very low.
   d. 2.4 GHz keyboard and mouse: There is a higher risk with using this technology, so it should not be used. There are no concerns with using a mouse. Contact askcybersecurity@inl.gov if you have any questions.
   e. Wired, wireless, or network printers: Acceptable. Users will have to disconnect from virtual private network (VPN) to print locally to home or network computers or when using wireless connections. When connected to VPN, users will be unable to connect to home networks.
2. **What is Remote Desktop?**
   a. Remote Desktop is a program or an operating system feature that allows a user to connect to a computer in another location (i.e., your work computer located on INL's campus).
3. **If I need to Remote Desktop in, will I be able to do this from home on a VPN connection?**
   a. Remote desktop connections are allowed, and impacts on VPN use is determined by the amount of data being transferred through the connection or how many users are utilizing VPN.
4. **Can I print controlled unclassified information (CUI) with my home printer?**
   a. Approval from the proper authorities listed below is required before printing the following types of CUI:
      - PII – Any employee taking PII off INL premises, whether in hard-copy or electronically, should do so only when there is a legitimate INL business need and with the pre-approval of (i) the employee's manager, and (ii) with written authorization from Mandi Hong, Privacy Program Manager.
      - Program specific protected critical infrastructure information (PCII), critical energy infrastructure information (CEII), safeguards information (SGI), and all other CUI printing must be approved by program managers
   b. Reminder: CUI must not be stored on nongovernment systems or storage devices (personal computers, USBs, etc.)
   c. The following **SHOULD NOT** be printed using a home printer: unclassified controlled nuclear information (UCNI), naval nuclear propulsion information (NNPI), export-controlled information, international traffic arms regulations (ITAR), etc.
5. **How do I handle CUI at home?**
   a. Keep information in your direct possession or locked out of sight in a container or receptacle.
6. **Can I use my personal cellphone for work-related calls and texts?**
   a. Phone conversations are acceptable.
   b. Text messages must not include CUI or other protected data.
   c. If you have questions, please speak with your manager.