Mobility Security Guide

04 November

2013

The Mobility Security Guide (MSG) describes a secure Enterprise Mobility Architecture, using a layered security approach with commercial products, services, devices and networks to securely connect mobile users to a U.S. Government (USG) enterprise. This release updates version 2.2 with the following minor changes: Updates the requirement ID numbers associated with mobility-related Protection Profiles (PP). While this document is intended for use within the USG, and national security systems in particular, NSA/IAD decided to make this information publically available as a service to other enterprise owners who may have a similar need to protect data and information within their own mobile ecosystem.

Enterprise Mobility Version 2.3

DISCLAIMER vi
COMMENTS vi
FURTHER INFORMATION vi
Change Log vii
Consolidated References viii
1 Enterprise Mobility 1
1.1 Goals 1
1.2 Enterprise Mobility Overview 2
1.3 Design Summary 4
2 User Equipment 6
2.1 Smartphone 7
3 Mobile Applications and Services 12
3.1 Secure Voice over Internet Protocol (SVoIP) Capability 13
3.2 Web-Based Non-Resident Data Capability 14
4 Access Networks 16
4.1 Cellular Services 16
5 Enterprise Mobility Infrastructure 18
5.1 Objective Enterprise Mobility Infrastructure Architecture 18
5.2 Prototype Enterprise Mobility Infrastructure Architecture 19
6 Mobility Threats, Risks, and Mitigations 24
6.1 Risks 24
6.2 Threats 24
6.3 Mitigation Considerations 25
Appendix A Architecture and Configuration - Enterprise Mobility Requirements A-1
Appendix B Test Criteria - Enterprise Mobility B-1
Appendix C Functional Requirements - Enterprise Mobility C-1
Appendix D Terminology D-1

FIGURES

Figure 1-1. Enterprise Mobility: Anytime, Anywhere Access 1
Figure 1-2. Basic Segments of the Enterprise Mobility Architecture 2
Figure 3-1. Two Tunnels of the Enterprise Mobility Solution 12
Figure 5-1. Objective Enterprise Mobility Infrastructure Architecture 19
Figure 5-2. Enterprise Mobility Infrastructure Architecture 19

TABLES

Table 1: Change Log vii
Table 2: Appendix A Requirement Designators A-1
Table 3: Overarching Mobility Requirements A-2
Table 4: VPN Requirements A-4
Table 5: SVoIP Requirements A-6
Table 6: Web Based Non-Resident Data Requirements A-9
Table 7: Carrier Service Integration Requirements A-10
Table 8: User Equipment Requirements A-11
Table 9: Infrastructure Requirements A-15
Table 10: PKI Requirements A-21
Table 11: Provisioning Requirements A-22
Table 12: Appendix B Requirements Designators B-1
Table 13: Overarching Mobility Test Criteria B-2
Table 14: VPN Test Criteria B-5
Table 15: SVoIP Test Criteria B-9
Table 16: Web Based Non-Resident Data Test Criteria B-15
Table 17: Carrier Service Integration Test Criteria B-17
Table 18: User Equipment Test Criteria B-18
Table 19: User Equipment Monitoring Service Requirements Test Criteria B-23
Table 20: Infrastructure Test Criteria B-26
Table 21: PKI Test Criteria B-38
Table 22: Provisioning Test Criteria B-41
Table 23: Appendix C Requirement Designators C-1
Table 24: Overarching Mobility Requirements C-2
Table 25: VPN Requirements C-2
Table 26: SVoIP Requirements C-3
Table 27: Web Based Non-Resident Data Requirements C-5
Table 28: User Equipment Requirements C-5
Table 29: Infrastructure Requirements C-10
Table 30: PKI Requirements C-10
Table 31: Provisioning Requirements C-10
Table 32: Acronyms D-1
Table 33: Definitions D-5
Table 34: Specialized Requirements Terms and Definitions D-6

MOBILITY SECURITY GUIDE OVERVIEW

The Mobility Security Guide (MSG) is a product of the National Security Agency's Information Assurance Directorate (NSA/IAD). To keep pace with technology and high customer demand, NSA/IAD developed a methodology and related architecture to enable commercial products and services to be used in layered solutions. When implemented properly these solutions provide sufficient security to protect classified National Security Systems (NSS) and related data. The process, entitled Commercial Solutions for Classified (CSfC), is based on commercial standards and facilitates development of solutions that may be fielded in months, not years. Vendor diversity for the encryption and security critical functions is essential to the security of the overall solution and particular component layering and implementation guidance in this document is required to provide adequate security.

