The following information was posted with the attached DRAFT document:

Mar. 14, 2016

SP 800-46 Rev. 2

DRAFT Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

NIST requests public comments on two draft Special Publications (SPs) on telework and BYOD security: Draft SP 800-46 Revision 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*, and Draft SP 800-114 Revision 1, *User's Guide to Telework and Bring Your Own Device (BYOD) Security*. Organizations are increasingly threatened, attacked, and breached through compromised telework devices used by their employees, contractors, business partners, and vendors. These publications make recommendations for organizations (in SP 800-46 Revision 2) and users (in SP 800-114 Revision 1) to improve their telework and BYOD security practices.

The public comment period for both publications closes on **April 15, 2016**.

Send comments on Draft SP 800-46 Revision 2 to 800-46comments<at>nist.gov with "Comments SP 800-46" in the subject line.
Send comments on Draft SP 800-114 Revision 1 to 800-114comments<at>nist.gov with "Comments SP 800-114" in the subject line.

Draft NIST Special Publication 800-46
Revision 2

Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

Murugiah Souppaya
Karen Scarfone

COMPUTER SECURITY

National Institute of
Standards and Technology
U.S. Department of Commerce

Draft NIST Special Publication 800-46 Revision 2

Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

March 2016

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3541 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-46 Revision 2
Natl. Inst. Stand. Technol. Spec. Publ. 800-46 Rev. 2, 53 pages (March 2016)
CODEN: NSPUE2

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by Federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, Federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Public comment period: *March 14, 2016* through *April 15, 2016*

All comments are subject to release under the Freedom of Information Act (FOIA).

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: 800-46comments@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

For many organizations, their employees, contractors, business partners, vendors, and/or others use enterprise telework or remote access technologies to perform work from external locations. All components of these technologies, including organization-issued and bring your own device (BYOD) client devices, should be secured against expected threats as identified through threat models. This publication provides information on security considerations for several types of remote access solutions, and it makes recommendations for securing a variety of telework, remote access, and BYOD technologies. It also gives advice on creating related security policies.

Keywords

bring your own device (BYOD); host security; information security; network security; remote access; telework

Acknowledgments

The authors, Murugiah Souppaya of the National Institute of Standards and Technology (NIST) and Karen Scarfone of Scarfone Cybersecurity, wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content.

The authors would also like to acknowledge the individuals who contributed to the original version of the publication: Simon Burson, Janet Cugini, Tim Grance (NIST), Anthony Grieco (Cisco Systems), Kurt Roemer (Citrix), Steven Sprague (Wave Systems), and representatives from the Department of Justice, the Department of Labor, the Department of State, the Federal Aviation Administration, and the Financial Management Service (U.S. Treasury). Special thanks go to Paul Hoffman of the VPN Consortium for his contributions to Revision 1 of the document. The authors would also like to acknowledge that NIST Special Publication (SP) 800-114*, User's Guide to Securing External Devices for Telework and Remote Access*, which was authored by Karen Scarfone and Murugiah Souppaya, was a major source of material for this publication.

Trademark Information

Table of Contents

Executive Summary vii

1. Introduction 1

1.1 Purpose and Scope 1
1.2 Audience 1
1.3 Document Structure 1

2. Overview of Enterprise Telework and Remote Access Security 2

2.1 Vulnerabilities, Threats, and Security Controls 2
2.2 Remote Access Methods 4
2.2.1 Tunneling 5
2.2.2 Application Portals 7
2.2.3 Remote Desktop Access 8
2.2.4 Direct Application Access 10
2.3 BYOD and Third-Party-Controlled Client Device Considerations 11
2.4 Summary of Key Recommendations 11

3. Remote Access Solution Security 13

3.1 Remote Access Server Security 13
3.2 Remote Access Server Placement 13
3.2.1 Intermediate Remote Access Servers 14
3.2.2 Endpoint Remote Access Servers 15
3.3 Remote Access Authentication, Authorization, and Access Control 15
3.3.1 Authentication 16
3.3.2 Authorization 17
3.3.3 Access Control for Network Communications 17
3.3.4 Access Control for Applications 18
3.4 Remote Access Client Software Security 19
3.5 Summary of Key Recommendations 20

4. Telework Client Device Security 21

4.1 Securing Telework PCs 22
4.2 Securing Telework Mobile Devices 24
4.3 Protecting Data on Telework Client Devices 25
4.3.1 Encrypting Data at Rest 26
4.3.2 Using Virtual Machines 26
4.3.3 Backing Up Data on Telework Devices 27
4.4 Summary of Key Recommendations 27

5. Security Considerations for the Telework and Remote Access Life Cycle 29

5.1 Initiation 30
5.1.1 Permitted Forms of Remote Access 30
5.1.2 Restrictions on Telework Client Devices and Remote Access Levels 30
5.1.3 Additional User Requirements 33
5.2 Development 34
5.3 Implementation 34
5.4 Operations and Maintenance 35
5.5 Disposal 36
5.6 Summary of Key Recommendations 36

Appendix A— NIST SP 800-53 Control Mappings..38
Appendix B— Cybersecurity Framework Subcategory Mapping 39
Appendix C— Glossary 40
Appendix D— Acronyms and Abbreviations 41
Appendix E— Resources...42

List of Figures and Tables

Figure 2-1. Tunneling Architecture 6
Figure 2-2. Portal Architecture 7
Figure 2-3. Remote Desktop Access Architecture 9
Figure 2-4. Direct Application Access Architecture..10
Table 5-1. Example of Access Tiers..33

Executive Summary

For many organizations, their employees, contractors, business partners, vendors, and/or other users utilize enterprise telework technologies to perform work from external locations. Most of these people use remote access technologies to interface with an organization's non-public computing resources. The nature of telework and remote access technologies—permitting access to protected resources from external networks and often externally controlled hosts as well—generally places them at higher risk than similar technologies only accessed from inside the organization, as well as increasing the risk to the internal resources made available to users through remote access.

All the components of telework and remote access solutions, including client devices, remote access servers, and internal resources accessed through remote access, should be secured against expected threats, as identified through threat models. Major security concerns include the lack of physical security controls, the use of unsecured networks, the connection of infected devices to internal networks, and the availability of internal resources to external hosts.

There are additional security concerns for organizations that permit the use of client devices outside the organization's control, such as employee, contractor, business partner, and vendor bring your own device (BYOD)[1] personally owned laptops, smartphones, and tablets; and contractor, business partner, and vendor-controlled devices, referred to in this publication as third-party-controlled technologies. Even though the organization may have agreements with employees and third parties that require their client devices to be properly secured, those agreements generally cannot be automatically enforced, so unsecured, malware-infected, and/or otherwise compromised devices may end up connected to sensitive organizational resources.

This publication provides information on security considerations for several types of remote access solutions, and it makes recommendations for securing a variety of telework, remote access, and BYOD technologies. It also gives advice on creating related security policies. To improve the security of their telework and remote access technologies, as well as better mitigate the risks posed by BYOD and third-party-controlled technologies to enterprise networks and systems, organizations should implement the following recommendations:

Plan telework-related security policies and controls based on the assumption that external environments contain hostile threats.

An organization should assume that external facilities, networks, and devices contain hostile threats that will attempt to gain access to the organization's data and resources. Organizations should assume that telework client devices, which are used in a variety of external locations and are particularly prone to loss or theft, will be acquired by malicious parties who will either attempt to recover sensitive data from them or leverage the devices to gain access to the enterprise network. Options for mitigating threats of loss or theft include encrypting the device's storage, encrypting all sensitive data stored on client devices, and not storing sensitive data on client devices. For mitigating device reuse threats, the primary option is using strong authentication—preferably multi-factor—for enterprise access.

Organizations should also assume that communications on external networks, which are outside the organization's control, are susceptible to eavesdropping, interception, and modification. This type of

[1] Strictly speaking, BYOD devices could be used only within the enterprise, and not for telework or remote access. However, the vast majority of BYOD devices are used externally, so for the purposes of this publication, all BYOD devices are considered telework devices. Also, the security concerns associated with enterprise-only BYOD devices are nearly identical to those for telework BYOD devices.

threat can be mitigated, but not eliminated, by using encryption technologies to protect the confidentiality and integrity of communications, as well as authenticating each of the endpoints to each other to verify their identities.

Another important assumption is that telework client devices will become infected with malware; possible controls for this include using antimalware technologies, using network access control solutions that verify the client's security posture before granting access, and using a separate network at the organization's facilities for telework client devices brought in for internal use (see the last recommendation in the Executive Summary for additional information).

Develop a telework security policy that defines telework, remote access, and BYOD requirements.

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, and the type of access each type of teleworker is granted. It should also cover how the organization's remote access servers are administered and how policies in those servers are updated.

As part of creating a telework security policy, an organization should make its own risk-based decisions about what levels of remote access should be permitted from which types of telework client devices. For example, an organization may choose to have tiered levels of remote access, such as allowing organization-owned personal computers (PCs) to access many resources, BYOD PCs and third-party-controlled client devices to access a limited set of resources, and BYOD smartphones and tablets to access only one or two lower-risk resources, such as webmail. Having tiered levels of remote access allows an organization to limit the risk it incurs by permitting the most-controlled devices to have the most access and the least-controlled devices to have minimal access.

There are many factors that organizations should consider when setting policy regarding levels of remote access to grant; examples include the sensitivity of the telework, the level of confidence in the telework client device's security posture, the cost associated with telework devices, the locations from which telework is performed, and compliance with mandates and other policies. For telework situations that an organization determines are particularly high-risk, an organization may choose to specify additional security requirements. For example, high-risk telework might be permitted only from organization-issued and secured telework client devices that employ multi-factor authentication and storage encryption. Organizations may also choose to reduce risk by prohibiting telework and remote access involving particular types of information, such as sensitive personally identifiable information (PII).[2]

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

The security of remote access servers is particularly important because they provide a way for external hosts to gain access to internal resources, as well as a secured, isolated telework environment for organization-issued, third-party-controlled, and BYOD client devices. In addition to permitting unauthorized access to enterprise resources and telework client devices, a compromised server could be used to eavesdrop on communications and manipulate them, as well as to provide a "jumping off" point for attacking other hosts within the organization. It is particularly important for organizations to ensure that remote access servers are kept fully patched and that they can only be managed from trusted hosts by authorized administrators. Organizations should also carefully consider the network placement of remote access servers; in most cases, a server should be placed at an organization's network perimeter so that it

[2] More information on protecting PII is available from NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (http://dx.doi.org/10.6028/NIST.SP.800-122).

acts as a single point of entry to the network and enforces the telework security policy before any remote access traffic or other traffic from telework client devices (such as BYOD devices using an organization's wireless BYOD network) is permitted into the organization's internal networks.

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

There are many threats to telework client devices, including malware and device loss or theft. Generally, telework client devices should include all the local security controls used in the organization's secure configuration baseline for its non-telework client devices.[3] Examples are applying operating system and application updates promptly, disabling unneeded services, and using antimalware software and a personal firewall. However, because telework devices are generally at greater risk in external environments than in enterprise environments, additional security controls are recommended, such as encrypting sensitive data stored on the devices, and existing security controls may need to be adjusted. For example, if a personal firewall on a telework client device has a single policy for all environments, then it is likely to be too restrictive in some situations and not restrictive enough in others. Whenever possible, organizations should use personal firewalls capable of supporting multiple policies for their telework client devices and configure the firewalls properly for the enterprise environment and an external environment, at a minimum.

Organizations should ensure that all types of telework client devices are secured, including PCs, smartphones, and tablets. For PCs, this includes physical security. For devices other than PCs, security capabilities and the appropriate security actions vary widely by device type and specific products, so organizations should provide guidance to device administrators and users who are responsible for securing telework mobile devices on how they should secure them.

If external device use (e.g., BYOD, third-party controlled) is permitted within the organization's facilities, strongly consider establishing a separate, external, dedicated network for this use.

Allowing personally owned and third-party-controlled client devices to be directly connected to an organization's enterprise networks adds considerable risk if the devices are placed on the organization's internal networks, because these devices are often not secured to the same degree as the organization's own devices. However, this risk can largely be mitigated by setting up a separate wired or wireless network within the enterprise dedicated to these devices. This network should be external (e.g., off the organization's demilitarized zone [DMZ]) and not grant any more access to enterprise resources than users already have through remote access. This network should be secured and monitored in a manner consistent with how remote access segments are secured and monitored.

[3] The National Checklist Repository (http://checklists.nist.gov/) is a source of security configuration baseline information.

