USAID
FROM THE AMERICAN PEOPLE

Wireless Standards and Guidelines

A Mandatory Reference for ADS Chapter 545

Full Revision Date: 12/23/2014
Responsible Office: M/CIO/IPM/ECM
File Name: 545mbg_122314

TABLE OF CONTENTS

1 Introduction

2 Purpose

3 Audience

4 Scope

4.1 Individuals
4.2 Devices
4.3 Locations
4.4 Networks
4.5 Methods of Access
4.6 Classifications of Information

5 Exceptions

6 Monitoring and Privacy Expectations

6.1 Government-Furnished Equipment (GFE)

6.2 Bring Your Own Device (BYOD)

7 Access Agreements

8 Privacy and Security

8.1 Physical Security
8.1.1 Safeguarding and Protection
8.1.1.1 CONUS
8.1.1.2 OCONUS

8.1.2 Incident Response

8.1.3 Inventory

8.1.4 Property Loss or Damage

8.2 Cyber Security
8.2.1 Data in Transit (DIT)
8.2.2 Configuration of WDs
8.2.2.1 Encryption
8.2.2.2 User and Device Authentication

9 Management

9.1 Patch Management

9.2 Vulnerability Management

9.3 User-Initiated Changes
9.3.1 GFE WDs
9.3.2 BYOD

10 Usage and Restrictions

10.1 DOS Classified Systems and Workspaces

10.2 Defense Intelligence Agency's (DIA's) Classified Systems and Workspaces

10.3 Travel

10.4 Suspicion of Compromise

11 List of Acronyms

1. Introduction

Wireless communications must comply with the minimum specifications outlined in the provisions of federal policy, laws and standards. The National Institute for Standards and Technology (NIST) is responsible for developing information security standards and guidelines including minimum requirements for federal information systems. NIST guidelines are consistent with the requirements of the Office of Management and Budget (OMB) **Circular A-130, Section 8b(3), Securing Agency Information Systems**, as analyzed in **Circular A-130, Appendix IV: Analysis of Key Sections**. Supplemental information is in **Circular A-130, Appendix III, Security of Federal Automated Information Resources**. Federal Information Security governance is in United States Code (USC) (a) **44 USC CHAPTER 35, Coordination of Federal Information Policy**, (b) **Public Law 107-347, E-Government Act of 2002**, and (c) the **Federal Information System Management Act of 2002 (FISMA)**.

These documents collectively create and define the positions of federal chief information officers (CIOs) to include their roles and responsibilities regarding Information-Security-Program compliance and reporting requirements for Information Technology (IT) assets of Executive Departments and Agencies of the Federal Government.

2. Purpose

The purpose of this document is to describe the standards for wireless communications that fall under its scope to avoid repeating what other policies, standards, laws, guidelines, etc. have already stated, and to keep this standard as concise, non-burdensome, and flexible as possible. Therefore, wherever appropriate, it references other documents that either support a given statement or dictate a required action.

3. Audience

While anyone is welcome to read this standard, the intended audiences are those USAID personnel responsible for ensuring that it is followed. Primarily, these personnel include designers, developers, operational personnel, and auditors (e.g., intra-office auditors, agency auditors, or external auditors).

4. Scope

The scope of this standard includes certain individuals, devices, locations, networks, etc. To help keep the document focused and concise, all elements below define the scope. The reader is to consider them together, not separate. That is, in order for a situation to fall within the scope of this document, it must fall under every element below: i.e., individuals, devices, etc.

Wireless communications are at the Open System Interconnect (OSI) model's Layer 1 (L1); that is, the physical layer. This standard, therefore, focuses only on L1 with respect to wireless networking and communications. All other layers of the OSI model, fall under other standards.

4.1 Individuals
This standard applies to all members of the USAID workforce including all employees in any direct or support capacity to include volunteers, trainees, and any other person whose conduct is under the direct control of USAID in the performance of work for or on behalf of USAID.

4.2 Devices
This standard applies to all government-owned, contractor-owned or contractor operated (COCO), or personally owned wireless devices (WDs). A WD is one that receives or transmits wireless frequencies of the electro-magnetic (EM) spectrum that the government or agency has set aside for communicative purposes. Some examples include (i) Wi-Fi, which follows the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 Standard; (ii) Bluetooth, which follows the IEEE 802.15.1 standard; (iii) Cellular such as 4G LTE; (iv) microwave; (v) satellite; and (vi) infrared.

