Cybersecurity Considerations for Telework
Fern Stewart, Jeffrey Gliese, and Mohammad Esseqwe
Comptroller/Cybersecurity
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction
Many people now rely on computers and smartphones, which is the ability for an organization’s employees, contractors, business partners, vendors, and other users to perform work from locations other than the organization’s facilities. Teleworkers use various client devices, such as desktop and laptop computers, smartphones, and tablets, to read and send email, access websites, review and edit documents, and perform many other tasks. These client devices may be controlled by the organization, but they are not located in the organization’s facilities (e.g., [R2]). Remote users (or remote access), which is the ability for an organization’s users or employees to non-geographically compute resources from external locations other than the organization’s facilities.

The National Institute of Standards and Technology (NIST) has developed guidelines on telework and remote access to help organizations mitigate security risks associated with the increased use of remote access and other technology used for telework and remote access. NIST Special Publication 800-147, Guide to Enterprise Telecom, Wireless, and Can Access Control (2018), along with its updates, remains relevant today. This Information Technology Laboratory (ITL) Bulletin summarizes key concepts and recommendations from SP 800-147, including:

- Developing and enforcing a network security policy, such as achieving levels of remote access
- Implementing multistep authentication for enterprise access

Fern Stewart is a NIST Associate from the Cybersecurity Division.
Enterprise Planning

Plan telework-related security policies and controls based on a zero-trust model.
- Encrypt client devices’ storage, encrypt all sensitive data stored on client devices, or don’t store sensitive data on client devices
- Use strong authentication, preferably multi-factor, for enterprise access
- Use encryption technologies to protect the confidentiality and integrity of communications
- Authenticate each endpoint to the other to verify their identities

Develop a telework security policy that defines telework, remote access, and BYOD requirements.
- Define in the policy which forms of remote access are permitted and how the remote access servers will be administered
- Make risk-based decisions about what levels of remote access should be permitted from which types of telework client devices
Enterprise Implementation

Ensure that remote access servers are secured effectively and configured to enforce telework security policies.

- Keep remote access servers fully patched
- Only allow remote access servers to be managed from trusted hosts by authorized administrators
- Carefully choose the placement of each remote access server

Secure organization-controlled telework client devices against common threats, and maintain their security regularly.

- Ensure all types of telework client devices are secured, including smartphones and tablets
- Include all of the local security controls used for non-telework client devices, such as applying updates promptly, disabling unneeded services, and using anti-malware software (for desktops and laptops)
- Use additional security controls, such as encrypting sensitive data stored on the devices
Additional Resources

- NIST SP 800-46 Revision 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security
- NIST SP 800-77 Revision 1 (Draft), Guide to IPsec VPNs
- NIST SP 800-52 Revision 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
- NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices
- NIST SP 800-124 Revision 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise
- NIST SP 800-40 Revision 3, Guide to Enterprise Patch Management Technologies
- NIST SP 1800-4, Mobile Device Security: Cloud and Hybrid Builds
- NIST SP 1800-21 (Draft), Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)
Security & Privacy
Virtual Meeting Security

- First Rule: use common sense
- Follow your organization’s rules
- Consider what security is necessary
  - Not all calls are created equal
- Low
  - Know who’s on the call
- Medium
  - Basic security steps go a long way
- High
  - Use extra precautions
Telework Security Basics

• First Rule: use common sense
• Follow your organization’s rules
• Use a VPN
• Secure your devices
• Basic hygiene, basic security – still essential
• Watch for unusual activity
Additional Resources

Blogs


• https://www.nist.gov/blogs/cybersecurity-insights/telework-security-basics