1. Introduction

1.1 Purpose and Scope

The purpose of this document is to assist organizations in mitigating the risks associated with the enterprise technologies used for telework, such as remote access servers, telework client devices (including bring your own device [BYOD] and contractor, business partner, and vendor-controlled client devices, also known as third-party-controlled devices), and remote access communications. The document emphasizes the importance of securing sensitive information stored on telework devices and transmitted through remote access across external networks. This document provides recommendations for creating telework-related policies and for selecting, implementing, and maintaining the necessary security controls for remote access servers and clients.

1.2 Audience

This document is primarily intended for security, system, and network engineers and administrators, as well as computer security program managers, who are responsible for the technical aspects of preparing, operating, and securing remote access solutions and client devices. Portions of the document are also intended for higher-level management, such as the individuals responsible for creating telework policies. The material in this document is technically oriented, and it is assumed that readers have at least a basic understanding of remote access, networking, network security, and system security.

1.3 Document Structure

The remainder of this document is organized into the following sections:

- Section 2 provides an overview of enterprise telework and remote access security. It discusses general vulnerabilities and threats against telework and remote access solutions. It also describes the high-level architectures of common remote access methods and the security characteristics of each architecture. Finally, it discusses concerns particular to BYOD use of organization networks.
- Section 3 presents recommendations for securing remote access solutions, including server security, server placement, and client software security. It also covers authentication, authorization, and access control for remote access solutions.
- Section 4 offers recommendations for securing telework client devices and protecting data on them.
- Section 5 discusses security throughout the telework and remote access life cycle. Examples of topics addressed in this section include telework security policy creation, design and implementation considerations, and operational processes that are particularly helpful for security.

The document also contains appendices with supporting material:

- Appendices A and B contain mappings to NIST Special Publication (SP) 800-53 controls and Cybersecurity Framework subcategories, respectively.
- Appendices C and D contain a glossary and an acronym list, respectively.
- Appendix E lists resources that may be useful for gaining a better understanding of telework and remote access security.

2. Overview of Enterprise Telework and Remote Access Security

Many people *telework* (also known as *telecommuting*), 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, by third parties (the organization's contractors, business partners, or vendors), or by the users themselves (e.g., BYOD). Most teleworkers use *remote access*, which is the ability for an organization's users to access its non-public computing resources from external locations other than the organization's facilities.

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.

2.1 Vulnerabilities, Threats, and Security Controls

Telework and remote access solutions typically need to support several security objectives. These can be accomplished through a combination of security features built into the remote access solutions and additional security controls applied to the telework client devices and other components of the remote access solution. The most common security objectives for telework and remote access technologies are as follows:

- Confidentiality—ensure that remote access communications and stored user data cannot be read by unauthorized parties;
- Integrity—detect any intentional or unintentional changes to remote access communications that occur in transit; and
- Availability—ensure that users can access resources through remote access whenever needed.

To achieve these objectives, all of the components of telework and remote access solutions, including client devices, remote access servers, and internal servers accessed through remote access, should be secured against a variety of threats. General security recommendations for any IT technology are provided in NIST Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*.[4] Specific recommendations for securing telework and remote access technologies are presented in this publication and are intended to supplement the controls specified in SP 800-53.

Telework and remote access technologies often need additional protection because their nature generally places them at higher exposure to external threats than technologies only accessed from inside the organization. Before designing and deploying telework and remote access solutions, organizations should develop system threat models for the remote access servers and the resources that are accessed through remote access. Threat modeling involves identifying resources of interest and the feasible threats,

[4] These recommendations are linked to three security categories—low, moderate, and high—based on the potential impact of a security breach involving a particular system, as defined in Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems* (http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf).

vulnerabilities, and security controls related to these resources, then quantifying the likelihood of successful attacks and their impacts, and finally analyzing this information to determine where security controls need to be improved or added. Threat modeling helps organizations to identify security requirements and to design the remote access solution to incorporate the controls needed to meet the security requirements. Major security concerns for these technologies that would be included in most telework threat models are as follows:

- **Lack of Physical Security Controls.** Telework client devices are used in a variety of locations outside the organization's control, such as users' homes, coffee shops, hotels, and conferences. The mobile nature of these devices makes them likely to be lost or stolen, which places the data on the devices at increased risk of compromise. When planning telework security policies and controls, organizations should assume that client devices will be acquired by malicious parties who will either attempt to recover sensitive data from the devices or leverage the devices to gain access to the enterprise network.

  The primary mitigation strategies for device loss or theft are to encrypt the client device's storage or just the sensitive data itself so that it cannot be recovered from the device by unauthorized parties, or to not store sensitive data on client devices. Even if a client device is always in the possession of its owner, there are other physical security risks, such as an attacker looking over a user's shoulder at a coffee shop and viewing sensitive data on the client device's screen. Organizations can mitigate threats involving device reuse, such as an attacker gaining remote control over a device or impersonating a user, by using strong authentication, preferably multi-factor authentication, for enterprise access.

- **Unsecured Networks.** Because nearly all remote access occurs over the Internet, organizations normally have no control over the security of the external networks used by telework clients. Communications systems used for remote access include broadband networks such as cable, and wireless mechanisms such as IEEE 802.11 and cellular networks.[5] These communications systems are susceptible to eavesdropping, which places sensitive information transmitted during remote access at risk of compromise. Man-in-the-middle (MITM) attacks may also be performed to intercept and modify communications.

  Organizations should plan their remote access security on the assumption that the networks between the telework client device and the organization cannot be trusted. Risk from use of unsecured networks can be mitigated, but not eliminated, by using encryption technologies to protect the confidentiality and integrity of communications, as well as using mutual authentication mechanisms to verify the identities of both endpoints.

- **Infected Devices on Internal Networks.** Telework client devices, particularly BYOD and third-party-controlled laptops, are often used on external networks and then brought into the organization and attached directly to the organization's internal networks. Also, an attacker with physical access to a client device may install malware on the device to gather data from it and from networks and systems that it connects to. If a client device is infected with malware, this malware may spread throughout the organization once the client device is connected to the internal network. Organizations should assume that client devices will become infected and plan their security controls accordingly.

  In addition to mandating use of appropriate antimalware technologies, such as antivirus software on laptops, organizations should consider the use of network access control (NAC) solutions that verify

[5] Because of this assumption of lack of security of the network connection, this publication does not address leased lines, dial-up and DSL modems, or other communications mechanisms that can be secured at the data link layer. If an organization uses a data link mechanism that adds security, the type of security described in this document would be on top of that data link security, but would not interact with it.

the security posture of a client device before allowing it to use an internal network. Organizations should also consider using a separate network for all external client devices, including BYOD and third-party-controlled devices, instead of permitting them to directly connect to the internal network. Section 4 contains additional recommendations and suggestions for improving client device security.

- **External Access to Internal Resources.** Remote access, including access from BYOD and third-party-controlled client devices attached to an organization's wireless BYOD networks, provides external hosts with access to internal resources, such as servers. If these internal resources were not previously accessible from external networks, making them available via remote access will expose them to new threats, particularly from untrusted client devices and networks, and significantly increase the likelihood that they will be compromised. Each form of remote access that can be used to access an internal resource increases the risk of that resource being compromised.

  Organizations should carefully consider the balance between the benefits of providing remote access to additional resources and the potential impact of a compromise of those resources. Organizations should ensure that any internal resources they choose to make available through remote access are hardened appropriately against external threats[6] and that access to the resources is limited to the minimum necessary through firewalling and other access control mechanisms.

See Section 2.3 for information on security concerns specific to BYOD and third-party-controlled client devices.

Section 2.2 describes remote access technologies and discusses security considerations for each, focusing on the elements described above.

2.2 Remote Access Methods

Organizations have many options for providing remote access to their computing resources. As previously mentioned, remote access methods can also be used to enable access to internal resources for BYOD and third-party-controlled client devices attached to an organization's wireless BYOD networks. For the purposes of this publication, the remote access methods most commonly used for teleworkers have been divided into four categories based on their high-level architectures: tunneling, portals, remote desktop access, and direct application access. The remote access methods in all four categories have some features in common:

- They are all dependent on the physical security of the client devices.
- They can use multiple types of server and user authentication mechanisms. This flexibility allows some remote access methods to work with an organization's existing authentication mechanisms, such as passwords or certificates. Some remote access methods have standardized authentication mechanisms, while others use implementation-specific mechanisms.
- They can use cryptography to protect the data flowing between the telework client device and the organization from being viewed by others. This cryptographic protection is inherent in VPNs and cryptographic tunneling in general, and it is an option in most remote desktop access and direct application access systems.
- They can allow teleworkers to store data on their client devices. For example, most tunnel, portal, and remote desktop access systems offer features for copying files from computers inside the organization to the teleworker's client device. This allows the teleworker to work with the data locally, such as in a

[6] Sources of hardening information include the National Checklist Repository (http://checklists.nist.gov/) and NIST SP 800-123, *Guide to General Server Security* (http://dx.doi.org/10.6028/NIST.SP.800-123).

locally installed word processor. Some applications that can be reached through direct application access also allow transmitting files to the teleworker. Data may also be stored on client devices inadvertently, such as through operating system page files or web browser caches. It is important that all data sent to the teleworker through remote access be covered by the organization's data distribution and data retention policies.

Sections 3 and 4 provide more details on remote access authentication, communications encryption, and client data security.

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

The figures in the following sections show some of the operational and security properties of the four categories of remote access methods.

- The flared pipe is the cryptographically-protected communications that originate with the teleworker's device.
- The arrow and the application software labels indicate the flow of communications between the application client and server software.
- The dotted vertical line shows the perimeter of the organization's network. Everything to the left of the dotted line represents the Internet and/or the organization's external wireless BYOD networks, while to the right of the dotted line is the internal network.

2.2.1 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. To use a VPN, users must either have the appropriate VPN software on their client devices or be on a network that has a VPN gateway system on it. In Figure 2-1, a VPN client is installed on each of the client devices, and there is a single VPN gateway that runs the VPN server software. The pipe represents a secure remote access connection (tunnel) between a client device and the VPN gateway. Through this tunnel, application client software (e.g., email client, word processor, web browser, database client) installed on the client device communicates with application server software residing on servers within the organization.[7] The VPN gateway can take care of user authentication, access control (at the host, service, and application levels), and other security functions for teleworkers.

[7] This architecture, with the VPN gateway and the application servers being on separate hosts, is the most commonly used tunneling solution for remote access. However, the VPN gateway and the application servers could be on a single host.

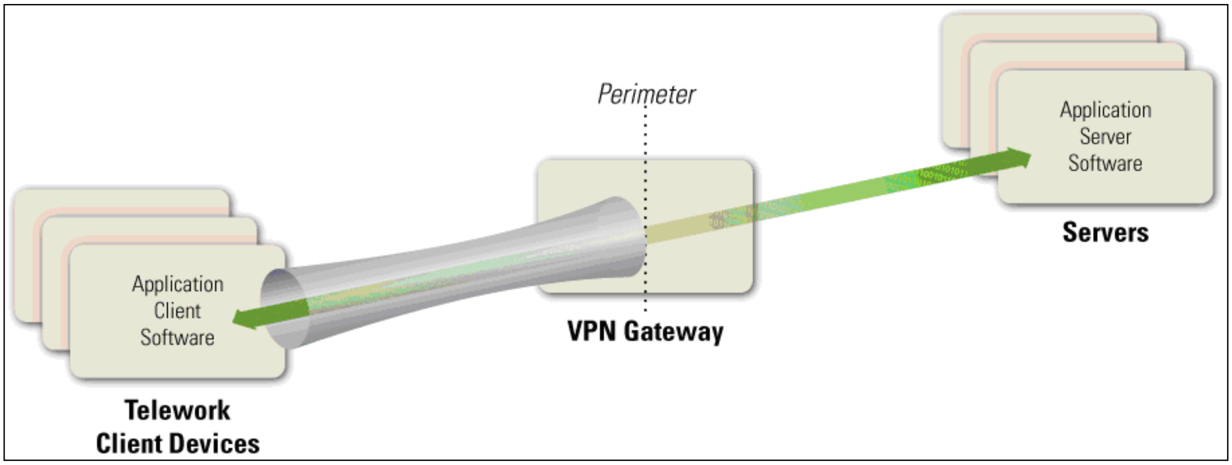

Figure 2-1. Tunneling Architecture

Tunnels use cryptography to protect the confidentiality and integrity of the transmitted information between the client device and the VPN gateway. Tunnels can also authenticate users, provide access control (such as restricting which protocols may be transmitted or which internal hosts may be reached through remote access), and perform other security functions. However, although remote access methods based on tunneling protect the communications between the client device and the VPN gateway, they do not provide any protection for the communications between the VPN gateway and internal resources. Also, in tunneling solutions, the application client software and data at rest resides on the client device, so they are not protected by the tunneling solution and should be protected by other means.

