DoD ANNEX
FOR
MOBILE DEVICE MANAGEMENT (MDM)
PROTECTION PROFILE

Version 1, Release 1

14 February 2014

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA FSO of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

This page is intentionally left blank.

1. INTRODUCTION

1.1 Background

A National Information Assurance Program (NIAP) approved Protection Profile (PP) includes requirements to ensure particular functionality is present and can be tested in a commercial product. It is possible there will be cases in which selections meet PP requirements but do not meet DoD-mandated specific values.

In accordance with the NIAP *Protection Profile for Mobile Device Managements* (version 1.0, dated 21 October 2013), selections, assignments, and objective requirements may be included in the NIAP Common Criteria Security Target (ST) such that the product still conforms to the Protection Profile. This document addresses the DoD specificity needed for mobile device management servers to be used within the DoD. As such, any vendor that wishes to be certified for DoD use, must indicate that they are claiming compliance with both the PP and the DoD Annex, and include the specified selections, assignments, and requirements in the ST upon initiation of a NIAP evaluation.

While a NIAP certificate can be awarded as long as the product meets all requirements in the PP, for use in the DoD it is also mandated that the product address all requirements listed in this DoD Annex.

1.2 Scope

The additional information in this document is applicable to all DoD-administered systems and all systems connected to DoD networks.

1.3 Relationship to STIGs

This Annex for Mobile Device Management Protection Profile (MDMPP) addresses the DoD specificity to the NIST SP 800-53 controls identified in the MDMPP. As a result, the Annex, in conjunction with the PP, serves as a single specification, within the DoD, for security of mobile device management servers and supersedes the current DISA MDM SRG Version 1, Release 1.

The publication of the Annex does not eliminate the DoD need for a product-specific Security Technical Implementation Guide (STIG); however, the results of the Common Criteria evaluation will be used to formulate a STIG. The benefit of this approach is that at the conclusion of a successful NIAP evaluation, a vendor's product will be certified as meeting the requisite NIST SP 800-53 controls and the information needed for a STIG will be available. The product may then be used within the DoD. STIGs will continue to be published in XCCDF format along with automation where applicable for assessment, as well as baseline configuration guidance for DoD.

1.4 Document Revisions

Comments or proposed revisions to this document should be sent via email to: disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil.

2. DOD-MANDATED INFORMATION

Convention: Underlined text indicates additional text not included in the MDM Protection Profile or selections or assignments that are applicable in the DoD environment.

2.1 DoD Assignments and Selections

FAU_ALT_EXT.1.1	[selection: change in enrollment state, any event logged by the mobile device as specified in the MDF PP and DoD Annex]
FAU_SEL.1.1(1)	[assignment: all FAU_ALT_EXT.1.1 and FAU_ALT_EXT.2.1 alerts]
FAU_SEL.1.1(2)	[assignment: all FAU_ALT_EXT.1.1 alerts]
FAU_STG_EXT.1.1	[selection: SNMPv3]
FIA_ENG_EXT.1.2	[selection: specific devices]
FMT_SMF.1.1(1)	enable/disable policy for [assignment: wireless remote access connections to the mobile device, including personal Hotspot service] (30) [assignment: enable/disable Location services, enable/disable [assignment: USB port, USB mass storage mode, USB tethering]] (48) Note: Personal Hotspot service is defined as the mobile device serving as a Wi-Fi access point providing mobile broadband wireless Internet access to a wirelessly connected device.
FMT_SMF.1.1(3)	[assignment: enforces organization-defined limits for consecutive invalid access attempts by an administrator during an organization-defined time period] [assignment: enforces organization-defined time period during which the limit of consecutive invalid access attempts by an administrator is counted] [assignment: automatically locks accounts for an organization-defined time period or must lock the account until released by an administrator IAW organizational policy when the maximum number of unsuccessful attempts is exceeded] [assignment: designated alerts to another enterprise network management application using an IPSec, TLS, or SSL encrypted secure connection] [assignment: supports administrator authentication to the server via the Enterprise Authentication Mechanisms authentication] [assignment: terminates administrator sessions upon administrator logout or any other organization- or policy-

	defined session termination events such as idle time limit exceeded] [assignment: logout functionality to allow the user to manually terminate the session] [assignment: enable/disable mobile device connections to back-office servers and network shares via the trusted channel between the MDM server and MDM agent]
FMT_SMR.1.2	[assignment: MDM Account Administrator [selection: account group name(s)], Security Configuration Policy Administrator [selection: configuration policy name(s)], Device Management Administrator [selection: device identifier(s)], Auditor, additional authorized identified roles]

2.2 Objective/Optional Functions Mandated for DoD

The following Optional and/or Objective Security Functional Requirements are mandated for the DoD:

- FAU_SAR.1.1
- FAU_SEL.1.1(1)
- FAU_STG_EXT.2.1
- FTA_TAB.1.1

2.3 DoD-Mandated Specific Values

The following value assignments are mandated for the DoD:

SFR ID	DoD Selections and Values
FTA_TAB.1.1	Note: The advisory notice and consent warning message is not required if the General Purpose OS or Network Device displays an advisory notice and consent warning message when the administrator logs into the General Purpose OS or Network Device prior to accessing the MDM server or MDM Server platform. The non-bracketed text below must be used without any changes as the warning banner. [A. Use this banner for desktops, laptops, and other devices accommodating banners of 1300 characters. The banner shall be implemented as a click-through banner at logon (to the extent permitted by the operating system), meaning it prevents further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating "OK."]

	You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: -The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. -At any time, the USG may inspect and seize data stored on this IS. -Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. -This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy. -Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.
FCS	The TOE must be FIPS 140-2 validated.
FMT_SMF.1.1(3)	For function: mobile device connections to back-office servers and network shares via the trusted channel between the MDM server and MDM agent o Disable unless the MDM server can support PKI-based mutual authentication between the network server and the mobile device user For function: MD user's ability to switch devices o Disable For function: enforces organization-defined limits for consecutive invalid access attempts by an administrator during an organization-defined time period o 3 attempts in 15 minutes For function: automatically locks accounts for an organization-defined time period or must lock the account until released by an administrator IAW organizational policy when the maximum number of unsuccessful attempts is exceeded

	○ Time period defined by local policy