U.S. OFFICE OF PERSONNEL MANAGEMENT

OFFICE OF THE CHIEF INFORMATION OFFICER

NETWORK MANAGEMENT
INFORMATION SYSTEM SECURITY CONTROLS

AC-18: Wireless Access

Version 1.2

Prepared for:

U.S. Office of Personnel Management
Theodore Roosevelt Building
1900 E Street NW
Washington, DC 20415

Prepared by:

Office of the Chief Information Officer

Theodore Roosevelt Building
1900 E Street NW
Washington, DC 20415

December 2010

Table of Contents

REVISION HISTORY

Release No.	Date	Revision Description
V1.0	October 29, 2010	Initial Issue
V1.1	December 1, 2010	Updated Control Implementation Procedures and updated Appendix A
V1.2	December 20, 2010	Updated Control Implementation Procedures and updated Appendix A

1.0 SCOPE

This document describes the policy and procedures necessary to comply with the Wireless Access information security controls (Access Control-18) recommended by National Institute of Standards and Technology (NIST) Special Publication 800-53 and required by the Federal Information Security Management Act (FISMA).

This policy covers all electronic devices with wireless data communication capabilities (i.e.: personal computers and laptops, thin clients, audio/video devices, wireless access points, etc.) connected to any of OPM's networks and resources. Excluded from this policy are wireless handheld devices such as smartphones. Additional guidance for wireless handheld devices can be found in the *OPM Policy on BlackBerry Devices and Personal Digital Assistants.*

2.0 ROLES AND RESPONSIBILITIES

OPM's Information Security and Privacy Policy can be found on OPM's internal web site: http://theo.opm.gov/policies/ispp/isp_policy1.pdf and it contains the overall roles and responsibilities for information security at OPM. This section summarizes the key roles and responsibilities applicable to Wireless Access at OPM.

2.1 OPM Chief Information Officer (CIO) has overall responsibility for OPM's Information Security Program.

2.2 OPM Chief Information Security Officer (CISO) is responsible for providing and tracking security awareness training for the agency to include wireless access usage restrictions and implementation guidance.

2.3 Network Management (NM) Director is responsible for developing appropriate usage restrictions and implementation guidance, monitoring for unauthorized access, authorizing appropriate wireless access, and enforcing this policy.

2.4 NM Security Branch Chief is responsible for updating these policies and procedures, and for validating compliance with federal information security requirements.

3.0 POLICY (SECURITY CONTROL REQUIREMENTS)

Pursuant to FISMA, there are four specific security control requirements for Wireless Access:

3.1 Establish usage restrictions and implementation guidance for wireless access;

3.2 Monitor for unauthorized wireless access to the information system;

3.3 Authorize wireless access to the information system prior to connection; and

3.4 Enforce requirements for wireless connections to the information system.

4.0 PROCEDURES

These procedures describe the actions necessary to satisfy OPM's security control requirements for wireless access:

4.1 Usage Restrictions and Implementation Guidance - NM has developed a separate document entitled "OPM Wireless Access Usage Restrictions and Implementation Guidance" which contains the applicable guidance necessary to satisfy this control. (See Appendix A, attached)

4.2 Wireless Access Monitoring - NM checks for unauthorized wireless access to the Local and Wide Area Networks (LAN/WAN) by monitoring all Virtual Private Network (VPN) traffic from remote devices. Suspicious activities from VPN connections are investigated to validate risks and perform remedial actions as necessary.

4.3 Two Factor Authentication - NM authorizes wireless access via two-factor authentication to OPM's VPN. All external OPM wireless access is technically forced to authenticate to OPM's VPN prior to establishing connectivity to the network.

4.4 Access Control Enforcement - Enforcement of OPM's wireless access controls is technically accomplished with FIPS 140-2 approved VPN authentication and through continuous monitoring and ongoing assessments of existing and planned controls.

5.0 COMPLIANCE WITH APPLICABLE REGULATIONS

This policy has been developed to meet or exceed all guidance detailed in *National Institute of Standards and Technology (NIST) Special Publication 800-53 rev 3: Recommended Security Controls for Federal Information System;, NIST Special Publication 800-48 Rev. 1: Guide to Securing Legacy IEEE 802.11 Wireless Network; and NIST Special Publication 800-97 Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, NIST Special Publication 800-121: Guide to Bluetooth Security.*

6.0 EFFECTIVE DATE

This policy is effective January 1, 2011.

APPENDIX A: OPM Wireless Access Usage Restrictions and Implementation Guidance Agreement

1.0 PURPOSE

OPM's Chief Information Officer (CIO) approves the use of wireless connectivity on OPM laptops and mobile devices. Wireless connections are typically made through:

- Wireless gateways on OPM premises (called access points, or APs).
- External hosts via remote access technology (for example, using a wireless router at home to connect to OPM network and server resources).
- Third party wireless Internet service providers (hotspots at a coffee shop or library).

All users accessing OPM network and server resources through wireless connections must adhere to this guidance to ensure Federal information is safeguarded to the greatest extent practicable. Following these guidelines helps protect OPM's technology-based resources and information is also mandatory.

This guidance is complementary to any previously-implemented policies dealing specifically with network access and remote access to the enterprise network.