The types of VPNs most commonly used for teleworkers are Internet Protocol Security (IPsec) and Secure Sockets Layer (SSL)[8] tunnels.[9] Tunneling may also be achieved by using Secure Shell (SSH), although this is less commonly used and is often considered more difficult to configure and maintain than IPsec or SSL tunnel VPNs. All three forms of tunneling mentioned in this section can protect many protocols at once. More information on the tunneling protocols is available from NIST SP 800-77, *Guide to IPsec VPNs*,[10] NIST SP 800-113, *Guide to SSL VPNs*,[11] and NIST Internal Report (IR) 7966, *Security of Interactive and Automated Access Management Using Secure Shell (SSH)*.[12]

Many communication encryption protocols can be expanded into tunneling protocols in the same way that TLS is used for SSL VPNs. For example, some systems use the SSH protocol to create tunnels. In general, standardized tunneling protocols can be configured to have the same cryptographic strength and to use the same (or functionally similar) mechanism for authenticating the two parties to each other. Different tunneling systems can tunnel various protocols; for example, IPsec has standardized extensions that allow it to tunnel Layer 2 protocols such as the Point-to-Point Protocol (PPP) and Multiprotocol Label Switching (MPLS). In general, almost any communication encryption protocol can be made to tunnel almost any layer.

[8] Although this technology is widely known as an SSL VPN, it typically uses Transport Layer Security (TLS) instead of SSL to encrypt communications because TLS offers stronger security than SSL. See 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) for additional insights into TLS and SSL.

[9] Another, more commonly used form of SSL VPNs uses a portal architecture. Section 2.2.2 discusses SSL portal VPNs. An SSL tunnel VPN generally uses a plug-in installed within a web browser that supports tunneling within a TLS connection.

[10] http://dx.doi.org/10.6028/NIST.SP.800-77

[11] http://dx.doi.org/10.6028/NIST.SP.800-113

[12] http://dx.doi.org/10.6028/NIST.IR.7966

The VPN gateway can control access to the parts of the network and the types of access that the teleworker gets after authentication. For example, a VPN might allow a user to only have access to one subnet, or to only run particular applications on certain servers on the protected network. In this way, even though the cryptographic tunnel ends at the VPN gateway, the gateway can add additional routing to the teleworker's traffic to only allow access to some parts of the internal network.

VPNs are usually established and managed by VPN gateway devices owned and managed by the organization being protected. In some cases, organizations outsource their VPNs to trusted third parties. Such a third party might simply manage the VPN gateway that is owned by the organization, but other third parties offer services where they own and control the VPN gateway. In the latter case, the organization should evaluate the security of the proposed solution and ensure it will support the organization’s security policy.

2.2.2 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. Most portals are web-based—for them, the portal client is a regular web browser. Figure 2-2 shows the basic portal solution architecture. The application client software is installed on the portal server, and it communicates with application server software on servers within the organization. The portal server communicates securely with the portal client as needed; the exact nature of this depends on the type of portal solution in use, as discussed below.

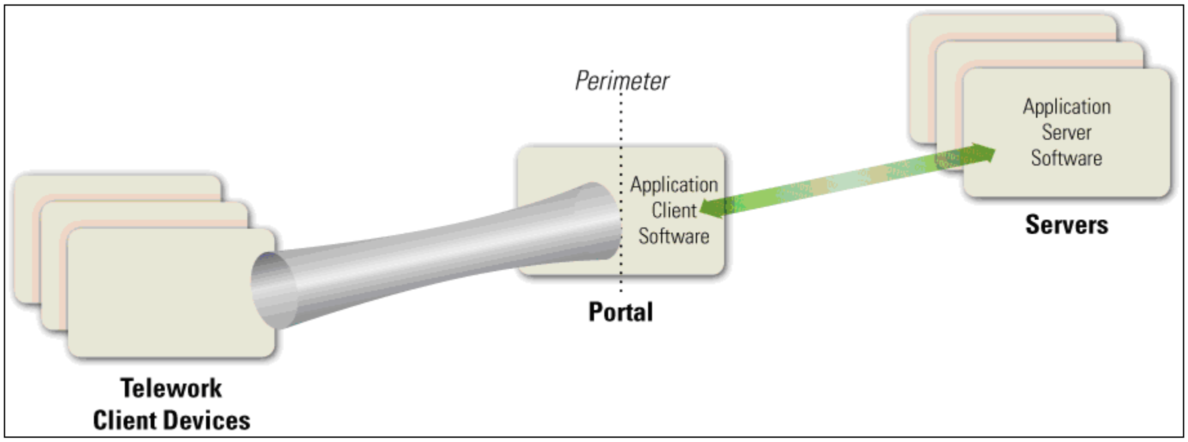

Figure 2-2. Portal Architecture

In terms of security, portals have most of the same characteristics as tunnels: portals protect information between client devices and the portal, and they can provide authentication, access control, and other security services. However, there is an important difference between tunnels and portals—the location of the application client software and associated data. In a tunnel, the software and data are on the client device; in a portal, they are on the portal server. A portal server transfers data to the client device as rendered desktop screen images or web pages, but data is typically stored on the client device much more temporarily than data for a tunneled solution is. (However, portals can be configured to allow clients to download content from the portal and store it on the client device or other locations outside the secure remote access environment.) Having the application client software centralized gives an organization more control over how the software and data is secured as opposed to more distributed remote access solutions. Portals limit the access a teleworker has to particular application clients running on the portal itself. Those applications further limit the access the teleworker has to the servers inside the network.

There are a few types of portal solutions commonly used for remote access. A *web-based portal* provides a user with access to multiple web-based applications from a single portal website. An SSL portal VPN is a common form of web-based portal. Another type of portal solution is *terminal server access*, which gives each teleworker access to a separate standardized virtual desktop. The terminal server simulates the look and feel of a desktop operating system and provides access to applications. Terminal server access requires the teleworker either to install a special terminal server client application on the client device or to use a web-based interface, often with a browser plug-in or other additional software provided by the organization. Another similar remote access method, called *virtual desktop infrastructure (VDI)*, involves the user connecting to a system that contains virtual images of standardized, non-simulated operating systems and desktops. When the teleworker is finished with a remote access session, the virtual image is discarded so that the next user will have a clean virtual desktop. VDI is particularly helpful for safeguarding telework on BYOD and third-party-controlled devices, which are more likely than organization-issued devices to not meet the organization's security requirements.

The mechanism for providing an interface to the teleworker varies among portals. For example, terminal server access and VDI present a standardized virtual desktop to the teleworker, while SSL portal VPNs present each application through a web page. The nature of this interface is important because it relates to the storage, temporary or permanent, of data. For many portals, the user interface is virtual, and after the user session is over, that instance of the interface is essentially destroyed and a clean version used for the next session. Some portals, such as SSL portal VPNs, can be configured to establish a secure virtual machine on the client device through a VDI solution, restrict all remote access data to reside within that virtual machine, and then securely destroy the virtual machine instance and all the data that existed within it when the session ends. This helps to ensure that sensitive information does not inadvertently become stored on a telework client device, where it could possibly be recovered by a future compromise.

Although terminal server access and VDI technologies are primarily meant for telework PCs, there is an emerging technology that provides similar capabilities for mobile devices: virtual mobile infrastructure (VMI). Just as a VDI solution delivers a secure virtual desktop to a telework PC, so does VMI deliver a secure virtual mobile device environment to a telework mobile device. Organizations considering the use of mobile devices for telework, particularly BYOD or third-party-controlled mobile devices, should investigate VMI technologies to see if they may be helpful in improving security.

2.2.3 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. The teleworker has keyboard and mouse control over the remote computer and sees that computer's screen on the local telework client device's screen. Remote desktop access allows the user to access all of the applications, data, and other resources that are normally available from their PC in the office. Figure 2-3 shows the basic remote desktop access architecture. A remote desktop access client program or web browser plug-in is installed on each telework client device, and it connects directly with the teleworker's corresponding internal workstation on the organization's internal network.

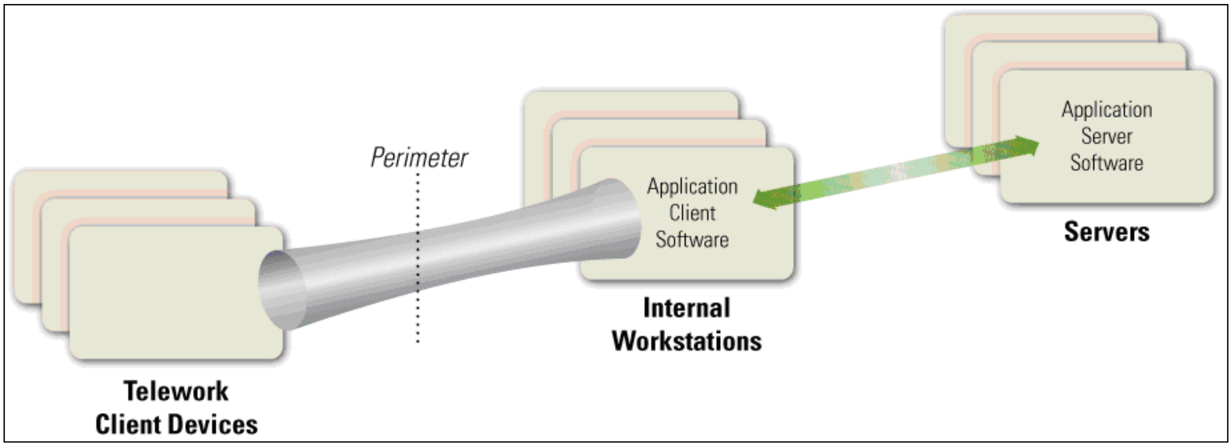

Figure 2-3. Remote Desktop Access Architecture

There are two major styles of remote desktop access: direct between the telework client and the internal workstation, and indirect through a trusted intermediate system. However, direct access is often not possible because it is prevented by many firewalls. For example, if the internal workstation is behind a firewall performing network address translation (NAT), the telework client device cannot initiate contact with the internal workstation unless either the NAT allows such contact[13] or the internal workstation initiates communications with the external telework client device (e.g., periodically checking with the client device to see if it wants to connect).

Indirect remote desktop access is performed through an intermediate server. This server is sometimes part of the organization's firewall, but is more often run by a trusted commercial or free third-party service outside the organization's network perimeter. Usually there are separate connections between the telework client device and the service provider, and between the service provider and the internal workstation, with the intermediate server handling the unencrypted communications between the separate connections. The security of this intermediate server is very important, because it is responsible for properly authenticating teleworkers and preventing unencrypted traffic from being accessed by unauthorized parties. Also, if the organization’s security policy requires particular kinds of authentication (such as the two-factor authentication required by federal agencies), the intermediate server should support this authentication in both directions. Before implementing an indirect remote desktop access solution, an organization should evaluate the security provided by the service provider, especially possible threats involving the intermediate server and the potential impact of those threats. The organization can then identify compensating controls to mitigate the threats, such as applying a second level of communications encryption at the application layer, and determine under what circumstances the intermediate system may be used, such as for low-risk activities.

The remote desktop access software protects the confidentiality and integrity of the remote access communications and also authenticates the user to ensure that no one else connects to the internal workstation. However, because this involves end-to-end encryption of the communications across the organization’s perimeter, the contents of the communication are hidden from the network security controls at the perimeter, such as firewalls and intrusion detection systems. For many organizations, the increased risk caused by this is not worth the benefits, and direct connections from external client devices to internal workstations are prohibited.

[13] This can be accomplished using a “pinhole” scheme that requires particular ports to be allocated to each workstation.

Another serious security issue with remote desktop access software is that it is decentralized; instead of the organization having to secure a single VPN gateway server or portal server, the organization instead has to secure each internal workstation that may be accessed through remote desktop access. Because these internal workstations can be accessed from the Internet, either directly or indirectly, they generally need to be secured nearly as rigorously as full-fledged remote access servers, yet such workstations were usually not designed with that degree of security in mind. Applying compensating controls for each workstation to raise its security to an acceptable level often involves a significant amount of time and resources, as well as acquisition of additional security controls. Also, authentication solutions such as two-factor authentication capabilities may need to be deployed to each internal workstation using remote desktop access.

Generally, remote desktop access solutions, such as those using the Microsoft Remote Desktop Protocol RDP) or Virtual Network Computing (VNC), should only be used for exceptional cases after a careful analysis of the security risks. The other types of remote access solutions described in this section offer superior security capabilities.

2.2.4 Direct Application Access

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.) Figure 2-4 shows the high-level architecture for direct application access. The application client software installed on the telework client device initiates a connection with a server, which is typically located at the organization's perimeter (e.g., in a demilitarized zone [DMZ]) or in an Internet-facing cloud architecture.