4.3 Locations
This standard applies to locations within the continental United States (CONUS) or outside of the CONUS (OCONUS) and that are in or near USAID facilities or workspaces including telework locations.

4.4 Networks
This standard applies to private networks that USAID owns, operates, or leases.

4.5 Methods of Access
This standard applies only to wireless access methods.

4.6 Classifications of Information
This standard applies only to unclassified information designated as Sensitive But Unclassified (SBU) information. It does not apply to classified information at any level; for classified standards, see **ADS 552, Classified Information Systems Security**.

5. Exceptions
Exception to this standard must be in writing, must demonstrate a compelling need, and must set forth a valid justification. Any exceptions to this standard must have approval from the agency's Authorizing Official (AO), who is the CIO or the CIO's designee.

6. Monitoring and Privacy Expectations
All devices, which fall under the scope of this standard, are subject to monitoring and privacy rules per the latest release of **NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations**. See also **NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations**.

6.1 Government-Furnished Equipment (GFE)
Governmental employees do not have a right, nor should they have an expectation, of privacy, at any time, while using GFE WDs to communicate including accessing the

Internet and using e-mail and voice communications. To the extent that employees wish that their private activities remain private, they should avoid using the GFE WDs for limited personal use. By acceptance of the GFE WD, employees imply their consent to disclosing and monitoring of device usage including the contents of any information maintained or transmissions passed through the WD.

6.2 Bring Your Own Device (BYOD)

For BYOD WDs, which access agency networks and information, only their communications and accesses are subject to monitoring and then only during connectivity to an agency network. BYOD WDs must also meet the other aspects of this standard.

7. Access Agreements

All personnel having GFE WDs must sign and follow the applicable CIO-approved access agreement(s). Access agreements include, for example, nondisclosure agreements, acceptable-use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational information systems to which access is authorized.

8. Privacy and Security

All WDs must meet federal privacy and security standards and policies as listed below.

8.1. Physical Security

With regard to wireless access points (WAPs), no one is allowed to move or change any fixed, CIO-installed WAP without going through the change-review process and gaining approval.

8.1.1. Safeguarding

GFE WDs must follow **Section 547.3.2** of **ADS 547, Property Management of Information Technology (IT) Resources** for the safeguarding of the device.

8.1.1.1. CONUS

Physical security within the CONUS must follow **ADS 547**.

8.1.1.2. OCONUS

Physical security OCONUS must follow **ADS 534, Personal Property Management Overseas** and the U.S. Department of State (DOS) Foreign Affairs Manual (FAM) Volume 14: specifically, **14 FAM 400, Post Operations** when at a DOS facility or using a DOS WD.

8.1.2 Incident Response

For incident response, users must follow **Section 545.3.4.11** of **ADS 545, Information Systems Security.**

8.1.3. Inventory
On inventory, GFE WDs must follow **Section 547.3.1** of **ADS 547**.

8.1.4. Property Loss or Damage
For property loss or damage, users must follow **ADS 547**.

8.2 Cyber Security

8.2.1. Data in Transit (DIT)
For DIT, GFE WDs and associated equipment must follow **Sections 545.3.4.9(b)5** and **545.3.5.5** of **ADS 545**.

8.2.2. Configuration of WDs

8.2.2.1. Encryption
All WDs, whether GFE or BYOD, must have active encryption that satisfies **NIST SP 800-53** and **NIST SP 800-124, Guidelines for Managing the Security of Mobile Devices in the Enterprise**. For example, if using Wi-Fi WDs, then encryption must be set according to the NIST standard for Wi-Fi WDs.

8.2.2.2. User and Device Authentication
All GFE WDs will be configured requiring active passcodes for authentication in accordance with parameters specified in **NIST SP 800-124** (Note: All GFE WDs should be base lined with authentication configuration prior to issuance/installation).

9. Management
WDs must follow an approved federal device-management solution, and it, at a minimum, must meet the requirements of this WD standard as well as **NIST SP 800-124.**

9.1. Patch Management
For patch management, GFE WDs must meet **NIST SP 800-53** with respect to patch management to include change and configuration management.

9.2. Vulnerability Management
For vulnerability management, GFE WDs must follow **Section 545.3.4(b)5** of **ADS 545** and "**The (SBU) USAID Vulnerability Management Guide**."

