Wireless Standards and Guidelines

A Mandatory Reference for ADS Chapter 545

Full Revision Date: 02/11/2019
Responsible Office: M/CIO/IA
File Name: 545mbg_021119

TABLE OF CONTENTS

1. Introduction

Wireless networks, technologies, and 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. For wireless networks, technologies, and communications, the specific NIST **Special Publications (SPs)** that constitute the mandatory framework for implementation are **SP 800-48**, **SP 800-97**, and **SP 800-153**.

NIST guidelines are consistent with the requirements of the Office of Management and Budget (OMB) **Circular A-130, Managing Information as a Strategic Resource**. 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)**.

2. Purpose

The purpose of this document is to describe the standards and provide guidelines for wireless networks, technologies, and communications. Wherever appropriate, it references other documents that either support a given statement or dictate a required action.

3. Audience

The intended audience for this standards and guidelines document is the USAID workforce, but primarily System Owners (SOs, Information System Security Officers (ISSOs)), IT designers, developers, operational personnel, and auditors (e.g., intra-office auditors, Agency auditors, or external auditors).

4. Scope

Wireless communications are at the Open System Interconnect (OSI) model's Layer 1 (L1); that is, the physical layer. The standard captured in this mandatory reference ("Standard") focuses only on L1 with respect to wireless networking and communications.

4.1 Definitions

1. Portable Electronic Device (PED): is an electronic device having the capability to store, record, and/or transmit text, images/video, or audio data. For the purposes of this policy, Mobile Devices (MDs) are a subset of PED. An MD is defined as a

PED that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable data storage; and (iv) is powered-on for extended periods of time with a self-contained power source. MDs may also have voice communication capabilities, on-board sensors that allow the device to capture information (e.g., photograph, video, record, or determine location), and/or built-in features to synchronize data with remote locations. Examples include smart phones, tablets, e-readers, and smart watches, or otherwise wireless-enabled wearable technology devices.

2. Wireless technologies: are the systems of hardware and its software protocols that permit the transfer of information between separated points without physical connection.

3. Wireless Device: is hardware that receives and/or transmits wireless frequencies of the electromagnetic (EM) spectrum that's used for communicative purposes.

4.2 Individuals

This Standard applies to all members of the USAID workforce, including individuals in a direct or support capacity. For the purposes of this Standard, the term workforce applies to all individuals working for, or on behalf of, the Agency, regardless of hiring or contracting mechanism, who have physical and/or logical access to USAID facilities and information systems. This includes Direct-Hire employees, Personal Services Contractors, Fellows, Participating Agency Service Agreements, and contractor personnel. Note: Contractors are not normally subject to Agency policy and procedures as discussed in ADS 501.1. However, contractor personnel are included here by virtue of the applicable clauses in the contract related to HSPD-12 and Information Security requirements.

4.3 Technologies, Networks, and Communications

This Standard applies to all government or contractor-owned or operated wireless technologies used for USAID business, and may apply to personally owned wireless technologies when used for USAID business. Wireless Technologies are the systems of hardware and its software protocols that permit the transfer of information between separated points without physical connection. 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 3G/4G/5G LTE; (iv) microwave; (v) satellite; and (vi) infrared. A Wireless Device (WD) is hardware that receives and/or transmits wireless frequencies of the electromagnetic (EM) spectrum that's used for communicative purposes.

4.4 Wireless Technology Locations

This Standard applies to USAID wireless networks, technologies, and communications located within the continental United States (CONUS) and outside of the CONUS (OCONUS), and locations in or near USAID facilities or workspaces where USAID wireless networks, technologies, and communications are accessible. For the purposes of this Standard, the term "controlled space" means USAID managed facilities in domestic and overseas posts. For guidance on restricted space, please see **ADS 565** and **ADS 568**.