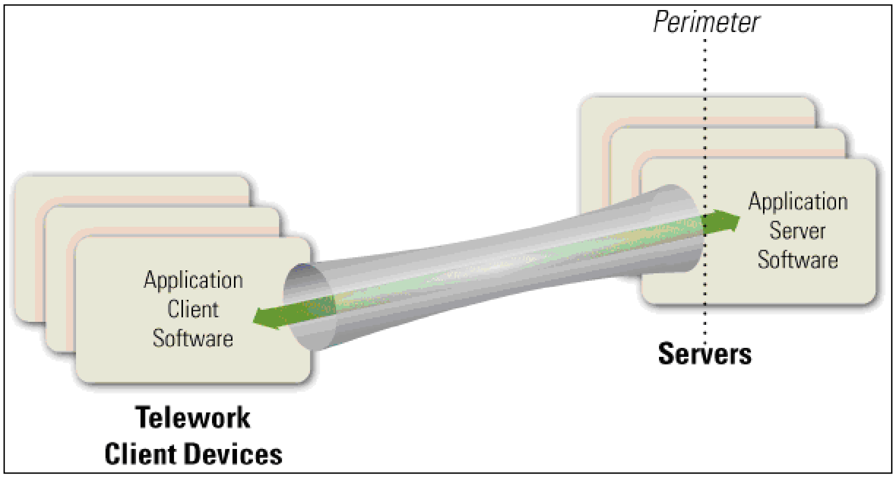

Figure 2-4. Direct Application Access Architecture

One of the most common examples of direct application access is webmail. The teleworker runs a web browser and connects to a web server that provides email access. The web server runs HTTP over TLS (HTTPS) to protect the communications, and the webmail application on the server authenticates the teleworker before granting access to the teleworker's email. For cases such as webmail that use a ubiquitous application client (e.g., a web browser), direct application access provides a highly flexible remote access solution that can be used from nearly any client device. Another common example of direct application access is a smartphone app (client software) that connects to a service provided by one of the organization's servers through HTTPS.

For the same reasons discussed in Section 2.2.3, the direct application access architecture is generally only acceptable if the servers being accessed by the teleworkers are located on the organization's network perimeter or in a public-facing cloud, and not internal networks. Servers that are directly accessible from the Internet should already be well-secured to reduce the likelihood of compromise. Many organizations choose to provide direct application access to only a few lower-risk applications that are widely used, such as email, and use tunnel or portal methods to provide access to other applications, particularly those that would be at too much risk if they were directly accessible from the Internet.

2.3 BYOD and Third-Party-Controlled Client Device Considerations

For many years, it has been a common practice for organizations to permit remote access and telework to be performed from employees, contractors, business partners, and vendors' personally owned computing devices. A more recent trend, BYOD, expands on this telework concept to allow these devices to be directly connected to an organization's enterprise networks. This adds considerable risk to an organization if the devices are placed on the organization's internal networks, because BYOD devices, which are managed by the users themselves, are typically not secured to the same degree as the organization's own devices. However, this risk can largely be mitigated by setting up a separate wired or wireless network within the enterprise dedicated to BYOD devices.[14] This BYOD network should be external (e.g., off the organization's DMZ) and not grant any more access to enterprise resources than users already have through remote access. Organizations considering permitting BYOD devices within the enterprise should strongly consider establishing a separate, external, dedicated network for BYOD use within enterprise facilities. This network should be secured and monitored in a manner consistent with how remote access segments are secured and monitored.

The risks of BYOD and third-party-controlled client devices specifically are quite similar to those of general telework and remote access. However, there are a few important distinctions:

- Malicious traffic generated by a BYOD or third-party-controlled client device on an enterprise network may appear to external parties to be generated by the organization itself. This could affect the organization's reputation.
- BYOD and/or third-party-controlled devices may attack each other over the dedicated network.

2.4 Summary of Key Recommendations

The following list presents some of the key recommendations from this section of the document.

- To support confidentiality, integrity, and availability, all of the components of telework and remote access solutions, including client devices, remote access servers, and internal servers accessed through remote access, should be secured against a variety of threats. (Section 2.1)
- Before designing and deploying telework and remote access solutions, organizations should develop system threat models for the remote access servers and the resources that are accessed through remote access. (Section 2.1)
- When planning telework security policies and controls, organizations should assume that client devices will be acquired by malicious parties who will either attempt to recover sensitive data from the devices or leverage the devices to gain access to the enterprise network. (Section 2.1)

[14] A similar network can be set up for third-party-controlled devices if desired, or the same network used for both BYOD and third-party-controlled devices. However, often this is not necessary because there are already contractual agreements and technical checks in place to ensure that these devices are secured in accordance with the organization's policies.

- Organizations should plan their remote access security on the assumption that the networks between the telework client device and the organization cannot be trusted. (Section 2.1)
- Organizations should assume that client devices will become infected with malware and plan their security controls accordingly. (Section 2.1)
- Organizations should carefully consider the balance between the benefits of providing remote access to additional resources and the potential impact of a compromise of those resources. Organizations should ensure that any internal resources they choose to make 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. (Section 2.1)
- When planning a remote access solution, organizations should carefully consider the security implications of the remote access methods in each of the four categories described in Section 2.2, in addition to how well each method may meet operational requirements. (Section 2.2)
- 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. (Section 2.3)

3. 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.

3.1 Remote Access Server Security

The security of remote access servers, such as VPN gateways and portal servers, is particularly important because they provide a way for external hosts to gain access to internal resources, as well as a secured, isolated telework environment for organization-issued, third-party-controlled, and BYOD client devices. In addition to permitting unauthorized access to enterprise resources and telework client devices, a compromised server could be used to eavesdrop on communications and manipulate them, as well as a "jumping off" point for attacking other hosts within the organization. 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 managed only from trusted hosts by authorized administrators.

VPN gateways and portals can run many services and applications, such as firewalls, antimalware software, and intrusion detection software. Organizations should carefully consider the security of any solutions that involve running a remote access server on the same host as other services and applications. Such solutions may offer benefits, such as equipment cost savings, but a compromise of any one of the services or applications could permit an attacker to compromise the entire remote access server. Placing the remote access server on a separate, dedicated host reduces the likelihood of a remote access server compromise and limits its potential impact. Using a separate host may also be advisable if the remote access server is likely to place other services and applications at significantly increased risk. An organization should also consider using multiple remote access solutions if its remote access users have vastly different security needs, such as one group accessing typical low-risk resources and another group accessing mission-critical confidential data.

The security of stored data is another important consideration for remote access server security. For portal servers that may temporarily store sensitive user data, wiping such data from the server as soon as it is no longer needed can reduce the potential impact of a compromise of the server. The need to wipe sensitive data from remote access servers should be determined based on a risk assessment.

3.2 Remote Access Server Placement

Major factors organizations should consider when determining where to place a remote access server include the following:

- **Device Performance.** Remote access services can be computationally intensive, primarily because of encryption and decryption. Providing remote access services from a device that also provides other services may put too high of a load on the server during peak usage, causing service disruptions. The performance impact caused by encryption and key exchange can be reduced by performing them on hardware-based cryptographic accelerator chips. These chips can be located on computer motherboards or add-on cards.

- **Traffic Examination.** Because the contents of encrypted remote access communications cannot be examined by network firewalls, intrusion detection systems, and other network security devices, it is generally recommended that the remote access architecture be designed so that an unencrypted form of the communications can be examined by the appropriate network and/or host-based security controls.

- **Traffic Not Protected by the Remote Access Solution.** Organizations should carefully consider the threats against network traffic not protected by the remote access solution, such as traffic passed between a remote access server and internal resources.
- **NAT.** The use of NAT can cause operational problems for some remote access solutions. For example, any remote access system that requires the teleworker to connect directly to a host inside the network, such as a remote desktop system or a VPN with its public endpoint inside the network, cannot work with a NAT without special configuration that may or may not work. NATs also prevent the use of applications that require addresses not to change (e.g., embed addresses in the application content). Protocols and mechanisms that break through NATs to solve particular access problems often introduce their own security problems, such as possibly allowing access to different hosts inside the NAT at different times. Some newer NAT technologies, particularly those involving IPv6, are not yet well understood and their security properties not yet fully analyzed.

Organizations should carefully consider the placement of their remote access servers. Some remote access servers, such as VPN gateways, generally act as intermediaries between telework devices and the organization’s internal computing resources. Other hosts providing remote access services, such as direct application access and remote desktop access solutions, are true endpoints for remote access communications. Both categories of remote access servers are discussed below.

Remote access servers are usually placed at an organization's network perimeter. Such placement is common because the organizational security policies most often apply to the entire network of an organization. Even if a particular security policy applies to one sub-network of the organization, most remote access servers can restrict access to sub-networks and therefore can be placed at the organization's perimeter. In some network layouts, it is better to put a remote access server inside the perimeter, at the boundary of a sub-network. The rest of this section describes when such a network layout might be appropriate.

3.2.1 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. If remote access is needed to a particular sub-network within the organization, there are generally two options: 1) place the remote access server at the edge of the sub-network, where the sub-network joins the full network; or 2) place it at the perimeter of the full network and use additional mechanisms to restrict the teleworkers to only be able to access the specified sub-network. The value of placing the remote access server at the network perimeter versus the sub-network perimeter differs for the four types of remote access methods:

- Tunneling servers usually give administrators sufficient control over the internal resources to which a teleworker has access, such that there is little advantage to setting up a tunneling server at the edge of a sub-network, as opposed to the network perimeter.
- Portal servers run the application client software on the servers themselves. Placing them at the network perimeter has a similar effect as placing them at the edge of a sub-network because the remote access user is only running applications on the portal server, not on servers inside the network.
- Remote desktop access does not involve remote access servers, so there is no issue with the placement of the remote access server.

- Direct application access servers run the application server software on the servers themselves. Placing them at the network perimeter has a similar effect as placing them at the edge of a sub-network because the remote access user is only running applications on the direct application access server, not on servers inside the network.

Thus, the only types of remote access servers that may be appropriate to place at the sub-network perimeter are portal servers and direct application access servers, but even in those two cases, it is often better to run those on the organization's perimeter so that the organization's firewall can control access to these servers for all workers, not just teleworkers. Further, to simplify management of the network and the network's security policy, running all remote access servers at the network perimeter is also advisable. Therefore, organizations should place remote access servers at the network perimeter instead of the sub-network perimeter unless there are compelling reasons to do otherwise.

If a network has a firewall at the perimeter, remote access servers on that network should be directly connected to, or in the same physical device as, the firewall so as to not circumvent the firewall's security policy. In the case that the two devices are the same, there is of course no question about the placement of the remote access server. However, if the remote access server is a different device than the firewall, the network planner must decide where to place the remote access server. If the firewall has a DMZ associated with it, then that DMZ is likely the best location for the remote access server, otherwise the server should be outside the firewall if the network topology allows for it. Both of these placements provide logical separation between the remote access server and the internal networks. To reduce the potential impact of a compromise of the remote access server, organizations should restrict communications between the server and internal networks. The server should only be able to initiate communications with the internal hosts and services specifically authorized for remote access usage, and only the appropriate internal hosts (e.g., trusted hosts used to administer the remote access server) should be able to initiate communications with the remote access server.

If the remote access server must be placed inside the firewall, the firewall's security policy should be adjusted to allow only the necessary traffic from teleworkers (and only teleworkers) to get to the remote access server. This could, for example, involve limiting incoming traffic to only the IP addresses or address ranges used by contractors, business partners, and vendors' networks and used by employees' home networks if those networks have stable addresses. Setting up such a precise policy for mobile telework client devices can be difficult to maintain and error-prone. Also, because all remote access communications should be encrypted, as discussed in Section 4, network security controls would be unable to monitor the contents of the communications. Therefore, this solution should be avoided.

3.2.2 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 discussed in Section 2.2.3 involved in allowing external traffic to pass directly into the internal network. Implementations of remote desktop access solutions usually rely on internal workstations to provide remote access services, so the use of such solutions is not generally recommended.

3.3 Remote Access Authentication, Authorization, and Access Control

Most of the computing resources used through remote access are available only to an organization's users, and often only a subset of those users. 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. Authentication can also be used to confirm the legitimacy of telework client devices and remote access servers. Access control technologies are also needed to restrict access to network communications and applications. This section provides additional details on remote access authentication, authorization, and access control.

3.3.1 Authentication

There are many ways to authenticate remote access users, such as with passwords[15], digital certificates, or hardware authentication tokens. If passwords are the only form of authentication for a remote access solution, then generally the remote access solution's authentication mechanism should be different from the organization's other authentication mechanisms, such as email or directory service passwords, unless direct application access is being used. Having different passwords reduces the impact that a compromise of remote access credentials would have on other information resources, and vice versa, and it is particularly important if users are entering passwords into telework devices not controlled by the organization. However, having different passwords for remote access and other systems is often not enforceable[16], and it should be assumed that some users will use the same passwords for both. 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.

