# SAFEGUARDING OUR FUTURE

## Virtual Telework Platforms - Protect Your Company Information

### THREAT

» Foreign powers can exploit virtual telework platforms to gain access to your company's proprietary data and your employees' sensitive personal information

### IMPACT

» Could support targeted cyber operations to expand access to your company's networks

» May record and archive your company's video conferences, revealing sensitive company data

» May be able to monitor your sessions in real-time

» May be able to gain access to your email, chats, contacts, and financial data

» Could provide a foreign entity with information that allows them to steal your market share

### MITIGATION

» Know your platform's country of origin as some foreign national security laws require your data to be stored on or pass through foreign servers -- they may even require direct or on-demand remote access

» Ensure your platform uses appropriate security features and strong encryption to prevent hacking and protect user confidentiality

» Use multifactor authentication and encrypted connections for sensitive discussions

» Know your terms of service and understand the encryption used for your connections

» Provide clear guidance to employees on which applications, sites, and platforms they can use, particularly on company or government computers

» Limit personal data you share on any virtual platform

» Use physical covers on your computer cameras when not in use

**For additional information on NCSC awareness materials or publications:**

» Follow us on Twitter : @NCSCgov

» Visit our Website : www.NCSC.gov

» For comments and questions, please contact us at : NCSC-Safeguarding-Our-Future@dni.gov

» Follow us on LinkedIn : https://www.linkedin.com/company/national-counterintelligence-and-security-center

Source image as of 7/2/2020: www.nist.gov/blogs/manufacturing-innovation-blog/are-you-ready | www.fda.gov/news-events/public-health-focus/lung-injuries-associated-use-vaping-products