4.5 Classifications of Information

This Standard applies only to unclassified information and devices. It does not apply to classified information or classified devices at any level. For classified standards, see **ADS 552, Cyber Security for National Security Information (NSI) Systems** for guidance. In the event of a security incident involving classified information on wireless networks or devices, users must immediately contact both the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** and the Office of Security (SEC) as instructed in **ADS 552** and **ADS 568, National Security Information Program**.

5. Exceptions

Exceptions to this Standard must be submitted in writing, and must demonstrate a compelling need and set forth a valid justification. Exceptions must be approved by the the Agency's Chief Information Officer (CIO) in coordination with the Office of Security when the exception request affects restricted space.

6. Wireless Spectrum Standard

M/CIO reserves the right to manage the wireless spectrum in USAID occupied areas to ensure adequate security and privacy for USAID data, and a fair and efficient allocation of the wireless resource. Ensuring availability requires the careful management of traffic and the minimization of interference in the Radio Frequency (RF) environment.

M/CIO reserves the right to monitor the wireless spectrum in USAID occupied areas.

Procurement, installation, and use of wireless scanning solutions, network or standalone (such as the ones used for tests, pilots, prototypes and feasibility studies, including site surveys and spectrum analysis equipment), are not authorized unless approved by the CIO and/or Chief Information Security Officer (CISO).

M/CIO's management scope covers the following:

a) Operation of wireless equipment and emanations around USAID areas where classified information is stored, discussed, or processed;

b) Wireless emanations leaking outside the boundaries of USAID- controlled space in both domestic and foreign posts;

c) Operation of wireless devices connected to USAID wired networks; and

d) Operation of wireless networks or wireless devices installed inside USAID space.

Any wireless network installed in USAID space (both CONUS and OCONUS) must be approved by M/CIO. Wi-Fi network standards are provided in Section 6.1 below.

USAID officials specifically identified in writing by M/CIO can restrict the use of, or permanently disconnect, any wireless device from USAID space if it disrupts or interferes with services provided by USAID, or if it is not properly configured in accordance with this Standard.

USAID wireless solutions such as Wi-Fi, cellular hotspots ("Mi-Fi"), Bluetooth, and emerging technologies that are approved by M/CIO for use in AID/W and in Missions must provide users with adequate security while at the same time enabling business to be conducted with partners and guests.

CISO maintains Wireless Technical Guidance for different wireless technologies (**contact M/CIO Security Engineering at: seceng@usaid.gov** for additional information).

6.1 Wireless Network Standards (Wi-Fi)

When more than one U.S. Government-provided wireless network is available for a user, the USAID workforce must use USAID wireless networks (e.g., AIDNet or guest wireless) for official business where available and accessible. These networks are designed to satisfy the Agency's business and technical requirements. The USAID Wi-Fi provides protection for proprietary systems/data and avoids interference with the systems and operations of other United States Government agencies and partners.

USAID requires its wireless solutions to be approved at the Federal Information Security Modernization Act (FISMA) - Moderate impact level. The USAID wireless solution must comply with Wi-Fi Protected Access II (WPA2) Enterprise with the Institute of Electrical and Electronic Engineers (IEEE) 802.1X standard, which offers enterprise-grade authentication.

M/CIO operates and manages an independent Guest Wireless network at Missions. Guest Wireless networks at Missions collocated within Department of State (DoS) compounds must collaborate with M/CIO to accommodate DoS requirements and design as governed by the DoS Overseas Wi-Fi Program.

M/CIO requires centralized management of USAID wireless networks. The M/CIO approved design provides centralized log management, and allows government-issued wireless devices to be placed in appropriate security roles based on the type of access

required with proper segregation from non-government issued devices. The USAID wireless networks provide enhanced security for government furnished equipment (GFE), allowing software updates to occur over encrypted means and providing compliance towards HSPD-12 requirements (e.g., integration with Single Sign On (SSO) and Two Factor Authentication verification).