This is the fifth in a series of Mobility releases and represents results of the ongoing exchanges among customers, private sector vendors and integrators, and NSA information security professionals. This release updates version 2.2 (published August 2013) and includes: mobile device management (MDM) to improve solution scalability and supportability, data at rest protection, and hardware root of trust requirements to provide a secure voice capability and web-arbitrated services. This solution is intended for users who have access to 3G/4G cellular infrastructure (2G cellular infrastructure is not supported).

The maturity of this solution continues to evolve at a rapid pace, but because commercial security solutions do not yet exist for every facet of this architecture, NSS users are required, as an interim measure, to submit a request for support to NSA/IAD prior to implementing a solution. Once the Mobile Access CP is published, customers will be able to use it to implement solutions without direct NSA/IAD involvement.

USG entities using this security guide to establish their own mobility capabilities must also present a solution to their organization's Delegated Authorizing Official (DAO) and must comply with all relevant policies on the use, storage, and management of mobile devices and infrastructure components. USG users must also comply with all existing applicable Certification & Accreditation (C&A) requirements levied by the organizational DAO including compliance with tailored controls drawn from catalogs such as NIST SP 800-53, Version 4. Guidance in the security guide takes precedence if a conflict occurs between the Mobility Security Guide requirements and the DAO requirements because of the security provided as a result of product diversity required in the security guide.

Any conflicts between the requirements contained in this guidance and any other national-level publications shall be identified and submitted for resolution through the appropriate service, command, and/or agency channels to the Director, National Security Agency (DIRNSA), ATTN: Information Assurance (IA) Policy and Doctrine. The National Manager is authorized to 1) approve, and has conditionally approved (based on contacting NSA for support), this security guide as an information assurance technique for securing NSS and the information they carry in the mobile environment and 2) prescribe this security guide guidance as the minimum standards for commercial solutions to protect such NSS and information in the mobile environment. (CNSS Directive 502, "National Directive on Security of National Security Systems," Section 8). However, users' application of this guidance does not constitute approval or accreditation of any particular solutions developed using this security guide. In accordance with Section 9.b of CNSSD 502, users of this security guide are responsible for obtaining, under their established agency accreditation and approval processes, C&A of any mobility solution processing classified information that has been developed in accordance with this security guide. Failure to properly and adequately follow the guidance in this security guide may reduce the security of the solution and, in the case of NSSs, provide insufficient protection for NSSs processing classified information, which would constitute a violation of CNSSD 502.

If users applying this security guide and developing solutions intended to process classified information need to deviate from the requirements and guidance in this document, they must obtain a waiver from their agencies' accrediting official as well as NSA before their solutions may be approved and accredited for use. Requests for exceptions to any of the provisions of this guidance must be submitted through the appropriate service, command, and/or agency channels to the DIRNSA ATTN: IA Policy and Doctrine, for approval prior to implementation. A request for a waiver must include a detailed justification for the deviation from the security guide.

DISCLAIMER

This security guide is provided "as is." Any express or implied warranties (including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose) are disclaimed. In no event shall the USG be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services, loss of use, data, or profits, or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this security guide, even if advised of the possibility of such damage.

The User of this security guide agrees to hold harmless and indemnify the USG, its agents and employees from every claim or liability (whether in tort or in contract), including attorneys' fees, court costs, and expenses, arising in direct consequence of Recipient's use of the item (including, but not limited to, claims or liabilities made for injury to or death of personnel of User or third parties, damage to or destruction of property of User or third parties, and infringement or other violations of intellectual property or technical data rights).

Nothing in this security guide is intended to constitute an endorsement, explicit or implied, by the USG of any particular manufacturer's product or service.

