GoldSky Cyber Security | White Paper

SECURING REMOTE WORKFORCES FOR SMALL-MIDSIZE BUSINESSES

How to prepare your remote workforce to operate in compliance with Federal Guidelines

Ron Frechette
Founder & CEO

Rudy Silva, CISSP
SE Cybersecurity Practice Director

TABLE OF CONTENTS

01 INTRODUCTION

02 OVERVIEW OF ENTERPRISE TELEWORK & REMOTE ACCESS SECURITY

03 REMOTE ACCESS SERVER SECURITY

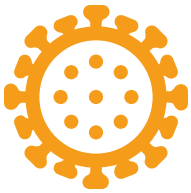
04 TELEWORK CLIENT DEVICE SECURITY

05 SECURITY CONSIDERATIONS FOR THE TELEWORK & REMOTE ACCESS LIFE CYCLE

06 CONCLUSION

01 INTRODUCTION

The spread of Coronavirus (aka COVID-19) has forced millions of companies to stand up remote workforces across the world, virtually overnight. Deploying this type of model on a global scale is unprecedented, especially for many small-midsize businesses (SMBs).



It is highly likely the majority of SMBs do not have the proper security controls in place, nor do they have the federal telework and remote access security guidelines required to help keep sensitive information and devices safe from cyber-attacks. Many global business thought leaders are predicting this could be the beginning of a Remote Workforce Revolution that will become the “new-normal” way of conducting business as we move further and further into the Digital Age.

This phenomenon has created the equivalent of the “California Gold Rush” within the cyber-criminal world. We are already beginning to see a dramatic increase in phishing, exploiting VPNs, malware dissemination, exploiting home network routers, and compromising unsecured IoT devices on home WiFi networks.

Threat actors use these types of nefarious tactics to exfiltrate sensitive data, subvert corporate networks, and leave behind malware Trojans for eventual remote exploitation, exfiltration and communication with unauthorized criminal networks.

Cyber security advisory firms have been quick to respond in advising their clients on deploying remote workforces that operate in a secure and compliant manner. Compliance is often a biproduct of having a secure environment. Knowing which compliance framework to use as a reference is critical to know as the Telework Trend evolves into the “new normal” way of conducting business.

01 INTRODUCTION

The federal government has established telework guidelines that are available free of charge under the National Institute of Standards and Technology (NIST). NIST is the federal government agency under the US Department of Commerce that is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems.

This white paper provides excerpts and summarizes remote workforce best practices as described in NIST Special Publication 800-46 Revision 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.

The NIST SP 800-46r2 publication is available free of charge and can be viewed in its entirety here.

02 OVERVIEW OF ENTERPRISE TELEWORK & REMOTE ACCESS SECURITY

This section of the publication provides an overview of security concerns for enterprise telework and remote access technologies. It explains the primary vulnerabilities and threats specific to telework and remote access security and recommends mitigation strategies for those threats. It also discusses the most commonly used types of remote access methods, examines their major vulnerabilities, and recommends security controls to mitigate threats. Finally, it briefly discusses special considerations related to the use of BYOD and third-party-controlled client devices on an organization's own networks.

VULNERABILITIES, THREATS, AND SECURITY CONTROLS SUMMARY

- To support confidentiality, integrity, and availability, all of the components of telework and remote access solutions should be secured against a variety of threats.
- Develop system threat models for the remote access servers and the resources that are accessed through remote access.
- Assume that client devices will be acquired by malicious parties
- Assume that the networks between the telework client device and the organization cannot be trusted.
- Assume that client devices will become infected with malware
- Conduct a Business Impact Analysis
- Ensure internal resources made available through remote access are hardened appropriately against external threats and that access to the resources is limited to the minimum necessary through firewalling and other access control mechanisms.

