

Mobile Technology and Telework



**Theresa Noll, Senior Telework Program Analyst
Alternative Workplace Arrangements (AWA)**

Objectives

- Proven technologies used to expand employee mobility and telework programs
- Understand mobile applications available today that best support teleworkers
- Key policy considerations for equipment, reimbursements, and program funding
- Learn recommended strategies to secure network access
- Discuss the pros and cons of using government-furnished versus employee-owned devices for the remote and mobile workforce

Alternative Workplace Arrangements (AWA)

AWA touches a broad range of policy areas, integral to a modern, well-managed workforce.

- Human Resources Management/Performance
- Information Technology
- Emergency Management / Continuity of Operations
- Facility Polices
- Green / Sustainability Initiatives
- Operating Costs

Infrastructure Supports Remote Access

- **Key components**
 - * **Help Desk Support**
 - * **Thin Client**
 - * **Firewall**
 - * **Security Software (e.g., virus scan)**
 - * **Password Policies**
 - * **Internet Applications**
 - * **Secure Remote Access with 'tunneling' (e.g. VPN, SSL)**

NIST Guide to Enterprise Telework and Remote Access (NIST SP 800-46 Revision 1, June 2009)

Guidance:

- define forms of remote access permitted
- define types of telework devices permitted for each form of remote access
- define type of access each type of teleworker is granted
- define administration and policies for updating remote access servers

NIST SP 800-46 Rev.1 (continued)

Tiered Levels of Remote Access

- **Allow GFE personal computers (PC) to access many resources**
- **Allow employee-owned PCs to access a limited set of resources**
- **Allow PCs and types of devices (e.g., cell phones, personal digital assistants [PDA]) to access only one or two lower-risk resources, such as Web-based email.**

NIST SP 800-46 Rev.1 (continued)

- **High-risk Telework**
 - **Permit only GFE and secure telework client devices using multi-factor authentication and storage encryption**
 - **Ensure that remote access servers are kept fully patched and that they can only be managed from trusted hosts by authorized administrators**

Telework Client Devices

- **Ensure telework client devices are secured, including PCs, cell phones, and PDAs (see NIST SP 800-114, Nov 2007, *Guide to Securing External Devices for Telework and Remote Access*)**
- **PCs may require additional physical security (for example, using cable locks to deter theft)**
- **Telework client devices vary widely and agencies should provide guidance to device administrators and users on how they should secure them.**
- **Examples include protecting the physical security of telework devices, encrypting files stored on devices, and ensuring that information stored on devices is backed up.**

Network Integrity, Availability, and Access

- Air Cards versus Hot Spots
- 1 Laptop Model w/Roller Carry Case
- Encryption
 - Cryptography is used to protect data flowing between the telework client device and the agency, 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.

Data Encryption

- Ensure that all data sent to the teleworker through remote access is covered by the agency's data distribution and data retention policies.
- Application client software and data at rest reside on the client device, so they are not protected by the tunneling solution and should be protected by other means (see NIST SP 800-111, Nov 2007, *Guide to Storage Encryption Technologies for End User Devices*)

Best Practices

- Annual Security and Privacy Training
- GFE and Personally Owned Computer
- Reimbursements (e.g., broadband use for telework at home)
- Program Funding - cost study recommends Telework be included in the Agency's Capital Planning and Investment Control (CPIC) Process

Alternative Workplace Arrangements (AWA)

Challenges to AWA are not technical, but relate to:

- **Management resistance to change**
- **Lack of firm, clear, and continuing top level support**
- **A cost effective strategy for secure, available technology infrastructure**

References

- <http://www.gsa.gov/telework>
- <http://www.gsa.gov/teleworklibrary>
- <http://www.gsa.gov/teleworkcenter>
- <http://www.csrc.nist.gov>
- <http://www.telework.gov>
- <http://www.apps.gov>

Contact Information

Theresa Noll

General Services Administration (GSA)

Office of Governmentwide Policy

Office of Real Property, AWA Team

Washington, DC

(202) 219-1443

Theresa.Noll@GSA.GOV

www.gsa.gov/teleworknow