COMMENTS

Please provide comments concerning the improvement of this solution to mobility@nsa.gov. When submitting comments, please indicate whether you are claiming any intellectual property rights in the information you are providing and, if so, indicate which particular information you claim to be intellectual property. For more information about the NSA/IAD Mobility Program, please visit: http://www.nsa.gov/ia/programs/mobility_program/index.shtml

FURTHER INFORMATION

For more information about the Commercial Solutions for Classified Program (CSfC) or the related National Information Assurance Partnership (NIAP), please visit the following web sites:

1. The CSfC website: http://www.nsa.gov/ia/programs/csfc_program/index.shtml
2. The NIAP website: http://www.niap-ccevs.org/pp
3. NSA/IAD external website: http://www.iad.gov

Change Log

Table 1: Change Log

#	Date	Change Description
1.1	02/29/12	Initial revision for public distribution.
1.2	03/26/12	• Document is product neutral. Removed all references to products that were used as examples for emphasis. • Added disclaimer statements and statements about intellectual property. • Added improved discussion of how to use this document and how it relates to the Commercial Solutions for Classified Process. • Edited the document improving readability and removing grammar issues. • Removed un-necessary requirements. Expectation should be that other requirements will be removed or added in this and future releases based upon that maturity of those requirements in other documents. • Statements regarding required approvals are being removed from current version and will be added back in a later version for improved clarity.
2.0	07/30/12	• Section 1 features overview and design concepts. • Section 2 becomes Mobile Applications and Services, including the Secure VoIP capability, and adding a Web-Based Non-Resident Capability. • Section 3 contains User Equipment (UE) information, initially only smartphone. • Section 4 covers Access Networks, initially only cellular systems, and removes background information. • Section 5 updates Enterprise Mobility Infrastructure with both objective and prototype architectures. • Section 6 contains risk, threat, and risk mitigation information previously in multiple sections. • Acronyms and Terms updated. • References updated. • Appendix A contains architectural and configuration requirements compiled from multiple sections and updated. • Appendix B added with test criteria. • Appendix C added with functional requirements compiled from multiple sections and updated.
2.1	11/15/12	• Clarifications, corrections, and edit due to received comments on v2.0 • Additional security requirements were added. • Added VPN.08,WND.03, WNS.04, UES.23 • FVPC.02 was withdrawn and incorporated into FVPG.14. • FVPG.10 was withdrawn after modifying FVPG.08, and FVPG.09 by adding applicable Requests for Comment (RFCs). • Replaced Mobility SVoIP System with Enterprise Mobility System • Replaced Mobility SVoIP Solution with Enterprise Mobility Solution • Added Appendix B Commentary and new Table B-1 for Requirements Designators that renumbered other tables for Appendix B. • Added definition of “fixed devices”.

#	Date	Change Description
2.2	07/29/13	• Clarifications, corrections, and edits due to received comments on v2.1 • Added references to applicable NIAP protection profiles and 800-164 • Section 2 now contains User Equipment (UE) information, initially only smartphone, now generalized to include all mobile devices with a cellular modem • Section 3 now contains Mobile Applications and Services, including the Secure VoIP and Web-based Non-Resident Data capabilities • Added introduction in Section 2 describing USG intentions regarding vendor testing • Added terminology tables as Appendix D • Compared existing requirements (Appendices A-C) with PP requirements; withdrew overlapping requirements, added new requirements to fill identified gaps • Mapping for requirements in Appendices A against NIST SP 800-53 Rev 4 controls
2.3	11/04/13	• Minor grammatical corrections made

Consolidated References

Compliance Documents

National Policies:

- CNSSP-11/NSTISSP-11 Fact Sheet for National Information Assurance Acquisition Policy
- CNSSP-15 National Information Assurance Policy on the Use of Public Standards for Secure Sharing of Information Among Security Systems
- CNSSD-502 National Policy on the Security of National Security Systems
- FIPS Publication 140-2, Version 4 "Security Requirements for Cryptographic Modules"

Protection Profiles (available from NIAP):

- [Draft] Protection Profile for Certificate Authority (CA)
- [Draft] Protection Profile for Intrusion Prevention Systems (IPS)
- [Draft] Security Requirements for Email Application
- [Final] Protection Profile for Mobile Device (MD) Fundamentals
- [Final] Protection Profile for Mobile Device Management (MDM)
- [Draft] Security Requirements for Web Browser Application
- [Final] Network Device (NDPP) Extended Package SIP Server
- [Final] Network Device (NDPP) Extended Package Stateful Traffic Filter Firewall
- [Final] Network Device (NDPP) Extended Package VPN Gateway
- [Final] Protection Profile for IPsec Virtual Private Network (VPN) Clients
- [Final] Protection Profile for Voice over IP Application
- [Withdrawn] Security Requirements for Mobile Operating Systems