Federal agencies are required to "allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access", according to OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.[17] Such two-factor authentication currently tends to be implemented through the use of a cryptographic token and a password, because other authentication methods are often not available on telework client devices. For example, most mobile devices do not have biometric capabilities, smart card readers, or other additional authentication capabilities.[18] This is particularly true for client devices not issued by the organization.

Many organizations require teleworkers to re-authenticate 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. OMB M-07-16 requires federal agencies to "use a 'time-out' function for remote access and mobile devices requiring user re-authentication after thirty minutes of inactivity".[19] Remote access servers vary in their support for authentication methods and session timeouts, so additional mechanisms may be needed to implement and enforce these policies. Additional information on the types of user authentication methods appropriate for remote access can be found in NIST SP 800-63, *Electronic Authentication Guideline*[20] and OMB M-04-04, *E-Authentication Guidance for Federal Agencies*.[21]

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. An example is verifying a digital certificate presented by the remote access server to ensure that the server is

[15] For more information and recommendations specific to passwords, see draft NIST SP 800-118, *Guide to Enterprise Password Management* (http://csrc.nist.gov/publications/PubsSPs.html#800-118).

[16] In some cases, it can be enforced by using a centralized password management system for both the remote access passwords and the other systems' passwords. Many centralized password management systems can ensure that the same password is not used for two different systems.

[17] http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf

[18] One possibility for an organization is to leverage derived Personal Identity Verification (PIV) credentials. For more information, see NIST SP 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials* (http://dx.doi.org/10.6028/NIST.SP.800-157).

[19] NIST SP 800-53 also has a security control for this, Access Control 11 (AC-11), Session Lock.

[20] http://dx.doi.org/10.6028/NIST.SP.800-63-2

[21] http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

controlled by the organization. User digital certificates can be used in many remote access systems, although the systems vary in the way that they handle certificates. Most user digital certificates have the private key associated with the certificate protected by a password. Some remote access methods, such as IPsec and SSL VPN technologies, include mandatory server authentication during the setup of the secure communications channel. Server authentication is most important for remote access methods where a user is manually establishing the remote access connection, such as typing a URL into a web browser. Section 3.4 presents additional information on this.

3.3.2 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. These health checks usually require software on the user's device that is controlled by the remote access server to verify compliance with certain requirements from the organization's secure configuration baseline, such as the user's antimalware software being up-to-date, the operating system being fully patched, and the user's device being owned and controlled by the organization. Fewer health checks are generally available on mobile devices, but an important check usually provided is to determine if a mobile device has been rooted or jailbroken, which can have serious negative security implications.

Some remote access solutions can also determine if the device has been secured by the organization and what type of device it is (e.g., desktop/laptop, smartphone, tablet). Based on the results of these checks, the organization can determine whether the device should be permitted to use remote access and what level of access should be granted. If the user has acceptable authorization credentials but the client device does not pass the health check, the user and device may be granted limited access to the internal network, no network access at all, or access to a quarantine network so that the security deficiencies can be fixed. This decision can also be based on the part of the network that the device is trying to access; an organization might have more stringent policies for more sensitive data. Some organizations also issue digital certificates to the client devices so that the devices themselves can be authenticated as part of the checks.

Authorization based on the type of device that is used and the device's properties is referred to as network access control (NAC). NAC is a security policy enforcement mechanism, not a true security protection mechanism. Examples of NAC checks include verifying the presence of security patches, confirming that antimalware software is enabled and up-to-date, ensuring that a personal firewall is enabled and blocking incoming traffic, and performing device authentication. However, many health checks are performed in ways that can be trivially circumvented by malware, so organizations should not rely on NAC to stop determined attackers from gaining network access. Organizations should use NAC whenever feasible to detect major security policy violations in telework client devices and to prevent teleworkers from inadvertently using the wrong device for telework. Some NAC solutions can also be used to control which internal resources each client device may access and whether remediation actions have to be performed on a client device before it is permitted access.

3.3.3 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.[22] It is important to note that for a remote access system to be considered compliant to FIPS 140, both sides of the interaction must have passed FIPS 140 validation. Many remote access systems, such as SSL VPNs, support the use of remote access client software from other vendors, so there may be two or more distinct validation certificates for a particular remote access system.

Some remote access methods, such as IPsec and SSL VPNs, often inherently include NIST-approved mechanisms for encrypting communications and verifying their integrity. Other remote access methods may use other NIST-approved cryptographic mechanisms to provide protection. Remote access methods that do not offer NIST-approved mechanisms for protecting the confidentiality and integrity of communications should have additional NIST-approved protection applied, such as tunneling the remote access method's communications within a VPN or running the communications over TLS. Remote access methods that offer both NIST-approved and non-NIST-approved cryptographic mechanisms should disable the use of all non-approved cryptographic mechanisms if possible. This is usually achieved through configuration of the remote access server.

Access control for network communications may also involve determining which traffic should be protected. Some remote access solutions offer options for this; for example, many VPN clients have a feature called *split tunneling* which, if enabled, will tunnel all communications involving the organization's internal resources through the VPN, thus protecting them, but will exclude all other communications from going through the tunnel. Split tunneling increases efficiency for communications and reduces load on the remote access solution, but it also prevents the organization from examining much of the teleworkers' network traffic and from protecting the confidentiality and integrity of that traffic. Further, using split tunneling could result in a telework device that has two active Internet interfaces—for example, a PC connected to Ethernet and a wireless network simultaneously—inadvertently becoming a bridge between a trusted and an untrusted network. This presents a significant security risk and is a violation of most organizations' security policies. For teleworkers using VPNs on untrusted networks, particularly higher-risk networks such as wireless hotspots, organizations should consider disabling split tunneling capabilities so that attackers cannot eavesdrop on any of the teleworkers' network communications.

For their teleworkers' home networks or their contractors, business partners, and vendors' networks, some organizations provide VPN gateways, firewall appliances, or other security devices that are configured to enforce the organization's security policies. This gives organizations greater control over telework security but may also involve significant costs in purchasing, deploying, managing, and maintaining the security devices. Also, because most networks used for telework are also used for other purposes, the security policies could interfere with other use of the network if not designed properly. Another drawback is that the security devices, if stolen by or otherwise acquired by an attacker, could grant an attacker easy access to the organization's systems if the organization's remote access solution authenticates the security device only and not the remote access user. Therefore, when such security devices are used, both the device and the user should be authenticated by the organization.

3.3.4 Access Control for Applications

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. Similarly, direct application

[22] The current version of FIPS 140 is 140-2, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

access limits the teleworker to a specific application on a single server. Remote desktop access can only provide access control to applications by combining its policies with the access control restrictions that are in place on the internal workstations.

Putting limits on which applications teleworkers can access does not necessarily prevent teleworkers from affecting other resources, because the applications being run may have access to other network resources. For example, a web server that the teleworker accesses may cause lookups on database servers, data retrieval from file servers, and other actions involving additional servers. Thus, the policy of limiting a teleworker to particular applications should be considered in light of what other applications and hosts those applications can interact with.

3.4 Remote Access Client Software Security

Another important element of remote access solution security is the security configuration of remote access client software. Many remote access clients have security features and settings that can be remotely managed by a system administrator. Such management is particularly important for client software that has complex security settings. For example, many users have difficulty with manually setting IPsec configurations or authentication options for remote desktop access. If the client has remote management capabilities, an administrator can view its configuration, reconfigure it, and possibly lock the configuration. Locking ensures that security settings are not inadvertently or intentionally altered, which could reduce remote access security. However, there is no standardization for remote management capabilities or interfaces, and many remote access systems do not have remote management features for their client software.

Organizations should carefully plan how remote access client software security will be maintained and managed before selecting and deploying a remote access solution. More broadly, organizations should also plan how the telework client devices that they provide to teleworkers will be managed and supported, such as a help desk agent remotely accessing a device to perform troubleshooting of operational problems reported by a teleworker. If not properly secured, remote management capabilities can be misused by attackers to compromise telework client devices and use them to gain access to an organization’s internal resources. Therefore, organizations should ensure that remote management is properly secured, particularly encrypting network communications and performing mutual authentication of endpoints.

Organizations should also consider the “thickness” of remote access client software. A remote access client is considered *thick* if it is configured so that the organization has nearly complete control over the remote access environment. For example, many VPN clients can be configured to be very thick, such as tunneling all network communications from the client device to the organization’s network, using the organization’s Domain Name System (DNS) services instead of the local network’s DNS services, and hard-coding the IP address of the VPN gateway instead of relying on local name resolution of the DNS server’s name.

However, many VPN clients can also be configured to be *thin*, which means that the client uses a common application already present on the telework device, such as a web browser. With a thin VPN client, the organization has considerably less control over the remote access environment as compared to a thick client. A thin VPN client might rely on local network services and permit communications not involving the organization’s internal resources to be passed unprotected across public networks. Some types of remote access solutions, such as portals, remote desktop access, and direct application access, have inherently thin remote access clients.

Thin remote access clients are generally more flexible and efficient than thick clients, but they also cause a greater risk of error and compromise—for example, a user could mistype a portal server’s URL in a web browser and reach a fraudulent website. Thick clients help ensure that clients are communicating with legitimate remote access servers and other resources. 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.

3.5 Summary of Key Recommendations

The following list presents some of the key recommendations from this section of the document.

- 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. (Section 3.1)

- 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. (Section 3.1)

- 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. (Section 3.2)

- 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. (Section 3.3)

- 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. (Section 3.3)

- Organizations should carefully plan how remote access client software security will be maintained and managed before selecting and deploying a remote access solution. Organizations should also plan how the telework client devices that they provide to teleworkers will be managed and supported. Organizations should ensure that remote management is properly secured, particularly encrypting network communications and performing mutual authentication of endpoints. (Section 3.4)

- 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. (Section 3.4)

4. Telework Client Device Security

Telework client devices can be divided into two general categories:

- **Personal computers (PC),** which are desktop and laptop computers. PCs run desktop/laptop operating systems such as Windows, Mac OS X, and Linux. PCs can be used for any of the remote access methods described in this section.
- **Mobile devices,** which are small mobile computers such as smartphones and tablets. Mobile devices are most often used for remote access methods that use web browsers, primarily SSL VPNs and individual web application access.

The difference between PCs and mobile devices is decreasing. Mobile devices are offering more functionality previously provided only by PCs. Still, the security controls available for PCs and mobile devices are significantly different as of this writing, so the rest of this publication provides separate recommendations for PCs and mobile devices, where applicable.

Another set of categories used in the recommendations is the party that is responsible for the security of the client device. These categories are as follows:

- **Organization.** Client devices in this category are usually acquired, configured, and managed by the organization. These devices can be used for any of the organization’s remote access methods.
- **Third-Party-Controlled.** These client devices are controlled by the teleworker’s employer, such as a contractor, business partner, or vendor. This third party is ultimately responsible for securing the client devices and maintaining their security, as documented in contracts between the organization and the third party. These devices can usually be used for many or all of the organization’s remote access methods.
- **BYOD.** These client devices are controlled by the teleworker, who is fully responsible for securing them and maintaining their security. These devices can usually be used for many or all of the organization’s remote access methods.
- **Unknown.** Labeled as “unknown” because there are no assurances regarding their security, these client devices are owned and controlled by other parties, such as kiosk computers at hotels, and PCs or mobile devices owned by friends and family. Remote access options for these devices are typically quite limited because users cannot or should not install software onto them, and their use is extremely risky because of the unknown nature of their security posture.

In today’s computing environment, there are many threats to telework client devices. These threats are posed by people with many different motivations, including causing mischief and disruption, stealing intellectual property, and committing identity theft and other forms of fraud. The primary threat against most telework client devices is malware, including viruses, worms, malicious mobile code, Trojan horses, rootkits, spyware, and bots.[23] Malware threats can infect client devices through many means, including email, websites, file downloads and file sharing, peer-to-peer software, instant messaging, and social media. The use of unauthorized removable media or devices, such as flash drives, is a common transmission mechanism for malware. Another common threat against telework client devices is loss or theft of the device. Someone with physical access to a device has many options for attempting to view or copy the information stored on it. An attacker with physical access can also add malware to a device that

[23] For more information on malware, see 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).

gives them access to data accessed from or entered into the device, such as users' passwords typed into a laptop keyboard.

Permitting teleworkers to remotely access an organization's computing resources or to have local access to the organization's networks gives attackers additional opportunities to breach the organization's security. When a client device uses remote access or has local network access, it is essentially an extension of the organization's own network. If the device is not secured properly, it poses additional risk not only to the information that the teleworker accesses, but also to the organization's other systems and networks. Therefore, 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—OS and application security updates applied promptly, unneeded services disabled, etc. 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. For example, storing sensitive data on a desktop computer housed at an organization's headquarters has different ramifications than storing the same data on a laptop used at several external locations. This section discusses recommendations for securing telework client devices and the data that they contain.