6.2 Access Agreements (Wi-Fi)

Individuals having access to Agency managed wireless networks must accept the applicable access agreement(s) before logging into the network. Signed access agreements include an acknowledgement that individuals have read the agreement, understand it, and agree to abide by the constraints in the agreement associated with organizational information systems to which access is authorized.

In instances where guests require internet wireless network access to conduct business related to USAID, the Bureau, Independent Office, or Mission (B/IO/M) can approve temporary access to the Guest Wireless network over which the B/IO/M has control.

7. Security and Privacy

All wireless networks, technologies, and communications must meet federal security and privacy standards and policies. Security and privacy controls must be applied to wireless technologies as a countermeasure to the use of pervasive tracking technologies.

All wireless devices and networks as defined in section 4.2 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**).

7.1 Cybersecurity

All Wi-Fi networks in USAID space (CONUS and OCONUS) and any other existing or emerging wireless-based technologies must meet CISO guidance and security controls specific for the impact level categorization approved, as described below.

7.1.1 Implementation of Wi-Fi

There are particular conditions for Wi-Fi network implementations that must be met after approval but prior to activation, and these controls must be maintained throughout the lifecycle of the implementation. The CISO must, at a minimum, implement the following:

- Wireless Intrusion Detection Systems (WIDS);
- Integrated Computer Incident Response Team (CSIRT) processes;

- Management Network Access Control and Authentication;
- User network access control and Terms of Use agreement;
- Radio Frequency (RF) containment;
- Agency approved positive disconnect switches within a Domestic Controlled Access Area (DCAA);
- Network segmentation via firewall;
- Registration of the Dedicated Internet Networks (DIN) with M/CIO; and
- Tamper-evident security seals applied to all approved Wi-Fi access points and WIDS modules in public areas.

Approved Wi-Fi equipment and locations will be tested on a yearly basis by M/CIO/IA. Wi-Fi equipment may be subject to random inspection throughout the year by the Office of Security (SEC) and/or M/CIO/IA in selected locations. Any equipment that is found to be in noncompliance with the above controls may be disabled and removed.

7.1.2 Access and Usage Controls for Wi-Fi

a) A segmented Wi-Fi Wireless Dedicated Internet Network (DIN) must be provided exclusively for users of USAID-owned mobile equipment, and an updated security profile and a strong authentication must be maintained.

b) In USAID/W, USAID-owned mobile equipment that has not been connected to AIDNET (GFE-Macs) or GFE that has not been connected for 90 days must use guest wireless to ensure the security posture of the network until the security profile is updated. GFE users must contact the M/CIO Service Desk at (202) 712-1234 or **cio-helpdesk@usaid.gov** and submit a ticket to request assistance in installing security updates to the GFE.

c) Where available, a dedicated Guest Wireless network is provided for users of non-USAID equipment (i.e., guests, other agencies, personally owned devices). Users of this network are responsible for the security of their devices, including the use of antivirus and personal firewalls. Any device exhibiting behavior indicative of being compromised will be removed from the network.

Contact M/CIO/IA at **seceng@usaid.gov** for additional information on Access and Usage controls.

7.1.3 Technology Controls for Other Wireless Technologies

a) Broadband access restrictions.

1. GFE mobile devices may use public broadband technologies (3G/4G/5G) to access USAID resources wirelessly when logged in using an RSA token or an M/CIO approved managed email client.

2. Users must assume that broadband connectivity is not secure to process sensitive USAID information, including voice communications, unless approved encryption is used. Voice communications and SMS texting can be intercepted and are not encrypted by default. Users must ensure they are using approved technologies such as USAID Google Meet.

b) Bluetooth requirements apply to all wireless clients (e.g., mobile devices (MDs), PDAs, laptops, and desktops) with Bluetooth capabilities. These requirements also apply to Bluetooth keyboards, mice, headsets, and any other Bluetooth devices that transmit or receive USAID data or voice communications. For guidance on Bluetooth requirements please contact **seceng@usaid.gov**.