Applicable Standards

- IETF RFC 6380 "Suite B Profile for Internet Protocol Security (IPsec)"
- IETF RFC 6460 "Suite B Profile for Transport Layer Security (TLS)"
- FIPS Publication 180-3 "Secure Hash Standard"
- FIPS Publication 186-3 "Digital Signature Standard"
- FIPS Publication 197 "Advanced Encryption Standard"
- NIST Special Publication 800-56A "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"
- Suite B Implementer's Guide to NIST SP 800-56A

Other References

- DHS Federal Mobile Security Reference Architecture
- US-CERT Technical Information Paper – TIP-10-105-01, Cyber Threats to Mobile Devices
- NIST Special Publication 800-124 “Guidelines on Cell Phone and PDA Security”
- Defense Acquisition Guidebook
- FIPS Publication 140-2, Version 4 “Security Requirements for Cryptographic Modules”
- IETF RFC 3711 “Secure Real-Time Transport Protocol”
- IETF RFC 3261 “SIP: Session Initiation Protocol”
- IETF RFC 4301 “Security Architecture for Internet Protocol”
- IETF RFC 4566 “Session Description Protocol”
- IETF RFC 4568 “Session Description Protocol Security Descriptions for Media Streams” (Proposed Standard)
- IETF RFC 5280 “Internet X.509 public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”
- NIST Special Publication 800-53 Revision 4 “Security and Privacy Controls for Federal Information Systems and Organizations”
- NIST Special Publication 800-90A “Recommendation for Random Generation Using Deterministic Random Bit Generators”
- NIST Special Publication 800-137 “Information Security Continuous Monitoring”
- NIST Special Publication 800-133 “Recommendation for Cryptographic Key Generation”
- NIST Special Publication 800-90B “Recommendation for the Entropy Sources Used for Random Bit Generation”
- NIST Special Publication 800-164 “Guidelines on H
- IETF RFC 6460 “Supporting Suite B Cipher Suites”
- RFC 4210 “Artifact Management Protocol”
- RFC 6277 “On-Line Certificate Status Protocol”
- RFC 6402 “Certificate Management System over CMS”
- NIST SP 800-56 “Key Transport Scheme – Optimal Asymmetric Encryption Padding
- CNSSD 505 Supply Chain Risk Management

1 Enterprise Mobility

1.1 Goals

Adhering to the requirements in the "Mobility Security Guide", Enterprise Mobility provides users with anytime, anywhere access to data, services, and other users to successfully and securely achieve their mission, whether it is war fighting, intelligence, or business. Figure 1-1 is an operational view of secure anytime, anywhere access to the Government enterprise infrastructure.

Figure 1-1. Enterprise Mobility: Anytime, Anywhere Access

This Mobility Security Guide (MSG) describes the layered security approach for using commercial devices and networks to securely connect mobile users to the Government enterprise. Since secure mobile access using commercial technology is a new enterprise capability and the products and technologies are still maturing, the MSG is incrementally evolving towards a complete enterprise solution:

- **Evolving Capabilities:** Version 1.1 focused on using smartphones and commercial cellular networks to provide a secure voice capability. Version 2.0 added web- arbitrated services with non-resident data. Future versions will add the use of tablets, laptops, and Wi-Fi access networks, as well as expand on Mobile Device Management (MDM) services described in general terms in this version.
- **Evolving Guidance:** Initial versions outlined the security roles of the major components within the Enterprise Mobility architecture and offered a broad-based set of requirements to ultimately build secure capabilities. This release refines requirements and adds testing procedures. In particular requirements in Section A.6 have been further extended in NIST 800-164 and the MDM and Mobile Device (MD) Fundamentals Protection Profiles (PP). In the Mobile Access CP, additional guidance will be provided.

Details on the various aspects of the Enterprise Mobility capability are provided in the sections that follow, with specific architectural, configuration, and functional requirements and testing procedures listed in the Appendices.