If the use of additional security controls installed on telework devices is not feasible or enforceable, other approaches may be better, such as providing a secure local environment for telework through use of VDI or VMI technologies, giving teleworkers removable media that they can use to boot their telework PC into a secure remote access and telework environment, or adopting mobile device management (MDM) and mobile application management (MAM) solutions for enhancing and enforcing mobile device security.

Organizations should be responsible for securing their own telework client devices and should also require their users or users' organizations to implement and maintain appropriate, often similar, levels of security for the non-organization-issued client devices that they use for telework. The mechanisms for securing organization-owned and other telework client devices are similar, but some of the security controls might not be feasible for teleworkers to implement on their own. See NIST SP 800-114 Revision 1, *User's Guide to Telework and Bring Your Own Device (BYOD) Security*, for recommendations for users securing BYOD telework client devices. Section 5 contains additional discussion of the feasibility of relying on users to establish and maintain the security of devices.

4.1 Securing Telework PCs

One of the most important security measures for a telework PC is having a properly configured personal firewall installed and enabled. Personal firewalls are needed to stop network-based threats in many environments. If a personal firewall has a single policy for all environments, then it is likely to be too restrictive at times, such as when on the organization's internal network, and not restrictive enough at other times, such as when on a third-party external wireless network. So 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.[24]

Many firewalls require the user to manually select the appropriate policy or environment from a list, but some personal firewalls can be configured to "auto-sense" the network they are on and choose a security

[24] For more information on personal firewalls, see NIST SP 800-41 Revision 1, *Guidelines on Firewalls and Firewall Policy* (http://dx.doi.org/10.6028/NIST.SP.800-41r1).

policy based on that information. Although auto-sensing helps to automate the security process, it may not always work correctly and could apply the wrong policy at times, making the computer insecure or blocking needed functionality. Thus, organizations that want to use auto-sensing features should test them thoroughly before relying on them, as well as educating users on how they work and how users can override them if the wrong policy has been selected. Auto-sensing features should only be used if they notify the teleworker what environment the feature thinks the user is in so that the user can override it if the auto-sensing feature has misidentified the environment.

Another important consideration for telework PCs is applying OS and application security updates.[25] For telework PCs secured by their users, this generally involves configuring the OS and applications to automatically contact the vendors' online services frequently to check for updates and download and install them. Determining how to configure other telework PCs (controlled by the organization or its contractors, business partners, vendors, etc.) to acquire updates can be significantly more complicated. An organization might wish to use a centralized patch management system for all its PCs, but if telework PCs rely on such a system, they may not receive updates promptly if they are configured to get updates only from the organization's centralized patch management system.[26] For example, a user might connect a telework PC to an external network but not establish a remote access connection to its own organization. The PC may be exposed to threats that could exploit its unpatched vulnerabilities, and patches would not be available until some time after the user established a remote access session with its own organization. Another potential problem with keeping software updated is that remote access sessions may be brief, particularly if the teleworker is on travel. This might preclude larger updates from being downloaded if the software performing the updates does not permit updates to be downloaded in pieces.

Organizations should carefully consider these issues when planning how telework PCs will be kept current with OS and application updates. Organizations should also encourage users to fully update their telework PCs before taking them on travel or to other uncontrolled environments, which are generally more likely to contain new threats than home networks.

Other security measures that are particularly important for telework include the following:

- Have a separate user account with limited privileges for each person that will use the telework PC. Teleworkers should use their limited privilege accounts for regular work and use a separate administrative account only for tasks that require administrator-level access, such as some software updates. This reduces the likelihood of an attacker gaining administrator-level access to the PC.

- Enforce *session locking*, which prevents access to the PC after it has been idle for a period of time (such as 15 minutes) or permits the user to lock a session upon demand. After a session is locked, access to the PC can only be restored through authentication. Session locking is often part of screen-saver software. This prevents an attacker within physical proximity of a PC from easily gaining access to the current session. However, it does not thwart an attacker who steals a PC or has access to it for an extended period of time; session locking can be circumvented through various techniques.

- Physically secure telework PCs by using cable locks or other deterrents to theft. This is most important for telework PCs in untrusted external environments. Also, in these environments, shut down the PC if it is going to be left unattended.

[25] Generally, the most important applications to keep up-to-date are those that are used for security (e.g., antimalware software, personal firewalls) or remote access, and those that are network-capable and frequent vectors for exploits, such as web browsers, email clients, and instant messaging clients.

[26] For more information on patch management, see NIST SP 800-40 Revision 3, *Guide to Enterprise Patch Management Technologies* (http://dx.doi.org/10.6028/NIST.SP.800-40r3).

In cases where organizations are concerned about risk from inadequate telework PC security, particularly from PCs that are not organization-controlled or are otherwise at higher risk of compromise, organizations may want to consider different security controls in addition to or instead of those described above. For example, some vendors offer solutions that provide a bootable OS on read-only removable media with pre-configured remote access client software. A user can insert this media into a PC and reboot the computer; this bypasses the PC's OS, which may be compromised, and loads the known-good OS and remote access client software from the removable media. In most cases, these solutions can be configured to prevent users from storing files on the local hard drive, saving files to removable media, and otherwise transferring information from the known-good OS to another location. Bootable OS solutions make the logical security of the telework PC much less important, although they do not prevent all compromises (for example, vulnerabilities in the removable media's OS could be exploited, or malicious code may be present in the PC's BIOS, firmware, or hardware). Another caveat with these solutions is that they require the PC to support booting the removable media before the hard drive, which may require the user to reconfigure the PC's BIOS settings.

Another option is to provide teleworkers with flash drives that are specifically configured for telework use. These drives hold organization-approved applications that are executed from a read-only portion of the drives, which protects them from unauthorized modification. Temporary files from these applications are stored in another portion of the flash drives, which reduces the likelihood of data leakage onto the PC.

4.2 Securing Telework Mobile Devices

Many telework mobile devices can have their security managed centrally through enterprise mobile device management software. Organizations should take advantage of such security management capabilities whenever available, particularly for organization-controlled devices—for example, by restricting the installation and use of third-party applications, or by providing an app store with authorized, vetted apps and only permitting apps to be downloaded and installed from that app store. However, many devices will need to be secured manually. Security capabilities and appropriate actions vary widely by device type and specific products, so organizations should provide guidance to device administrators and users who are responsible for securing telework mobile devices on how they should secure them.

NIST SP 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*,[27] recommends safeguards for the most common types of telework mobile devices. The following are examples of these safeguards:

- Limit the networking capabilities of mobile devices. This is particularly important for devices that have multiple wireless capabilities; the teleworker might not even know that some wireless protocols are exposing the device to access by attackers, such as Bluetooth and shared wireless networking. Sometimes it is necessary to allow multiple networking capabilities simultaneously, such as allowing voice/data cellular access at the same time as Wi-Fi.
- For devices that face significant malware threats, run antimalware programs. Devices that connect to the Internet may even have personal firewalls; these should be enabled to prevent attacks and unauthorized access.
- Determine if the device manufacturer provides updates and patches; if so, ensure that they are applied promptly to protect the device from attacks against known vulnerabilities.
- Strongly encrypt stored data on both built-in storage and removable media.

[27] http://dx.doi.org/10.6028/NIST.SP.800-124r1

- Require a password/passcode and/or other authentication before accessing the organization's resources.
- Restrict which applications may be installed through whitelisting or blacklisting.[28]

Given the similarity between the functions of mobile devices, particularly as they become more advanced, and PCs, organizations should strongly consider treating them similar to, or the same as, PCs. This means that organizational policies for PCs may simply be extended to mobile devices; if the two policies are kept separate, the policy documents should heavily cross-reference each other.

Organizations should consider taking advantage of mobile device management (MDM) solutions, mobile application management solutions (MAM), and other technologies for controlling the use of mobile devices. MDM solutions are capable of enforcing a variety of security policies on behalf of the organization, even to some extent on mobile devices that are not controlled by the organization. For example, MDM software is frequently used to require the use of a PIN to unlock a mobile device, to enable encryption technologies to protect sensitive data stored on a mobile device, and to determine if a mobile device has been jailbroken or rooted. MDM software can also be used to perform a remote wipe when a mobile device has been lost or stolen to prevent unauthorized access to any sensitive data it contains. An organization can set different MDM policies for each category of mobile devices, such as organization-issued, third-party-controlled, and BYOD, to take into account the differing levels of access each device may provide to the MDM solution. MAM software provides an environment that isolates the enterprise applications and data from the rest of the device. Strong authentication can be required to access the enterprise environment, which is also encrypted to protect the organization's sensitive data and applications, and to minimize data leakage from those applications to other applications and services running on the device. In the event the device is lost or the employee leaves the organization, the protected environment can be remotely wiped to remove the enterprise data.

In addition to or instead of MDM/MAM solutions, organizations may rely on NAC solutions, as discussed in Sections 2 and 3 of this document. NAC solutions can identify jailbroken or rooted mobile devices and other major security policy violations on mobile devices attempting to connect to the organization's networks.

4.3 Protecting Data on Telework Client Devices

Telework often involves creating and editing work-related information such as email, word processing documents, and spreadsheets. Because that data is important, it should be treated like other important assets of the organization. Two things an organization can do to protect data on telework devices are to secure it on the telework device and to periodically back it up to a location controlled by the organization. More information on this is provided in Sections 4.3.1 through 4.3.3. Organizations can also choose not to allow the organization's information to be stored on telework devices, but to instead store it centrally at the organization.

Sensitive information, such as certain types of personally identifiable information (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. For example, teleworkers often forget that storing sensitive information on a CD that is carried with their device, or printing the information on a public printer, can also expose the information in ways that are not significant within a typical enterprise environment. An unauthorized release of sensitive information could damage the public's trust in an

[28] For more information on application whitelisting, see NIST SP 800-167, *Guide to Application Whitelisting* (http://dx.doi.org/10.6028/NIST.SP.800-167).

organization, jeopardize the organization's mission, or harm individuals if their personal information has been released.

4.3.1 Encrypting Data at Rest

All telework devices, regardless of their size or location, can be stolen. Some thieves may want to read the contents of the data on the device, and quite possibly use that data for criminal purposes. To prevent this, 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.[29]

There are many methods for protecting data at rest, and they mostly depend on the type of device or removable media that is being protected. Most operating systems have their own data encryption mechanisms, and there are also numerous third-party applications that provide similar capabilities.[30] Generally, when technologies such as full disk encryption are being used to protect data at rest on PCs, teleworkers should shut down their telework devices instead of placing them into sleep mode when the devices will not be used for an extended time or when the teleworker will not be with the device. This helps ensure that the data at rest and the decryption key are protected by the storage encryption technology.

4.3.2 Using Virtual Machines

If an organization has direct control over a telework device, the organization can enforce its policies for remote access, updating, etc. For other telework devices, such as BYOD PCs, the organization has a limited ability to enforce security policies. A method for controlling the environment in which a teleworker operates is to run a virtual machine (VM) on the telework PC. This is normally done by running a VM *hypervisor* program within the telework PC's operating system, but some newer telework PCs allow the installation of a hypervisor that runs in place of the PC's operating system. This is known as a *bare-metal hypervisor*. Bare-metal hypervisors are generally considered more secure than other hypervisors because there is one less major piece of software that can be attacked.[31]

A user runs a VM *image* in the virtual machine environment; this image acts just like a full computer with an operating system and application software. (Using virtual machines as telework devices is an extension of the concept of thin clients.) To use VM images to enforce telework policy, the organization distributes a VM image that is configured to be fully compliant with all relevant security policies. The teleworker runs the VM image on the telework computer. When the image needs to be updated, the organization distributes a new image to its teleworkers. Using a VM to support telework security works well as long as the telework computer itself does not have any malware that will attack the VM. For hypervisors that run within the host OS (i.e., not bare-metal hypervisors), any compromise within the host OS could affect the security of the VM and the VM image.

VM disks act just like the disks on a regular computer, so organizations should have policies for telework data that is stored in a VM image. VM images can be encrypted on the telework computer when they are not in use and only decrypted after the user provides proper authentication just before booting an image.

[29] For more information on cryptographic key usage, see NIST SP 800-57 (Parts 1-3), *Recommendation for Key Management* (http://csrc.nist.gov/publications/PubsSPs.html#800-57pt1).

[30] See NIST SP 800-111, *Guide to Storage Encryption Technologies for End User Devices*, for more information on encrypting storage on client devices and removable media.