9.3. User-Initiated Changes

9.3.1. GFE WDs
Per **Sections 545.3.4.9(d)6, "Hardware and Software"** and **545.3.5.6(11)**, **"System and Information Integrity"** of **ADS 545,** the user, of any GFE WD that falls under the scope of this standard, must not attempt any hardware or software changes to the device. The only allowable WDs for GFE are those that allow locking the device down so that such changes are possible only by authorized personnel (e.g., authorized device administrators).

9.3.2. BYOD

Owners may change BYOD WDs so long as the change does not violate any other part of this standard.

10. Usage and Restrictions

This document defines National Security Information (NSI) as classified information. It defines NSI systems as any system (e.g., network, end point, server, etc.) that is used to handle or process NSI information, and it defines associated workspaces as those areas where NSI exists.

WDs must follow the restrictions (see **CNSSP-17, Policy on Wireless Standards**) for being or operating in and around NSI systems and workspaces as well as the DOS restrictions below.

a. **WLAN Security Standard**
b. **Secure Enterprise Wireless Devices for Unclassified Use within Department of State**

GFE WDs and handicap assisted technologies that use WDs (whether GFE or not) may be used in or around NSI systems and workspaces only if authorized, in writing, by the AO. Non-authorized WDs must not be in or around any NSI system or workspace. All personally owned wireless devices are prohibited in a NSI workspace and must be stored in approved faraday locker prior to entering the NSI workspace.

10.1. DOS Classified Systems and Workspaces

Secret-collateral resources are managed by DOS; therefore, these NSI systems and associated workspaces fall under DOS policies (see **12 FAM 500, Information Security** and **12 FAM 600, Information Security Technology**; also see ADS **545**, **565 (Physical Security Programs (Domestic))**, and **552**).

10.2. Defense Intelligence Agency's (DIA's) Classified Systems and Workspaces

These NSI Sensitive Compartmented Information (SCI) Facilities (SCIFs) fall under Defense Intelligence Agency Directives (DIADs). Users of WDs that work in or near SCIFs must follow the DIADs, which can be obtained by contacting DIA HQ, Office the Chief Information Officer, Information Assurance Division, 200 MacDill Blvd., Joint Base Anacostia Bolling, Washington, DC 20340-5100.

10.3 Travel

When traveling to locations that pose an "unacceptable" risk of theft or technical exploitation (whether clandestine or not) of WDs, users must obtain temporary ("loaner") GFE WDs from the office of the CIO. An "unacceptable" risk rating is based upon the technical and HUMINT threat as identified and defined within the Department of State's Security Environment Threat Listing (SETL) (is available on classified network) and is covered during the overseas travel security brief, which USAID personnel must attend prior to traveling OCONUS. The CIO's office works with the security office to establish this risk. Visit SEC for questions regarding the threat evaluation for a particular post.

Due to its rapid response requirements, the Office of U.S. Foreign Disaster Assistance (OFDA) maintains and follows its own comprehensive set of security controls for travel with WDs, which may vary from the standard USAID policy but will be in compliance with applicable FISMA and NIST guidelines.

10.4. Suspicion of Compromise

If a user knows or ever suspects that their WD has been compromised, then the user must immediately turn off the WD and deliver it to the CIO's Information System Security Officer (**ISSO@usaid.gov**). The user must not allow the compromised or possibly compromised WD to connect to any networks (wireless or wired) or GFE.

11. List of Acronyms

AO	Authorizing Official
ADS	Automated Directives System
BYOD	Bring Your Own Device
CIO	Chief Information Officer
COCO	Contractor Owned Contractor Operated
CONUS	Continental United States
CUI	Controlled Unclassified Information
DIA	Defense Intelligence Agency
DIAD	DIA Directive
DIT	Data In Transit
DOS	Department of State
EM	Electro-Magnetic
FAM	Foreign Affairs Manual
FISMA	Federal Information System Management Act
GFE	Government Furnished Equipment
IEEE	Institute of Electrical and Electronics Engineers
ISSO	Information System Security Office
IT	Information Technology
L1	Layer One (1)
NIST	National Institute of Standards and Technology
NSI	National Security Information
OCONUS	Outside Continental United States
OMB	Office of Management and Budget
OSI	Open System Interconnect
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmentalized Information
SCIF	SCI Facility
SP	Special Publication
USAID	United States Agency for International Development
USC	United States Code
WAP	Wireless Access Point
WD	Wireless Device

545mbg_122314