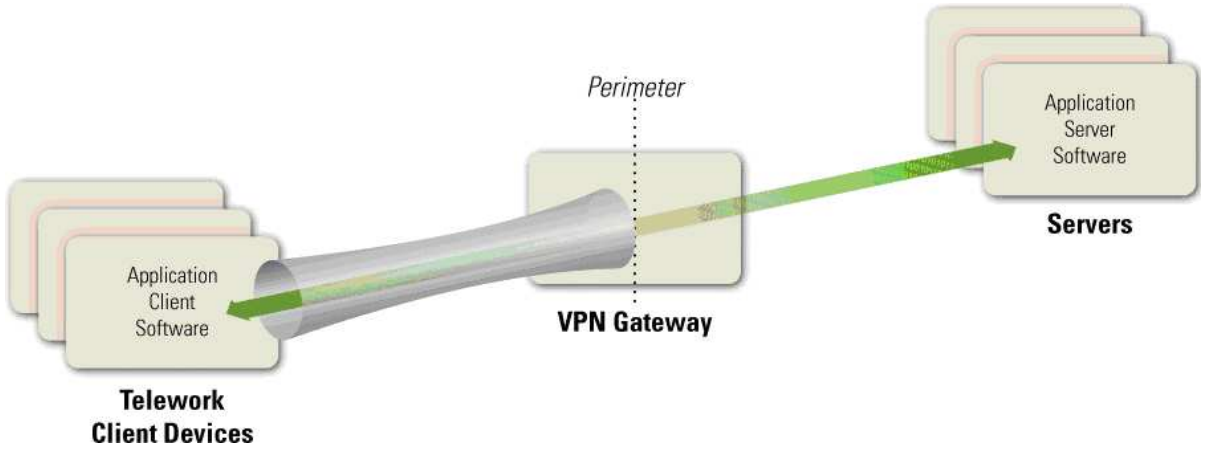
REMOTE ACCESS METHODS

When planning a remote access solution, organizations should carefully consider the security implications of the remote access methods in each of the four categories listed below, in addition to how well each method may meet operational requirements.

TUNNELING

Many remote access methods offer a secure communications tunnel through which information can be transmitted between networks, including public networks such as the Internet. Tunnels are typically established through virtual private network (VPN) technologies. Once a VPN tunnel has been established between a teleworker's client device and the organization's VPN gateway, the teleworker can access many of the organization's computing resources through the tunnel.

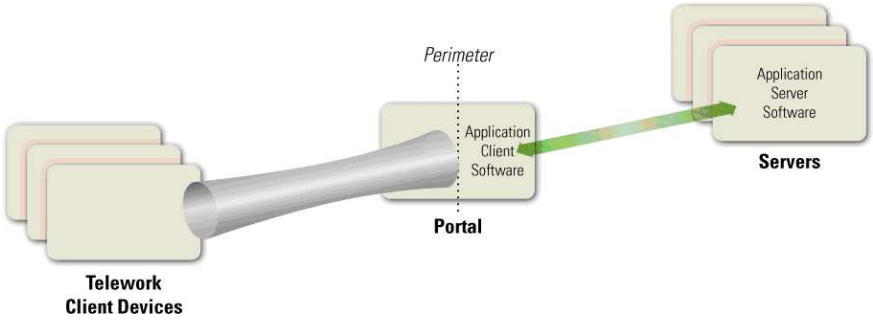
TUNNELING ARCHITECTURE



APPLICATION PORTALS

Another category of remote access solutions involves portals. A portal is a server that offers access to one or more applications through a single centralized interface. A teleworker uses a portal client on a telework client device to access the portal.

