Mobile-Computing Device (MCD) Standards and Guidelines

A Mandatory Reference for ADS Chapter 545

Full Revision Date: 09/26/2014
Responsible Office: M/CIO
File Name: 545mat_092614

Table of Contents

1. INTRODUCTION

The purpose of this document is: to describe the standards for those Mobile Computing Devices (MCDs)/Mobile Devices that fall under its scope; to avoid repetition regarding other policies, standards, etc., already in use; and, to keep these standards as concise, non-burdensome, and flexible as possible. Therefore, wherever appropriate, ADS 545mat references other documents that either support a given statement or dictate a required action.

An MCD is one that (i) has a small form factor that 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 or removable data storage; and (iv) includes a self-contained power source. Within USAID MCD and Mobile Devices are synonymous; MCDs may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers: See **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations**. While NIST's definition does not list laptops as an example, most laptops fall within the definition, and this USAID MCD standard applies to laptops whether or not they meet all of NIST's criteria.

While anyone is welcome to read these standards, the intended audiences are those USAID personnel responsible for ensuring that these policies are followed, e.g., designers, developers, operational personnel, and agency auditors/external auditors.

2. SCOPE

The scope of this standard includes, but is not limited to, individuals, devices, locations, networks. The reader is to consider them together, not separately. That is, in order for a situation to fall within the scope of this document, it must fall under every element below.

2.1. Individuals

All members of the USAID workforce including all employees in any direct or support capacity. These individuals 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.

2.2. Devices

All government-owned, contractor-owned or contractor-operated (COCO), or personally owned MCDs.

2.3. Locations

Any locations within the continental United States (CONUS) or outside of the CONUS (OCONUS).

2.4. Networks

Private networks that are leased, owned or operated by and/or on behalf of USAID.

2.5. Methods of Access

Wired (such as copper and fiber) and wireless access (for example Bluetooth, Wi-Fi, and cellular) methods.

2.6. Classifications of Information

All unclassified information to include 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.**

2.7. Portable Media

The scope of this standard does not include portable media (e.g., thumb drives, external solid-state drives (SSDs), etc.). See **ADS 545, Information Systems Security** for the policy and/or standard regarding such devices.

3. EXCEPTIONS

Any exceptions to this standard must have approval from the agency's Authorizing Official (AO), who is the M/CIO or the M/CIO's designee. Exceptions to this standard must be in writing, must demonstrate a compelling need, and must set forth a valid justification. Please contact the **CIO Helpdesk** to initiate your request for an exception and include the information outlined above.

4. MONITORING AND PRIVACY EXPECTATIONS

All devices must display the standard governmental privacy notice per the latest release of **NIST SP 800-53**. See also **NIST SP 800-137, Continuous Monitoring**. MCDs must also follow **ADS 508, Privacy Program**.

4.1. Government-Furnished Equipment (GFE)

Personnel do not have a right to, or expectation of, privacy while using GFE MCDs. This includes but is not limited to accessing the Internet, using e-mail and voice communications. To the extent that employees wish that their private activities remain private, they should avoid using the GFE MCD for personal use. By acceptance of the

GFE MCD, employees imply their consent to disclosing and monitoring of device usage including the contents of any files or information maintained or passed through that device.

4.2. Bring Your Own Device (BYOD)

When the Agency implements BYOD it must be in accordance with the White House's **Digital Government Strategy**, governance, and deliverables.

4.2.1. Zero-Client-Type (ZCT) MCDs

For BYOD MCDs that access agency networks and information via a ZCT interface (e.g., a web browser or similar mobile application), they must follow the **Digital Government Strategy**. ZCT MCDs store nothing locally and provide remote-access services only.

4.2.2. Thick-Client-Type (TCT) MCDs

For TCT MCDs (e.g., a smart phone that can have multiple personas), the persona set aside for work must be subject to this standard as if it were GFE, since it is a virtual GFE device.

5. ACCESS AGREEMENTS

All personnel having MCDs must sign and follow the applicable USAID-approved access agreement(s). Access agreements include, but are not limited to, 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.

6. OFF-LINE OPERATONS

All MCDs must provide off-line operations for those capabilities that apply (e.g., processing e-mail that has been downloaded to the device). Such devices and their associated networked infrastructure must provide the capability to re-synchronize (re-sync) when the user connects to a suitable network and either (1) direct a re-sync or (2) has the device set to automatically re-sync.

7. SECURITY

All MCDs must meet federal privacy and security standards and policies. These are detailed below, and available in the latest release of **NIST SP 800-124, Guidelines for Managing the Security of Mobile Devices** and **NIST SP 800-53**.

7.1. Physical Security

7.1.1. Safeguarding

MCDs must follow **ADS 547.3.2 (Safeguarding IT Resources)** for the safeguarding of the device.

7.1.1.1. CONUS

Physical security within the CONUS must follow **ADS 547, Property Management of Information Technology (IT) Resources**, and **ADS 565, Physical Security Programs (Domestic)**.

7.1.1.2. 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** when at a DOS facility.

7.1.1.3. Encryption

Regarding encryption, MCDs must follow **ADS 545** and **OMB M-06-16, Protection of Sensitive Agency Information** (or its successor).

7.1.2. Incident Response (IR)

For IR, personnel must follow **ADS 545.3.4.11 (Incident Management and Response)**.

7.1.3. Inventory

For inventory, MCDs must follow **ADS 547** regarding IT property management and inventory.

7.1.4. Property Loss or Damage

For property loss or damage, users must follow **ADS 547**.

7.2. Cyber Security

7.2.1. Anti-Virus (AV) Protection and Firewalls (FWs)

For AV and FW protection, MCDs must follow **ADS 545**.