[31] More information on hypervisors is available from NIST SP 800-125, *Guide to Security for Full Virtualization Technologies* (http://dx.doi.org/10.6028/NIST.SP.800-125).

If VM images are encrypted, an unauthorized person that gets access to the telework device will not be able to read the data stored in the VM image. Similarly, a VM image can have multiple disks within it, and some of those can be encrypted; if the teleworker stores their data on an encrypted disk within the VM, it will be just as if the data were stored on an encrypted disk directly on the telework computer.

Organizations should consider encrypting all VM images used for telework to reduce the risk of compromise. This can be accomplished through the use of full disk encryption, file encryption, or other means.[32] For high-risk situations, particularly involving access to highly sensitive information, organizations should encrypt each individual VM image used for telework and may also want to provide a second layer of protection through full disk encryption.

4.3.3 Backing Up Data on Telework Devices

Most organizations have policies for backing up data on a regular basis. Such a backup policy should cover data on telework PCs and mobile devices. However, such a policy may need different provisions for backups performed at the organization’s facilities versus external locations. If the data to be backed up contains sensitive information or needs its confidentiality protected for other reasons, there are additional security considerations if that backup is performed at an external location.

If data is being backed up remotely—from the telework device to a system at the organization—then the communications carrying that data should be encrypted and have their integrity verified. This is discussed in more detail in Section 3.3.3. If data is being backed up locally—to removable media such as CDs or flash drives, for example—the backup should be protected at least as well as the original data is. For example, if the original data is encrypted, then the data in the backup should be encrypted as well. If the original data is encrypted in a portable form, such as through virtual disk encryption or an encrypted VM image, then it may be sufficient to copy that encrypted entity onto the backup media. However, for non-portable forms of storage encryption, such as full disk encryption, the data would need to be decrypted on the telework device and then encrypted for storage on the backup media.

4.4 Summary of Key Recommendations

The following list presents some of the key recommendations from this section of the document.

- 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. (Section 4 introduction)

- 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. (Section 4.1)

- For telework mobile devices, organizations should take advantage of centralized security management capabilities whenever available. However, many devices will need to be secured

[32] NIST SP 800-111, *Guide to Storage Encryption Technologies for End User Devices*, explains these options (http://dx.doi.org/10.6028/NIST.SP.800-111).

manually. Organizations should provide guidance to device administrators and users who are responsible for securing telework mobile devices on how they should secure them. (Section 4.2)

- 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. (Section 4.3)

5. Security Considerations for the Telework and 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*.[33] 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. The phases of the life cycle are as follows:

- **Phase 1: Initiation.** This phase includes the tasks that an organization should perform before it starts to design a telework or remote access solution. These include identifying needs for telework and remote access (including possible support for BYOD devices and/or third-party-controlled devices), providing an overall vision for how telework and remote access solutions would support the mission of the organization, creating a high-level strategy for implementing telework and remote access solutions, developing a telework security policy, and specifying business and functional requirements for the solution.

- **Phase 2: Development.** In this phase, personnel specify the technical characteristics of the telework or remote access solution and related components. These include the authentication methods; the cryptographic mechanisms used to protect communications; and firewalls and other mechanisms used to control access to networks and resources on those networks. The types of telework clients to be used should also be considered, since they can affect the desired policies. Care should be taken to ensure that the telework security policy can be employed and enforced by all clients. At the end of this phase, solution components are procured.

- **Phase 3: Implementation.** In this phase, equipment is configured to meet operational and security requirements, including the telework security policy documented in the system security plan, installed and tested as a prototype, and then activated on a production network. Implementation includes altering the configuration of other security controls and technologies, such as security event logging, network management, and authentication server integration.

- **Phase 4: Operations and Maintenance.** This phase includes security-related tasks that an organization should perform on an ongoing basis once the telework or remote access solution is operational, including log review, attack detection, and incident response and recovery. These tasks should be documented in the configuration management policy.

- **Phase 5: Disposal.** This phase encompasses tasks that occur when a remote access solution or its components are being retired, including preserving information to meet legal requirements, sanitizing media, and disposing of equipment properly.[34]

This section highlights security considerations of particular interest for telework and remote access solutions. These considerations are not intended to be comprehensive, nor is there any implication that security elements not listed here are unimportant or unnecessary.

[33] http://dx.doi.org/10.6028/NIST.SP.800-64r2

[34] The life cycle information presented in this introduction is derived from Section 8 of 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).

5.1 Initiation

The initiation phase involves many preparatory actions, such as identifying current and future needs, and specifying requirements for performance, functionality, and security. A critical part of the initiation phase is the development of a telework security policy for an organization. The section lists elements that a telework security policy should contain and, where relevant, describes some of the factors that should be considered when making the decisions behind each element. A telework security policy should define which forms of remote access the organization permits, which types of telework devices (e.g., organization-controlled PCs and mobile devices, BYOD mobile devices, contractor-controlled PCs) 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.

In addition to the considerations described in this section for telework security policies, organizations should also consider how other security policies may be affected by telework. For example, an organization may require that certain types of locked-out user accounts be unlocked only in person, but this may not be viable for teleworkers who are on travel or on long-term assignments in external locations. Other security policies should be adjusted as needed to take telework into consideration.

5.1.1 Permitted Forms of Remote Access

One of the first decisions to make when creating a telework security policy is which types of remote access solutions will be permitted. Each type of solution has its strengths and weaknesses, and the usefulness of each will depend on many factors within the organization. Some of those factors include:

- Existing remote access used by the organization, such as remote control systems used by IT staff
- Software already installed on telework devices that can be used for remote access
- Capabilities available in firewalls that are already installed at the edge of the organization's network.

The policy for which types of remote access are permitted for telework should be closely tied to the organization's overall security policy. If one of the forms of remote access under consideration cannot be secured in a fashion that is required by the organization's security policy, such as using approved cryptographic algorithms to protect sensitive data, then that form of remote access should not be used by the organization. The overall security policy should take priority when creating a telework security policy.

5.1.2 Restrictions on Telework Client Devices and Remote Access Levels

A telework security policy can limit the types of client devices that teleworkers are allowed to use. For a variety of reasons, including security policies and technology limitations, organizations often limit which types of devices can be used for remote access. For example, an organization might permit only organization-controlled PCs to be used. Some organizations have tiered levels of access, such as allowing organization-controlled PCs to access many resources, BYOD PCs and third-party-controlled PCs to access a limited set of resources, and BYOD mobile devices to access only one or two resources, such as webmail. This allows an organization to limit the risk it incurs by permitting the most-controlled devices to have the most access and the least-controlled devices to have minimal access or no access at all.

Each organization should make its own risk-based decisions about what levels of remote access should be permitted from which types of devices. Factors that organizations should consider when setting telework security policy for this include the following:

- **Sensitivity of telework.** Some telework involves access to sensitive information or resources, while other telework does not. Organizations may have more restrictive requirements for telework involving sensitive information, such as permitting only organization-controlled telework devices to be used.

- **The level of confidence in security policy compliance.** Meeting many of an organization's security requirements can typically be ensured only if the organization controls the configuration of the telework devices. For non-organization-controlled devices, some requirements can be verified by automated security health checks conducted by the remote access server on devices attempting to connect, but other requirements cannot be verified by the organization by automated means. Making users aware of their responsibilities can help to improve security on BYOD telework devices, but will not result in the same degree of security policy compliance as mandatory security controls enforced on organization-controlled telework devices. Even the most conscientious users may fail to properly maintain the security of their BYOD devices at all times because of the technical complexity or effort involved or their lack of awareness of new threats. For third-party-controlled devices, the organization may be able to enforce security policy compliance through contractual provisions.

- **Cost.** Costs associated with telework devices will vary based on policy decisions. The primary direct cost is issuing telework devices and client software to teleworkers. There are also indirect costs in maintaining telework devices and in providing technical support for teleworkers. Another consideration related to cost is telework frequency and duration; an organization might justify purchasing telework devices for individuals who telework regularly (e.g., one day per week from home, frequent business travel), but not purchasing telework devices for individuals who telework only occasionally for short durations, such as quickly checking email from home a few evenings a month.

- **Telework location.** Risks will generally be lower for devices used only in the home environment or only in an enterprise environment (e.g., contractor, business partner, or vendor network) than for devices used in a variety of locations.

- **Technical limitations.** Certain types of devices may be needed for particular telework needs, such as running specialized programs locally. Also, if an organization has a single type of remote access server, and that server can only allow connections through a custom client that is installed on the telework device, then only the types of devices that can support the client are allowed.

- **Compliance with mandates and other policies.** Organizations may need to comply with telework-related requirements from mandates and other sources, such as a federal department issuing policy requirements to its member agencies. An example of a possible requirement is restrictions on performing telework in foreign countries that have strong known threats against Federal agency systems.

Although deciding which types of client devices should be permitted for remote access is ultimately up to each organization, organizations are cautioned to prohibit the use of unknown devices unless they can provide a way for teleworkers to use these devices in a secure fashion. An example is issuing removable media containing a secure bootable environment, instructing users on how to use this removable media with PCs, and configuring the remote access solution to block use of any unknown device not using this secure environment. The risks posed by using unknown devices for remote access without a secure environment are extremely high, so organizations should avoid this if at all possible.

Organizations may choose to specify additional security requirements that are tied to factors such as the sensitivity of telework. Many organizations require more stringent security controls for telework situations that are particularly high-risk. Security requirements that may be particularly helpful for such situations include the following:

- Permit high-risk telework only from organization-issued and secured telework devices.
- Require the use of multi-factor authentication for access to the telework device and to remote access solutions.
- Use storage encryption on the telework device, at a minimum to protect all sensitive information. Multiple levels of encryption may be needed. For example, full disk encryption may be needed to mitigate an attacker who gains physical access to the device; at the same time, virtual disk encryption or file/folder encryption may be needed to mitigate an attacker who gains logical access to the device (i.e., access after full disk encryption authentication has occurred and the data on the hard drive is being decrypted automatically as needed). Removable media containing telework data should also be encrypted.
- Migrate high-risk resources to servers that assume responsibility for protecting them. For example, a teleworker could connect to a terminal server that holds sensitive data that the teleworker needs to access.
- Store and access only the minimum data necessary. Some organizations issue "loaner" devices that are completely wiped before and after the high-risk telework (such as certain foreign travel) is performed. Only the data and authorized applications needed for the telework are loaded onto the loaner device. The loaner devices are used for telework only and may not be connected to the organization's internal networks. The pre-use wiping ensures that the device is clean before any telework is conducted, and the post-use wiping ensures that no telework data remains that could be accessed in the future.

In high-risk situations, organizations may also choose to reduce risk by prohibiting telework and remote access involving particular types of information, such as sensitive PII.

Table 5-1 shows an example of how access tiers could be defined. There are seven categories of client devices: government-furnished equipment (GFE) in the office, GFE in telework, BYOD in the office, BYOD in telework, contractor/business partner/vendor in the office, contractor/business partner/vendor in telework, and third-party devices (e.g., Internet café, hotel kiosk). This table lists a few examples of applications or systems and how access to them might be restricted based on device type and location. For example, access to the personnel system might be authorized only from GFE devices in the office, and prohibited for GFE devices in telework and all other types of devices, because of the sensitivity of the PII it contains. Access to email, calendaring, and other general resources might be permitted from all device types and locations other than third party devices. Note that in many cases, an organization could combine the BYOD in office and BYOD telework columns because of recommendations to secure BYOD in office as if it were telework/remote access. Also note that the rightmost column could be eliminated if the organization does not permit any access from third party devices.

Table 5-1. Example of Access Tiers

Application or System	GFE in office	GFE telework	BYOD in office	BYOD telework	Contractor, partner, vendor in office	Contractor, partner, vendor telework	Third party (Internet café, etc.)
Personnel system	Yes	No	No	No	No	No	No
Financial system	Yes	Yes	No	No	No	No	No
Email	Yes	Yes	Yes	Yes	Yes	Yes	No
Calendaring	Yes	Yes	Yes	Yes	Yes	Yes	No
Intellectual property	Yes	No	No	No	No	No	No
…							

Every year, there are many changes in telework device capabilities, the security controls available to organizations, the types of threats made to different types of devices, and so on. Therefore, 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. Organizations should also be aware of the emergence of new types of remote access solutions and of major changes to existing remote access technologies, and ensure that the organization's policies are updated accordingly as needed.

5.1.3 Additional User Requirements

Organizations often have additional security considerations for telework that, while helpful in mitigating threats, cannot be directly enforced by the organization. Organizations should educate users on the importance of these additional security measures and define teleworkers' responsibilities for implementing these measures in policy and telework agreements.