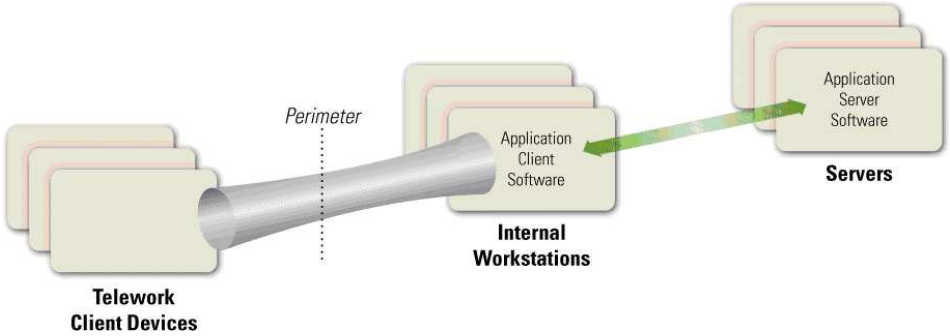
PORTAL ARCHITECTURE



REMOTE DESKTOP ACCESS

A remote desktop access solution gives a teleworker the ability to remotely control a particular PC at the organization, most often the user's own computer at the organization's office, from a telework client device.

REMOTE DESKTOP ACCESS ARCHITECTURE

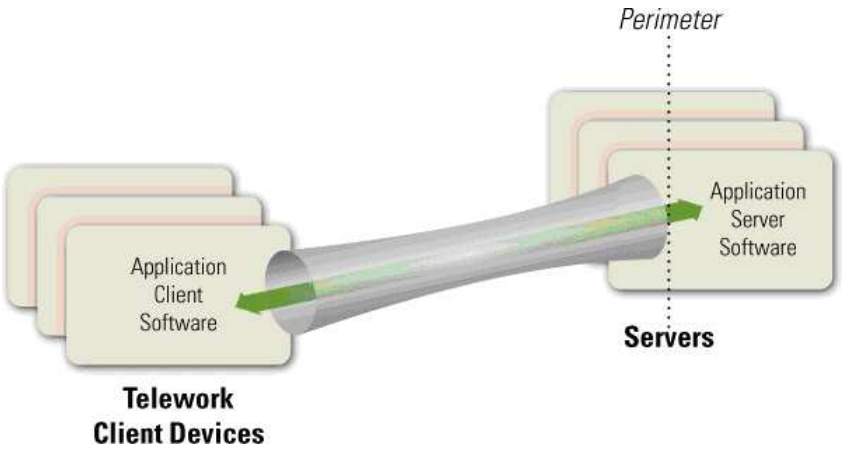


02 OVERVIEW OF ENTERPRISE TELEWORK & REMOTE ACCESS SECURITY

DIRECT APPLICATION PORTALS

Remote access can be accomplished without using remote access software. A teleworker can access an individual application directly, with the application providing its own security (communications encryption, user authentication, etc.)

DIRECT APPLICATION ACCESS ARCHITECTURE



BYOD & THIRD-PARTY CONTROLLED DEVICE CONSIDERATIONS

Organizations considering permitting BYOD devices within the enterprise should strongly consider establishing a separate, external, dedicated network for BYOD use within enterprise facilities. Such a network may also be used for third-party-controlled client devices if desired.

03 REMOTE ACCESS SOLUTION SECURITY

This section presents recommendations for securing remote access solutions. It focuses on remote access server security and server placement. It also discusses authentication, authorization, and access control. Recommendations for securing remote access client software are presented in this section, while recommendations for telework client device security are presented in Section 4.

REMOTE ACCESS SERVER SECURITY

- The security of remote access servers is particularly important. Recommendations for general server security are available from NIST SP 800-123, Guide to General Server Security. Remote access servers should be kept fully patched, operated using an organization-defined security configuration baseline, and only managed from trusted hosts by authorized administrators.
- Organizations should carefully consider the security of any remote access solutions that involve running a remote access server on the same host as other services and applications.

REMOTE ACCESS SERVER PLACEMENT

Organizations should consider several major factors when determining where to place a remote access server, including device performance, traffic examination, unprotected traffic, and NAT. Organizations should place remote access servers at the network perimeter unless there are compelling reasons to do otherwise.

INTERMEDIATE REMOTE ACCESS SERVERS

Intermediate remote access servers connect external hosts to internal resources, so they should usually be placed at the network perimeter. The server acts as a single point of entry to the network from the perimeter and enforces the telework security policy.

