Mitigation

- Communicate telework and cybersecurity policies to your workforce
- Use Virtual Private Networks to guarantee encrypted connections to business networks
- Secure your virtual meetings:
  - Do not make meetings public
  - Require meeting passwords and use the waiting room feature to control the admittance of guests
  - Monitor and visually verify the identity of meeting members as they join
  - Lock events once all members have joined
  - Have a plan to terminate compromised meetings
- Telework connections outside the U.S. are less secure; have a plan in place to address potential risks posed by telework from foreign countries
- Use only the software and tools approved by your business for work-related meetings
- Consider limiting or prohibiting telework on public WiFi
- Regularly patch and update any personal device you use for telework
- Know your virtual telework platform’s country of origin. Some countries’ national security laws require your data to be stored on host-country servers, and may require on-demand remote access
- Use passphrases (instead of passwords) and multi-factor authentication to login to your systems
- Use security software that provides layered defenses via anti-virus, anti-phishing, anti-malware, safe browsing, and firewall capabilities
- Limit the personal data you share on any virtual platform
- Practice good cyber hygiene:
  - Always use caution when opening email attachments and clicking on links in emails
  - Backup data on external drives
  - Disable or disconnect devices when not in use
- Disconnect internet access when devices are not in use at home
- Cover your computer cameras when not in use