2.0 SCOPE

This guidance applies to all OPM employees, OPM contractors and any other individuals accessing OPM resources or data (collectively called "users"). This guidance also applies to all computer equipment used to access OPM resources, even if the equipment is not OPM-owned or supplied. For example, use of a public library's wireless network to access the OPM network would fall under the scope of this guidance.

3.0 ELIGIBLE USERS

All users with authorized and active Local Area Network (LAN) accounts are eligible for wireless access.

4.0 WIRELESS ACCESS USAGE RESTRICTIONS

Although OCIO provides tools and technologies to make the network and devices secure, OPM users have a responsibility to ensure that their wireless connection remains secure. Users must observe the following rules in order to ensure a safe and secure wireless connection:

- All OPM-provided wireless devices to be used at OPM or for accessing OPM network and server resources will be purchased through the OCIO as defined in the Information Technology Procurement Policy.

- When desktop or laptop computers are connected physically to the OPM network via a network cable, wireless will be disabled automatically.
- Users traveling with wireless devices to locations with current travel warnings from the U.S. State Department (http://travel.state.gov/travel/cis_pa_tw/tw/tw_1764.html) must take extra measures to physically safeguard mobile devices. Upon return from locations with "current travel warnings" users must return mobile devices to OPM Customer Support (Help Desk) for inspection and/or re-imaging as appropriate. The use of Bluetooth or infrared technologies is currently prohibited on OPM's network. Desktop or laptop computers will be configured in a manner that disables these features.
- Users can connect to OPM through cellular technology (using an air card, for example) or through a wifi connection, but not both at the same time.
- In an effort to ensure the highest level of security while accessing network and server resources, the NM Network Security team (NS) may disconnect any devices connected to OPM network and server resources if they are not configured properly.
- Government-furnished and contractor-furnished equipment connecting to OPM network and server resources will have an approved OPM configuration image.
- OPM users need to ensure that their physical environment is protected from unauthorized viewing of login credentials and OPM data.
- OPM users need to report any incident or suspected incidents of unauthorized access and/or disclosure of OPM's information and technology resources to their manager and OPM's Situation Room (202-418-0111).

5.0 IMPLEMENTATION GUIDANCE

Connecting to OPM's Wireless Network

Even though OPM's wireless network has security measures in place, it is still important that you follow certain steps to make sure your system is secure:

- When you step away from your computer make sure to lock the system so that no one can use it without your knowledge or permission.
- Do not bring in your own wireless access points and attempt to use them on the OPM network.
- Do not attempt to access the OPM network using a cable at the same time that you are connected wirelessly. Similarly, do not attempt to access another wireless service (such as through an air card) while connected wirelessly to the OPM network.

Connecting to a Home Wireless Network

The Help Desk will ensure that your wireless device is working properly on your laptop when you bring it to the Help Desk for configuration and/or troubleshooting. However, because of the number of wireless network devices and numerous configuration options, the OPM Help Desk cannot setup or trouble-shoot individual home network configurations. OPM employees

should take the following steps to make sure their home networks are configured correctly and secured:

- Modern wireless equipment for the home, such as wifi routers, has the capability to be secured. Each device manufacturer has different ways of implementing these security controls, but they all conform to a common set of standards (such as WiFi Protected Access, or WPA). OPM employees who wish to use their home wireless networks to access OPM resources should refer to their equipment documentation to make sure they have taken steps to protect their network. Internet Service Providers may also have support phone numbers that employees can call to get assistance securing their wireless home networks.
- Do not share passwords, keys, PINs or other information about home wireless networks with anyone.
- Change device passwords periodically and do not use default passwords set by equipment manufacturers.
- Do not allow anyone, including family members, to use OPM-issued equipment for any reason.
- When you step away from your computer at home, just like you would at work, make sure to lock the system so that no one can use it without your knowledge or permission.
- During setup of wireless equipment at home, always select the option that requires a heightened level of security and password. Do not configure wireless devices so that anyone can access without permission or a password or passphrase.

Connecting to a Third-Party Wireless Network

There are wifi networks almost everywhere you go these days. Many of these are managed by retail companies that want to provide the service as a way to attract customers. It is extremely important that you know who is running a wireless network before you connect to it. Here are some steps you should follow to make sure you connect securely:

- Do not connect to a wireless network if you are not sure who is running it. For example, if you are in a coffee shop, you may see several wifi network names when you use your computer. You should only connect to the network run by that coffee shop; if you are not sure which network is the right one, either do not connect at all or ask an employee.
- When traveling, the hotel wher you stay may provide wireless access. Often, in order to use these networks, you must verify that you are a guest of the hotel by providing a key or other information. As with the coffee shop example above, make sure to verify with the hotel the proper network and the right procedures.
- It is your responsibility to practice safe computing. Third party wireless networks may be run by someone trying to get access to your personal information or other information on your computer. If you are not sure who is managing a wireless network, do not use it!

6.0 POLICY NON-COMPLIANCE

Failure to comply with this Policy and Agreement may result in the suspension of remote access privileges, disciplinary action and possibly termination of employment.

7.0 EMPLOYEE DECLARATION

I have read and understand the above Wireless Security Access Policy and Agreement and consent to adhere to the rules outlined therein.

_____	_____
Employee Signature	Date
_____	_____
Manager Signature	Date