ENDPOINT REMOTE ACCESS SERVERS

Endpoint remote access servers should be placed in the organization's DMZ whenever possible. This allows a perimeter firewall to limit access to the servers from both external and internal hosts, and avoids the security issues involved in allowing external traffic to pass directly into the internal network.

REMOTE ACCESS AUTHENTICATION, AUTHORIZATION, AND ACCESS CONTROL

- To ensure that access is restricted properly, remote access servers should authenticate each teleworker before granting any access to the organization's resources, and then use authorization technologies to ensure that only the necessary resources can be used. Whenever feasible, organizations should implement mutual authentication, so that a remote access user can verify the legitimacy of a remote access server before providing authentication credentials to it.
- Any sensitive information from remote access communications passing over the Internet, wireless networks, and other untrusted networks should have its confidentiality and integrity preserved through use of cryptography. Federal agencies are required to use cryptographic algorithms that are NIST-approved and contained in FIPS-validated modules.

AUTHENTICATION

Organizations with higher security needs or with concerns about the security of passwords should consider using authentication that does not rely solely on passwords, such as multi-factor authentication.

AUTHORIZATION

After verifying the identity of a remote access user, organizations may choose to perform checks involving the telework client device to determine which internal resources the user should be permitted to access. These checks are sometimes called health, suitability, screening, or assessment checks. The most common way of implementing this is having the remote access server perform health checks on the teleworker's client device.

ACCESS CONTROL FOR NETWORK COMMUNICATIONS

A major component of controlling access to network communications and protecting their content is the use of cryptography. At a minimum, any sensitive information passing over the Internet, wireless networks, and other untrusted networks should have its confidentiality and integrity preserved through use of cryptography. Federal agencies are required to use cryptographic algorithms that are NIST- approved and contained in FIPS-validated modules. The FIPS 140 specification, Security Requirements for Cryptographic Modules, defines how cryptographic modules are validated.

03 REMOTE ACCESS SOLUTION SECURITY

REMOTE CONTROL CLIENT SOFTWARE SECURITY

Different types of remote access architectures offer different levels of granularity for application access control. Tunnels often have a mechanism for an administrator to specify which ports on which hosts the teleworker has access to; this can limit access so that only specific applications can be used. Portals, by their nature, limit the teleworker to applications run on the portal server.

REMOTE ACCESS CLIENT SOFTWARE SECURITY

- Organizations should ensure that remote management is properly secured, particularly encrypting network communications and performing mutual authentication of endpoints.
- Organizations with higher security needs or with particularly high risks against their remote access communications should use thick remote access clients whenever possible to reduce the risk of compromise.

04 TELEWORK CLIENT DEVICE SECURITY

Telework client devices should be secured properly and have their security maintained regularly. Generally, telework client devices should have the same local security controls as other client devices in the enterprise. However, because of the threats that client devices face in external environments, additional security controls are recommended, and some security controls may need to be adjusted to work effectively in telework environments. If the use of additional security controls is not feasible or enforceable, other approaches may be better, such as using VDI or VMI technologies or bootable removable media to establish a secure environment or adopting MDM solutions for enhancing and enforcing mobile device security.

SECURING TELEWORK PC'S

For telework PCs, personal firewalls capable of supporting multiple policies should be used whenever possible and configured properly for the enterprise environment and an external environment, at a minimum.

SECURING TELEWORK MOBILE DEVICES

For telework mobile devices, organizations should take advantage of centralized security management capabilities whenever available. However, many devices will need to be secured manually. Organizations should provide guidance to device administrators and users who are responsible for securing telework mobile devices on how they should secure them.

