Security Checklist for Teleworkers

Anti-virus Software

Anti-virus application is installed and is configured to do the following:

- Start with the boot of the operating system.
- Run in the background and automatically scan all incoming files.
- Enable web browser protection, if available.
- Automatically update the virus signature database weekly.
- Schedule it to be run at least weekly to scan all hard drive files.
- Attempt to recognize unknown viruses, if available.

Spyware Removal Tools

Install and run a spyware removal tool to identify and eliminate (as appropriate) spyware. On a monthly basis, update and run spyware removal tool, again eliminate discovered spyware if appropriate.

Firewall

A firewall is an application that is employed to monitor and limit dangerous packets from entering a network, providing the capability to:

- Log all suspicious traffic (this is generally true for default installs).
- Examine log on a periodic basis.
- Block traffic to ports that support services that should not be accessible from the Internet (e.g., NetBIOS, Telnet, etc.).
- Automatically lock out network access to the host when network connectivity is not required (e.g., when the screensaver activates or computer is inactive for a fixed period of time).
- Notify the user when an application attempts to make an outbound connection..
- Set to medium to high level of security (e.g., "paranoia level").

Encryption Software

Ensure that appropriate encryption software is being used.

Securing the Operating System

- Secure or disable file and printer sharing.
- Ensure that the latest operating system patches are installed.
- Use a password-protected screensaver to lock it during periods of inactivity.
- Where appropriate use a BIOS password to restrict personal able to start system.
- Turn your system off when it is not being used.

Securing Wireless Networks

- Place wireless base station away from outside walls in order to minimize transmission of data outside of building.
- Use additional encryption beyond WEP (VPN, PGP, and so on).
- Enable 128-bit WEP encryption.
- Change SSID to a hard-to-guess password.
- Enable additional authentication schemes supported by your wireless base station.
- Disable broadcasts of SSID in the wireless base station beacon message.

Security Checklist for Teleworkers

- Disable SNMP or change the SNMP community strings to a hard-to-guess password.
- Install personal firewall on all wireless clients.

Online Security Assessment

Ensure that an online security assessment has scanned the current configuration (including the firewall) and that all major vulnerabilities identified by the assessment have been corrected and confirmed by a rescan.

Securing Web Browsers

Browser(s) configured to limit or disable plug-ins. Browser(s) configured to limit ActiveX, Java, and JavaScript.

Source: U.S. Commerce Department