7.2.2. Data at Rest (DAR)

For DAR, MCDs must follow **ADS 545**.

7.2.3. Data in Transit (DIT)

For DIT, MCDs and associated equipment must follow **ADS 545**.

7.2.3.1. Wireless

For wireless standards, see **ADS 545mbg, Wireless Access Standards and Guidelines.**

7.2.3.2. Wired

For wired connections, MCDs must follow **ADS 549, Telecommunications Management.**

7.2.4. Passcodes

All MCDs, whether GFE or BYOD, must have passcodes to protect them from unauthorized access (see **NIST SP 800-124** and **ADS 545mau, Password Creation Standards and Technical Controls**). For BYOD MCDs, the work persona must follow this standard.

8. MANAGEMENT

MCDs must be under an approved federal mobile-device-management (MDM) solution: see also **NIST SP 800-124**. The MDM solution, at a minimum, must meet the requirements of this standard.

8.1. Patch Management

For patch management, MCDs must meet **NIST SP 800-53** with respect to patch management to include change and configuration management.

8.2. Mobile Application Management (MAM)

For MAM, MCDs must meet **ADS 545** for management to include change and configuration management.

8.3. Remote Wiping, Locking, and Disabling

The MDM solution must be able remotely to wipe or lock the MCD per **NIST SP 800-53**.

8.4. Vulnerability Management

For vulnerability management, the MCDs must follow **ADS 545** and "**The (SBU) USAID Vulnerability Management Guide**."

8.5. User-Initiated Changes

Per **ADS 545.3.4.9(d) (Hardware and Software)** and **ADS 545.3.5.6 (System and Information Integrity)**, the user, of any government-provided MCD (i.e., government-furnished equipment or GFE) that falls under the scope of this standard, must not attempt any hardware or software changes to the device. The MDM solution must lock down the device so that such changes are possible only by authorized personnel (e.g., authorized device administrators). This restriction also applies to BYOD as follows.

8.5.1. BYOD ZCT MCDs

The standard applies to the remote desktop but not the ZCT MCD, since the ZCT MCD has no persistence of information or data.

8.5.2. BYOD TCT MCDs

This standard applies only to the persona(s) set aside for work.

9. USAGE AND RESTRICTIONS

This document refers to 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. GFE MCDs and handicap assistive technologies that use MCDs (whether GFE or not) may be used in or around NSI systems and workspaces only if authorized, in writing, by the AO. Non-authorized MCDs must not be in or around any NSI system or workspace.

9.1. 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** and **12 FAM 600**; also see ADS **545**, **552** and **565**.

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

These NSI Sensitive Compartmented Information (SCI) Facilities (SCIFs) fall under DIA directives (DIADs). Users of MCDs that work in or near SCIFs must follow DIAD 8460.002 [available via the Joint Worldwide Intelligence Communications System (JWICS) or from the Classified Operations ISSO].

9.3. Travel

When traveling to locations that pose an "unacceptable" risk of theft or exploitation (whether clandestine or not) of MCDs, as determined and established by DOS, on behalf of the Federal Government; users must obtain temporary ("loaner") GFE MCDs from the office of the CIO. These temporary, loaner MCDs must be returned to the CIO's office, where they will be wiped clean, prior to reconnecting them to any USAID network. An "unacceptable" rating is covered during the overseas travel security brief, which USAID personnel must attend prior to traveling OCONUS. M/CIO works with the Office of Security (SEC) to establish this risk.

Users may take their GFE or BYOD MCDs when traveling to a location that has an acceptable risk, if the MCD meets all other elements of this standard, and if it only contains CUI necessary for the travel. All other CUI must be securely removed so as not to leave any forensic footprint.

9.4. Suspicion of Compromise

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

10. ACRONYMS

AO	Authorizing Official
ADS	Automated Directives System
AV	Anti-Virus
BYOD	Bring Your Own Device
CIO	Chief Information Officer
COCO	Contractor Owned Contractor Operated
CONUS	Continental United States
CUI	Controlled Unclassified Information
DAR	Data At Rest
DIA	Defense Intelligence Agency
DIAD	DIA Directive
DIT	Data In Transit
DoD	Department of Defense
DOS	Department of State
FAM	Foreign Affairs Manual
FISMA	Federal Information System Management Act
FW	Firewall
GFE	Government Furnished Equipment
IR	Incident Response
ISSO	Information System Security Officer
IT	Information Technology
MAM	Mobile-Application Management
MCD	Mobile Computing Device
MDM	Mobile-Device Management
NIST	National Institute of Standards and Technology
NSI	National Security Information

OCONUS	Outside Continental United States
OMB	Office of Management and Budget
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmentalized Information
SCIF	SCI Facility
SP	Special Publication
SSD	Solid State Drive
TCT	Thick Client Type
USAID	United States Agency for International Development
USC	United States Code
ZCT	Zero Client Type

11. DEFINITIONS

This section defines terms, including acronyms used in this document. For additional definitions, please see the **ADS Glossary**.

Thick Client Type (TCT) – is a computing workstation that includes most or all of the components essential for operating and executing software applications independently. A thick client is one of the components in client-server computing architecture that is connected to the server through a network connection and does not consume any of the server's computing resources to execute applications. A thick client may also be known as a heavy, fat or rich client.

Patch Management – is a strategy for managing patches or upgrades for software applications and technologies. The patch management plan helps the organization handle these changes efficiently.

Vulnerability Management – refers to the management and limiting of any perceived vulnerability or flaw in the system that can leave it open to attack. A vulnerability may refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.

Zero Client Type (ZCT) – is a type of thin client device that has a very small factor with little to no processing, storage and memory components. It is a compact client-end PC that is used in a centralized computing infrastructure or virtual desktop infrastructure (VDI).