PROTECTING DATA ON TELEWORK CLIENT DEVICES

Sensitive information, such as certain types of PII (e.g., personnel records, medical records, financial records), that is stored on or sent to or from telework devices should be protected so that malicious parties cannot access or alter it. An organization should have a policy of encrypting all sensitive data when it is at rest on the device and on removable media used by the device. The creation and use of cryptographic keys for encrypting remote data at rest should follow the same policies that an organization has for other keys that protect data at rest.

05 SECURITY CONSIDERATIONS FOR THE TELEWORK & REMOTE ACCESS LIFE CYCLE

This section brings together the concepts presented in the previous sections of the guide and explains how they should be incorporated throughout the entire life cycle of telework and remote access solutions, involving everything from policy to operations. The section references a five-phase life cycle model to help organizations determine at what point in their telework and remote access deployments a recommendation may be relevant. This model is based on one introduced in NIST SP 800-64 Rev. 2, Security Considerations in the System Development Life Cycle. Organizations may follow a project management methodology or life cycle model that does not directly map to the phases in the model presented here, but the types of tasks in the methodology and their sequencing are probably similar.

PERMITTED FORMS OF REMOTE ACCESS

A telework security policy should define which forms of remote access the organization permits, which types of telework devices are permitted to use each form of remote access, the type of access each type of teleworker is granted, and how user account provisioning should be handled. It should also cover how the organization's remote access servers are administered and how policies in those servers are updated. The telework security policy should be documented in the system security plan.

RESTRICTIONS ON TELEWORK CLIENT DEVICES AND REMOTE ACCESS LEVELS

Each organization should make its own risk-based decisions about what levels of remote access should be permitted from which types of telework client devices.

05 SECURITY CONSIDERATIONS FOR THE TELEWORK & REMOTE ACCESS LIFE CYCLE

EXAMPLE OF ACCESS TIERS

APPLICATION OR SYSTEM	GFE IN OFFICE	GFE TELEWORK	BYOD IN OFFICE	C,P, V IN OFFICE	C,P,V TELEWORK	3RD PARTY
Personnel System	Yes	No	No	No	No	No
Financial System	Yes	Yes	No	No	No	No
Email	Yes	Yes	Yes	Yes	Yes	No
Calendaring	Yes	Yes	Yes	Yes	Yes	No
Intellectual Property	Yes	No	No	No	No	No

ADDITIONAL USER REQUIREMENTS

Organizations should periodically reassess their policies for telework devices and consider changing which types of client devices are permitted and what levels of access they may be granted.

DEVELOPMENT

Organizations should document the security aspects of the telework and remote access solution design in the system security plan.

IMPLEMENTATION

Before putting a remote access solution into production, an organization should implement and test a prototype of the design and evaluate it, including its connectivity, traffic protection, authentication, management, logging, performance, implementation security, and interference with applications.

OPERATIONS AND MAINTENANCE

- Organizations should regularly perform operational processes to maintain telework and remote access security, such as deploying updates, verifying clock synchronization, reconfiguring access control features as needed, and detecting and documenting anomalies within the remote access infrastructure.
- Organizations should also periodically perform assessments to confirm that the organization's remote access policies, processes, and procedures are being followed properly.

DISPOSAL

Before disposing of a telework client device or remote access server, the organization should remove any sensitive data from it.

06 CONCLUSION

Oftentimes a playbook this comprehensive can seem complex or maybe even overwhelming at first glance. However, if one steps back and thinks about the basic concepts it has been developed to address, an organization can quickly and easily start down the path to successfully addressing the risks associated with a dispersed, remote workforce.

In essence this guidebook, like all cybersecurity frameworks, is intended to help an organization address the 4 main vulnerabilities that lead to the majority of successful attacks. Those are: Human Error, Unpatched Systems, Password Breaches, and Social Engineering. As an organization assesses and remediates the implementation of their remote workforce, focusing on these 4 main vulnerabilities can help everyone involved in understanding the Why and How of what the organization is trying to achieve.

A security initiative such as this does not have to be overly sophisticated. As long as these 4 areas are being addressed, an organization can ensure they are protecting themselves against the majority of the attacks that may be perpetrated against them and can move forward with continuing to securely transition the way it operates in this ever-changing environment.