1.2 Enterprise Mobility Overview

Enterprise Mobility is supported by the use of commercial cellular and wireless devices to access sensitive data and voice services, while addressing risk in the Government enterprise. Commercial cellular carriers and other open access networks provide the controlled connectivity between mobile users and the Government enterprise.

Figure 1-2 depicts the basic segments of the Enterprise Mobility architecture.

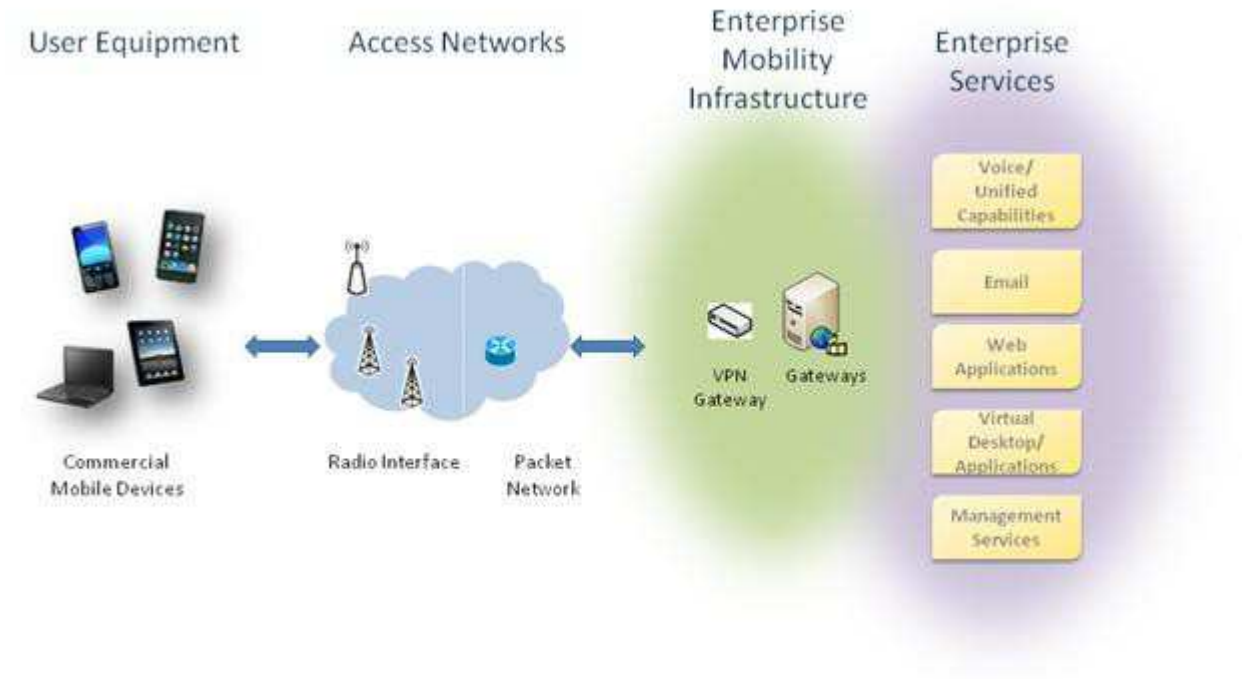

Figure 1-2. Basic Segments of the Enterprise Mobility Architecture

User Equipment are commercial mobile devices, including smartphones, tablets, and laptop computers, that support multiple radio connectivity options (primarily cellular and Wi-Fi) and host voice and data applications on general purpose operating system environments. Because commercial mobile devices will be used outside a classified environment, this security guide will consider the devices unclassified when powered down. However, they will be considered classified while in use.

- Commercial mobile devices provide widely available, cost effective, up-to-date technology for communications and application functionality. Use of these consumer-oriented devices minimizes the device cost and reduces technical obsolescence compared with Government specified and developed devices.
- Current commercial mobile devices have not fully addressed security issues relevant to Government operations. Enterprise Mobility will use commercially available protections that currently exist and compensate for device limitations within the overall Enterprise Mobility architecture, primarily by leveraging the secure Government enterprise. Where necessary, commercial mobile devices may be further hardened to improve integrity and reduce risks.

- Section 2 contains additional information on User Equipment.

Enterprise Services are the existing and evolving services provided for all enterprise users, including mobile users. At present, Government enterprise services include unified communications such as data (email, chat, presence) and voice (telephone/teleconferencing). They also include data services used by applications and/or web interfaces. Potentially this could be extended in the future to encompass video telecommunications and geo-location.