c) Cellular Base Transceiver Stations (BTS) or signal boosters (microcells) in USAID controlled space falls under M/CIO spectrum management. They are typically used in buildings that have poor cellular signals and consist of a small cellular transmitter/receiver that is connected to the Internet.

d) Cellular hotspots, Mobile Wi-Fi Hotspots (e.g., Mi-Fi) and smartphones with data sharing capabilities must be approved to be used to provide cellular Internet service connection to portable Wi-Fi devices, including laptops and MDs. M/CIO must maintain an inventory of approved Mi-Fis and personal hotspots, including location of the devices (see 7.4 for guidance).

e) Wireless capabilities of peripheral equipment must be disabled by default. This applies to all peripherals connected to any USAID network and to systems processing or hosting USAID sensitive data. In cases where valid mission requirements or equipment limitations prevent disabling wireless capabilities, System Owners must comply with all requirements outlined in **ADS 545, Information Systems Security** and obtain a written waiver or written exception in accordance with this policy.

Contact M/CIO/IA at **seceng@usaid.gov** with questions about technical security specifications and implementation guidance about the technologies described above, or submit a **SHARP request** to request a review of emerging technologies.

7.2 Encryption

All wireless communications and technologies that process sensitive USAID information must have encryption that satisfies **NIST SP 800-53** and **Federal Information Processing Standards (FIPS)**. Users working remotely must only process sensitive information when logged into the Agency network via **https://remoteaccess.usaid.gov**.

7.3 Continuous Monitoring

Automated wireless scanning technologies must continuously detect, log, and when possible mitigate 24/7 harmful wireless activities in the different USAID wired and wireless network environments, such as:

a) Unauthorized active Wi-Fi signals (including Mi-Fi and smartphone hotspots) in USAID controlled space;

b) Unauthorized active Wi-Fi connections in wired and wireless networks, including Wi-Fi bridging, ad hoc Wi-Fi signals, and peer-to-peer Wi-Fi networks;

c) Leakage of strong USAID Wi-Fi signals outside specified boundaries in government-controlled spaces;

d) Wireless denial of service attacks and RF jamming of USAID Wi-Fi networks;

e) Misconfigured Wi-Fi network devices; or

f) Violation of the wireless and mobile security policy, such as:

1. No mandatory (or required) log-in for open access hotspots (including Mi-Fi and cell phone hotspots) in USAID controlled space;

2. Unauthorized access to approved Wi-Fi networks; and

g) Malicious wireless scanning or disruptive activities.

Manual and physical compensating countermeasures must be implemented when automation is not possible to detect or locate malicious WDs or technologies. Where feasible, a Wireless Intrusion Detection System (WIDS)/Wireless Intrusion Prevention System (WIPS) will be configured to locate/triangulate unauthorized Wi-Fi devices on a floor plan for quick removal.

7.4 Installation of, Relocation of, or Changes to Wi-Fi

USAID/W:

In order for Wi-Fi access points (including Mi-Fis and personal hotspots) to be approved in AID/W, several steps must be completed, as follows:

a) B/IOs must submit a written request to SEC's Information and Industrial Security Branch (**secinformationsecurity@usaid.gov**), and Domestic Security Branch (**secdomestic@usaid.gov**). The written request must detail the specific office space(s) that are requesting Wi-Fi, the designation of that space (unrestricted or restricted), and the purpose of Wi-Fi (see **ADS 565** and **ADS 568** for definitions on Restricted Space and Unrestricted Space).

b) If the request and the possible space re-designation (to unrestricted) is approved by SEC, M/CIO/IA reviews the request and ensures it meets all of the Wi-Fi requirements listed in this policy. See Section 8.1 for guidance on Wi-Fi use in restricted space.