APPENDIX - A

NIST SP 800-53 CONTROL MAPPINGS

This appendix lists the NIST SP 800-53 Revision 4 security controls that are most pertinent for securing enterprise telework, remote access, and BYOD technologies. Next to each control is an explanation of its implications particular to enterprise telework, remote access, and BYOD security.

NIST SP 800-53 CONTROL	TELEWORK / REMOTE ACCESS/BYOD IMPLICATIONS
AC-2, Account Management	This control involves managing single-factor or multi-factor authentication for remote access users, such as passwords, digital certificates, and/or hardware authentication tokens.
AC-17, Remote Access	This entire control is dedicated to documenting remote access requirements, authorizing remote access prior to allowing connections, monitoring and controlling remote access, encrypting remote access connections, etc.
AC-19, Access Control for Mobile Devices	This control includes requirements for organization-controlled mobile devices and authorization to connect mobile devices to organizational systems, such as through remote access.
AC-20, Use of External Information Systems	This control involves the use of external information systems, such as personally owned client devices (BYOD) and third-party-controlled client devices, that may process, store, or transmit organization-controlled data on behalf of the organization.
CA-9, Internal System Connections	This involves connections between a system and system components, including mobile devices and laptops.
CP-9, Information System Backup	Telework devices need to have their data backed up either locally or remotely.
IA-2, Identification and Authentication (Organizational Users)	This control involves using single-factor or multi-factor authentication for remote access users, such as passwords, digital certificates, and/or hardware authentication tokens.
IA-3, Device Identification and Authentication	Mutual authentication is recommended whenever feasible to verify the legitimacy of a remote access server before providing authentication credentials to it.
IA-11, Re-Authentication	Many organizations require teleworkers to reauthenticate periodically during long remote access sessions, such as after each eight hours of a session or after 30 minutes of idle time. This helps organizations confirm that the person using remote access is authorized to do so.
RA-3, Risk Assessment	A risk assessment should be performed as part of selecting a remote access method (tunneling, application portals, remote desktop access, direct application access).
SC-7, Boundary Protection	This control involves segmenting a network (e.g., using subnetworks) to keep publicly accessible components off internal networks, and monitoring and controlling communications at key boundary points.
SC-8, Transmission Confidentiality and Integrity	The various remote access methods discussed in this publication protect the confidentiality and integrity of transmissions through use of cryptography.

APPENDIX - B

CYBERSECURITY FRAMEWORK SUBCATEGORY MAPPING

This appendix lists the Cybersecurity Framework48 subcategories that are most pertinent for securing enterprise telework, remote access, and BYOD technologies. Next to each subcategory is an explanation of its implications particular to enterprise telework, remote access, and BYOD security.

CYBERSECURITY FRAMEWORK SUBCATEGORY	TELEWORK/REMOTE ACCESS/BYOD IMPLICATIONS
ID.GV-1: Organizational information security policy is established	An organization should have a telework security policy.
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	A risk assessment should be performed as part of selecting a remote access method (tunneling, application portals, remote desktop access, direct application access).
PR.AC-1: Identities and credentials are managed for authorized devices and users	This control involves using single-factor or multi-factor authentication for remote access users, such as passwords, digital certificates, and/or hardware authentication tokens. Also, mutual authentication is recommended whenever feasible to verify the legitimacy of a remote access server before providing user authentication credentials to it.
PR.AC-3: Remote access is managed	An organization should formally manage all remote access processes and technologies.
PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	This involves segmenting a network (e.g., using subnetworks) to keep publicly accessible components off internal networks, and monitoring and controlling communications at key boundary points.
PR.DS-2: Data-in-transit is protected	The various remote access methods discussed in this publication protect the confidentiality and integrity of transmissions through use of cryptography.
PR.IP-4: Backups of information are conducted, maintained, and tested periodically	Telework devices need to have their data backed up either locally or remotely.