One example of a possible security consideration is phone services. Depending on the sensitivity of telework communications, telephone security may be a consideration. Corded phones using traditional wired telephone networks cannot be intercepted without physical connections, so they are sufficiently secure for typical telework. Cordless phones using traditional wired telephone networks should employ spread spectrum technology to scramble transmissions, thus reducing the risk of eavesdropping within physical proximity (usually a few hundred yards at most). Digital cell phones should be acceptable for typical telework.[35] Communications carried over voice over IP (VoIP) services should not be considered secure unless some form of encryption is used; however, many VoIP services now provide strong encryption, which should be used to protect sensitive information. Any encryption used must be certified to follow NIST requirements. The FIPS 140 specification, *Security Requirements for Cryptographic Modules*, defines how cryptographic modules are validated.

Another possible security consideration involves wireless personal area networks (WPAN), which are small-scale wireless networks that require no infrastructure to operate. Examples of WPAN technologies are using a wireless keyboard or mouse with a computer, printing wirelessly, synchronizing a smartphone with a computer, and allowing a wireless headset or earpiece to be used with a smartphone. The most commonly used type of WPAN technology is Bluetooth. For devices within proximity of threats, teleworkers should disable WPAN technologies when not in use to prevent misuse by unauthorized parties.

[35] Analog cell phone communications can be intercepted by individuals with scanning equipment, so their use should be avoided when discussing sensitive or proprietary information. However, analog cell phone networks have been retired.

Additional information on these security considerations is available from NIST SP 800-114 Revision 1, *User's Guide to Telework and Bring Your Own Device (BYOD) Security*, and NIST SP 800-121 Revision 1, *Guide to Bluetooth Security*.

5.2 Development

Once the organization has established a telework security policy, identified telework and remote access needs, and completed other preparatory activities, the next step is to determine which types of telework or remote access technologies should be used and to design a solution to deploy. There are many considerations for designing a solution, most of which are generally applicable to any IT technology; some of these are covered in Section 2.1 of this document and NIST SP 800-53. This section focuses on the technical security considerations that are most important for designing telework and remote access solutions. Major considerations include the following:[36]

- **Architecture.** Designing the architecture includes the placement of the remote access server, the selection of remote access client software (if needed), and the design of one or more organization network segments for non-organization-controlled client devices.
- **Authentication.** Authentication involves selecting a remote access authentication method, as described in Section 3, and determining how its client/user and server components should be implemented, including procedures for issuing and resetting authenticators and for provisioning users and client devices with authenticators.
- **Cryptography.** Decisions related to cryptography include selecting the algorithms for encryption and integrity protection of remote access communications, and setting the key strength for algorithms that support multiple key lengths.
- **Access Control.** This involves determining which types of remote access communications should be permitted and denied. Section 3 provides additional information on access control capabilities.
- **Endpoint Security.** Endpoint security decisions involve determining how remote access servers and telework client devices should be secured, as described in Sections 3 and 4, respectively.

The security aspects of the telework and remote access solution design should be documented in the system security plan. The organization should also consider how incidents involving the telework and remote access solutions should be handled and document those plans as well.[37]

5.3 Implementation

After the remote access solution has been designed, the next step is to implement and test a prototype of the design before putting the solution into production. Aspects of the solution that should be evaluated include the following: [38]

- **Connectivity.** Users can establish and maintain remote access connections. Users can connect to all of the resources that they are permitted to and cannot connect to any other resources.
- **Protection.** Each traffic flow is protected in accordance with the established requirements. This includes flows between the telework client device and the remote access server, and between the

[36] These considerations are based on material from Section 4 of NIST SP 800-77, *Guide to IPsec VPNs* (http://dx.doi.org/10.6028/NIST.SP.800-77).

[37] For more information on incident handling, see NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide* (http://dx.doi.org/10.6028/NIST.SP.800-61r2).

[38] These considerations are based on material from Section 4 of NIST SP 800-77, *Guide to IPsec VPNs*.

remote access server and internal resources. Protection should be verified by means such as monitoring network traffic or checking traffic logs.

- **Authentication.** Authentication is required and cannot be readily compromised or circumvented. All authentication policies are enforced. Performing robust testing of authentication is important to reduce the risk of attackers accessing protected internal resources.

- **Applications.** The remote access solution does not interfere with the use of software applications that are permitted to be used through remote access, nor does it disrupt the operation of telework client devices (for example, a VPN client conflicting with a host-based firewall).

- **Management.** Administrators can configure and manage the solution effectively and securely. This includes all components, including remote access servers, authentication services, and client software. The ease of deployment and configuration is particularly important, such as having fully automated client configuration versus administrators manually configuring each client. Another concern is the ability of users to alter remote access client settings, which could weaken remote access security. Automating configurations for devices can greatly reduce unintentional errors from users incorrectly configuring settings.

- **Logging.** The remote access solution logs security events in accordance with the organization's policies. Some remote access solutions provide more granular logging capabilities than others—for example, logging usage of individual applications versus only connections to particular hosts—so in some cases it may be necessary to rely on the resources used through remote access to perform portions of the logging that the remote access server cannot perform.

- **Performance.** The solution provides adequate performance during normal and peak usage. It is important to consider not only the performance of the primary remote access components, but also that of intermediate devices, such as routers and firewalls. Performance is particularly important when large software updates are being provided through the remote access solution to telework client devices. In many cases, the best way to test the performance under load of a prototype is to use simulated traffic generators on a live test network to mimic the actual characteristics of expected traffic as closely as possible. Testing should incorporate a variety of applications that will be used with remote access.

- **Security of the Implementation.** The remote access implementation itself may contain vulnerabilities and weaknesses that attackers could exploit. Organizations with high security needs may choose to perform extensive vulnerability assessments against the remote access components. At a minimum, all components should be updated with the latest patches and configured following sound security practices.

- **Default Settings.** Implementers should carefully review the default values for each remote access setting and alter the settings as necessary to support security requirements. Implementers should also ensure that the remote access solution does not unexpectedly "fall back" to default settings for interoperability or other reasons.

5.4 Operations and Maintenance

Operational processes that are particularly helpful for maintaining telework and remote access security, and thus should be performed regularly, include the following:[39]

[39] Portions of the information on operations and maintenance were derived from Sections 5.4 and 5.5 of NIST SP 800-92, *Guide to Computer Security Log Management* (http://dx.doi.org/10.6028/NIST.SP.800-92).

- Checking for upgrades and patches to the remote access software components, and acquiring, testing, and deploying the updates

- Ensuring that each remote access infrastructure component (servers, gateways, authentication servers, etc.) has its clock synched to a common time source so that its timestamps will match those generated by other systems

- Reconfiguring access control features as needed based on factors such as policy changes, technology changes, audit findings, and new security needs

- Detecting and documenting anomalies detected within the remote access infrastructure. Such anomalies might indicate malicious activity or deviations from policy and procedures. Anomalies should be reported to other systems' administrators as appropriate.

Organizations should also periodically perform assessments to confirm that the organization's remote access policies, processes, and procedures are being followed properly. Assessment activities may be passive, such as reviewing logs, or active, such as performing vulnerability scans and penetration testing. More information on technical assessments for telework and remote access is available from NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*.[40]

5.5 Disposal

Before a telework client device or remote access server permanently leaves an organization (such as when a leased server's lease expires or when an obsolete PC is being recycled), the organization should remove any sensitive data from the host. Data may also need to be wiped if an organization provides "loaner" devices to teleworkers, particularly for travel. The task of scrubbing all sensitive data from storage devices such as hard drives and memory cards is often surprisingly difficult because of all the places where such data resides. See NIST SP 800-88 Rev. 1, *Guidelines for Media Sanitization*,[41] for additional information and recommendations on removing data from telework and remote access devices. Note that sensitive data is often found in places other than just the user's data area; for example, software that runs under Microsoft Windows often stores possibly-sensitive data in the Windows registry. An organization should strongly consider erasing all storage devices completely.

Organizations may find it particularly challenging to address data wiping for BYOD devices. Because the devices are used for both personal and work purposes, it may be necessary to scrub the telework data without affecting the personal data. Selective data scrubbing can be performed through enterprise mobile device management software (for mobile devices) and specialized utilities. Organizations should carefully consider data scrubbing issues involving BYOD devices before authorizing BYOD use.

Organizations may also have concerns about data wiping on third-party-controlled client devices. Similar to the situation with BYOD devices, an organization may want to scrub its data from these devices without disrupting the controlling organizations' data. Selective data scrubbing by the organization may be an option, or it may be more practical to have the controlling organization do its own scrubbing for the data in question.

5.6 Summary of Key Recommendations

The following list presents some of the key recommendations from this section of the document.

[40] http://dx.doi.org/10.6028/NIST.SP.800-115

[41] http://dx.doi.org/10.6028/NIST.SP.800-88r1

- 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. (Section 5.1)
- 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. (Section 5.1)
- 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. (Section 5.1)
- Organizations should document the security aspects of the telework and remote access solution design in the system security plan. (Section 5.2)
- 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. (Section 5.3)
- 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. (Section 5.4)
- Organizations should also periodically perform assessments to confirm that the organization’s remote access policies, processes, and procedures are being followed properly. (Section 5.4)
- Before disposing of a telework client device or remote access server, the organization should remove any sensitive data from it. (Section 5.5)

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 Framework[42] 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	This is self-explanatory.
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.

[42] *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0*, NIST, February 2014. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Appendix C—Glossary

Selected terms used in the publication are defined below.

Bring Your Own Device (BYOD): A non-organization-controlled telework client device.

Client Device: A system used by a remote worker to access an organization's network and the systems on that network.

Direct Application Access: A high-level remote access architecture that allows teleworkers to access an individual application directly, without using remote access software.

Mobile Device: A small mobile computer such as a smartphone or tablet.

Personal Computer: A desktop or laptop computer.

Portal: A high-level remote access architecture that is based on a server that offers teleworkers access to one or more applications through a single centralized interface.

Remote Access: The ability for an organization's users to access its non-public computing resources from external locations other than the organization's facilities.

Remote Desktop Access: A high-level remote access architecture that gives a teleworker the ability to remotely control a particular desktop computer at the organization, most often the user's own computer at the organization's office, from a telework client device.

Session Locking: A feature that permits a user to lock a session upon demand or locks the session after it has been idle for a preset period of time.

Split Tunneling: A VPN client feature that tunnels all communications involving the organization's internal resources through the VPN, thus protecting them, and excludes all other communications from going through the tunnel.

Telecommuting: See "Telework."

Telework: 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.

Telework Client Device: A PC or mobile device used by a teleworker for performing telework.

Tunneling: A high-level remote access architecture that provides a secure tunnel between a telework client device and a tunneling server through which application traffic may pass.

Virtual Private Network (VPN): A virtual network, built on top of existing physical networks, that provides a secure communications tunnel for data and other information transmitted between networks.

Appendix D—Acronyms and Abbreviations

Selected acronyms and abbreviations used in this publication are defined below.

BYOD	Bring Your Own Device
DMZ	Demilitarized Zone
DNS	Domain Name System
DSL	Digital Subscriber Line
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over TLS
IP	Internet Protocol
IPsec	Internet Protocol Security
ISP	Internet Service Provider
IT	Information Technology
ITL	Information Technology Laboratory
MDM	Mobile Device Management
MITM	Man-in-the-Middle
MPLS	Multiprotocol Label Switching
NAC	Network Access Control
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OS	Operating System
PC	Personal Computer
PII	Personally Identifiable Information
PPP	Point-to-Point Protocol
RDP	Remote Desktop Protocol
SP	Special Publication
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
VDI	Virtual Desktop Infrastructure
VM	Virtual Machine
VMI	Virtual Mobile Infrastructure
VNC	Virtual Network Computing
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WPAN	Wireless Personal Area Network

Appendix E—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 http://csrc.nist.gov/publications/PubsSPs.html.

Telework Security Resource Sites

Site Name	URL
Home Network Security	https://www.us-cert.gov/security-publications/home-network-security
Safety & Security Center	http://www.microsoft.com/security/default.aspx
StaySafeOnline.org	http://www.staysafeonline.org/
telework.gov	http://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://www.whitehouse.gov/digitalgov/bring-your-own-device
Guide to Telework in the Federal Government	http://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
NIST SP 800-111, *Guide to Storage Encryption Technologies for End User Devices*	http://dx.doi.org/10.6028/NIST.SP.800-111
NIST SP 800-113, *Guide to SSL VPNs*	http://dx.doi.org/10.6028/NIST.SP.800-113
NIST SP 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*	http://dx.doi.org/10.6028/NIST.SP.800-114
NIST SP 800-114 Revision 1 (Draft), *User's Guide to Telework and Bring Your Own Device (BYOD) Security*	http://csrc.nist.gov/publications/PubsSPs.html#800-114r1

Document Title	URL
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 800-167, *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*	http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-27.pdf