OCONUS:

In order for Wi-Fi access points (including Mi-Fis and personal hotspots) to be approved in Missions, the Mission Executive Officer must contact M/CIO at **clientservices@usaid.gov** to initiate M/CIO/IA review. The EXO must provide documentation showing that the Regional Security Officer (RSO) has reviewed and agreed that Wi-Fi access points are permitted in the facility.

M/CIO must approve any move, addition and change for Wi-Fi appliances across USAID including CONUS and OCONUS (e.g., wireless arrays or Mi-Fi). M/CIO provides guidance to Missions on moves, additions, changes to wireless appliances modification and relocation of wireless network appliances; and disposition or transport of wireless equipment. M/CIO must be notified of any renovations or changes to workspace in order to ensure appropriate configurations are maintained.

In an emergency situation or during an extended disruption of services (more than four hours during core business hours), the user must submit a ticket to the M/CIO Helpdesk at **cio-helpdesk@usaid.gov** or (202) 712-1234 to request expedited approval from the CISO to use a temporary mobile hotspot.

8. National Security Information Usage and Restrictions

This document defines Classified National Security Information (CNSI) as classified information. It defines an NSI system 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.

Wireless communications in USAID managed or owned spaces must follow specific restrictions, outlined in the Wireless Local Area Network (WLAN) Security Standard or in DoS guidance, when located or operating in or around NSI systems and workspaces. Contact **seceng@usaid.gov** for the WLAN Security Standard and DoS guidance.

GFE WDs and handicap assisted technologies that use WDs (whether GFE or not) may be used in or around CNSI systems and workspaces only if authorized, in writing, by the Agency Authorizing Official (AO) (the Chief Information Officer is the USAID AO). Unauthorized wireless devices must not be in any restricted space or around any CNSI system. All GFE or personally owned wireless devices are prohibited in a CNSI workspace and must be stored in a SEC-approved locker prior to entering the restricted space.

8.1. Classified Systems and Workspaces

Wi-Fi active signals (including Mi-Fis, hot spots, etc.) are not permitted within restricted spaces due to the potential for compromise of classified information. Signal strength, emitting from Wireless Access Points (WAPs) and measured within restricted spaces must be deflected to prevent unauthorized wireless connections and classified data exfiltration.

An M/CIO approved wireless transport network is authorized to transmit strictly unclassified information. Processing or transmitting classified information via Wi-Fi is prohibited and would result in a security incident. WLAN implementations suspected or found to be in violation of this policy will be reported to M/CIO/IA and SEC and will be handled pursuant to the established security incident procedures.

Secret collateral resources are managed by DoS; therefore, these NSI systems and associated workspaces fall under DoS policies (**5 FAM 580, Wireless Information Technology,** **12 FAM 500, Information Security** and **12 FAM 600, Information Security Technology**). Also see USAID policies ADS **545**, **565, Physical Security Programs**, and **552**.

8.2. Sensitive Compartmented Information Facilities (SCIF)

See **ADS Chapter 568** for guidance.

9. List of Acronyms

AO	Authorizing Official
ADS	Automated Directives System
B/IO/M	Bureau, Independent Office, or Mission
BTS	Base Transceiver Stations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COCO	Contractor Owned Contractor Operated
CONUS	Continental United States
DIN	Dedicated Internet Network
DoS	Department of State
EM	Electro-Magnetic
FAM	Foreign Affairs Manual
FIPS	Federal Information Processing Standards
FISMA	Federal Information System Modernization Act
GFE	Government Furnished Equipment
IEEE	Institute of Electrical and Electronics Engineers
ISSO	Information System Security Office
IT	Information Technology
L1	Layer One (1)
MD	Mobile Device
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
PED	Portable Electronic Device
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SCIF	SCI Facility
SEC	Office of Security
SP	Special Publication
SSO	Single Sign On
USAID	United States Agency for International Development
USC	United States Code
WD	Wireless Device
WFGB	DoS Wi-Fi Governance Board
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WLAN	Wireless Local Area Network
WPA2	Wi-Fi Protected Access II

545mbg_021119