APPENDIX - C

RESOURCES

The lists below provide examples of resources that may be helpful in better understanding telework and remote access security. The NIST Special Publications identified below, along with many others, can also be **accessed via this link.**

TELEWORK SECURITY RESOURCES SITES

SITE NAME	URL
Home Network Security	www.us-cert.gov/security-publications/home-network-security
Safety & Security Center	www.microsoft.com/security/default.aspx
National Cyber Security Alliance	www.staysafeonline.org
telework.GOV	www.telework.gov

TELEWORK SECURITY-RELATED DOCUMENTS

DOCUMENT TITLE	URL
Bring Your Own Device: A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs	https://obamawhitehouse.archives.gov/digitalgov/bring-your-own-device
Guide to Telework in the Federal Government	www.telework.gov/guidance_and_legislation/telework_guide/telework_guide.pdf
NIST SP 800-48 Revision 1, Guide to Securing Legacy IEEE 802.11 Wireless Networks	http://dx.doi.org/10.6028/NIST.SP.800-48r1
NIST SP 800-52 Revision 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations	http://dx.doi.org/10.6028/NIST.SP.800-52r1
NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations	http://dx.doi.org/10.6028/NIST.SP.800-53r4
NIST SP 800-55 Revision 1, Performance Measurement Guide for Information Security	http://dx.doi.org/10.6028/NIST.SP.800-55r1
NIST SP 800-63-2, Electronic Authentication Guideline	http://dx.doi.org/10.6028/NIST.SP.800-63-2
NIST SP 800-77, Guide to IPsec VPNs	http://dx.doi.org/10.6028/NIST.SP.800-77
NIST SP 800-83 Revision 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops	http://dx.doi.org/10.6028/NIST.SP.800-83r1
NIST SP 800-88 Revision 1, Guidelines for Media Sanitization	http://dx.doi.org/10.6028/NIST.SP.800-88r1
NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i	http://dx.doi.org/10.6028/NIST.SP.800-97

APPENDIX - C

RESOURCES

TELEWORK SECURITY-RELATED DOCUMENTS

DOCUMENT TITLE	URL
NIST SP 800-113, Guide to SSL VPNs	http://dx.doi.org/10.6028/NIST.SP.800-113
NIST SP 800-114 Revision 1, User's Guide to Telework and Bring Your Own Device (BYOD) Security	http://dx.doi.org/10.6028/NIST.SP.800-114r1
NIST SP 800-115, Technical Guide to Information Security Testing and Assessment	http://dx.doi.org/10.6028/NIST.SP.800-115
NIST SP 800-118 (Draft), Guide to Enterprise Password Management	http://csrc.nist.gov/publications/PubsSPs.html#800-118
NIST SP 800-121 Revision 1, Guide to Bluetooth Security	http://dx.doi.org/10.6028/NIST.SP.800-121r1
NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)	http://dx.doi.org/10.6028/NIST.SP.800-122
NIST SP 800-123, Guide to General Server Security	http://dx.doi.org/10.6028/NIST.SP.800-123
NIST SP 800-124 Revision 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise	http://dx.doi.org/10.6028/NIST.SP.800-124r1
NIST SP 800-125, Guide to Security for Full Virtualization Technologies	http://dx.doi.org/10.6028/NIST.SP.800-125
NIST SP 800-147, BIOS Protection Guidelines	http://dx.doi.org/10.6028/NIST.SP.800-147
NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs)	http://dx.doi.org/10.6028/NIST.SP.800-153
NIST SP 800-163, Vetting the Security of Mobile Applications	http://dx.doi.org/10.6028/NIST.SP.800-163
NIST SP 800-167, Guide to Application Whitelisting	http://dx.doi.org/10.6028/NIST.SP.800-167
OMB Memorandum M-11-27, Implementing the Telework Enhancement Act of 2010: Security Guidelines	https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2011/m11-27.pdf