- Using enterprise service interfaces that are secured for all clients reduces the scope and complexity of Enterprise Mobility implementations; features implemented in the mobility architecture instead of the client need only be implemented once for all clients.
- It is assumed that the enterprise will provide archival and recovery services to all clients to include key escrow for emergency recovery functions.
- Section 3 contains more information on specific mobile applications and services.

Access Networks are commercial networks, such as commercial cellular providers and Wi-Fi access systems, which provide data network connectivity and capacity. These same commercial network technologies can be implemented on Government campuses and in tactical, deployable solutions. Whether commercial or Government controlled, these networks provide wireless data network access to mobile users that allows them to connect to Government enterprise services.

- Use of commercial mobile access networks reduces the cost of service at some expense of trust and control; interactions with commercial network providers must minimize visibility into Government subscriber information and usage data.
- Commercial network services provide limited security capabilities, but network services can be made more secure by tunneling encrypted sensitive data across them directly from the user equipment to Government facilities.
- The only commercial network service allowed for use by the mobile device is the data service that carries the tunneled encrypted sessions. The implication for Enterprise Mobility is that all services available to the mobile users will be provided via the Government enterprise. In particular, the carrier will not provide voice, Short Message Service (SMS), and other value-added services. Although an Enterprise Mobility user may not interact with cellular carrier services in the same ways as typical personal device users do, the capabilities can be similar and the user experience as close as practical.
- Section 4 contains additional information on Access Networks.

Enterprise Mobility Infrastructure provides the enterprise connection for all communications with User Equipment including call control establishing data connections for authorized User Equipment. Mobility-specific applications may also be hosted here, or proxies/gateways may be provided to interact with User Equipment security applications and to route Enterprise Services traffic.

- The Enterprise Mobility capability will secure, mediate, and manage the interaction between Government enterprise services and authorized User Equipment and users. User requests for service are always routed to and handled by enterprise mediation; authentication and authorization decisions for access to secure data and services are made in the enterprise.
- Since connection to commercial and public networks could expose the Government enterprise to a large number of threats, strong boundary protection must ensure that only authorized users, devices**,** and permitted traffic types are allowed.

- Since current mobile devices cannot provide sufficient trust and policy enforcement alone, the enterprise will need to monitor device usage and manage policy enforcement updates to ensure proper configuration. Enterprise security management services need to ensure that there is a solid foundation and a common, interoperable basis for secure operations.

Section 5 contains additional information on the Enterprise Mobility Infrastructure.

1.3 Design Summary

Layered solutions are the basis for the secure use of mobile devices and commercial components for access to Government enterprise services and data. Layers of commercial encryption, layers of authentication and authorization, boundary protection, appropriate hardening of devices, and mobile device provisioning and management all contribute to the overall security.

The following are the overarching themes for secure Enterprise Mobility capabilities.

- Employ layered data-in-transit protection to tunnel traffic from user equipment to the Government enterprise.
- Ensure that all service requests and user traffic from user equipment are mediated through the Enterprise Mobility Infrastructure.
- Locate the bulk of security functionality and trust in the enterprise.
  - Provision and manage devices to establish and maintain secure operations.
  - Authenticate devices and users prior to authorizing network and service access.
  - Provide strong boundary protection to limit risk to Government resources
  - Reuse enterprise services to the greatest extent possible including (but not limited to) certificate management, disaster recovery, and authentication

  Where necessary, harden commercial devices to protect integrity and reduce risks.

In order to promote interoperability and enable the use of a wide variety of commercial products, the following additional guidelines are used in the Enterprise Mobility architecture.

- Use open standards and protocols wherever possible.
- Avoid vendor lock-in, such as use of proprietary protocols; prefer vendor neutral applications and standard protocols.
- Any software license acquired should be non-exclusive and worldwide, with a right to distribute and sublicense the software to third parties. The license should not require the Government to obtain system configuration, maintenance, updates, or other technical support services from the vendor and it should not allow the vendor to audit the Government's use of the software.

  Use standards and service interfaces common with other clients (e.g., fixed, tactical) wherever practical.

In order to adequately protect sensitive information using commercial devices, the following cryptographic principles apply.

- To cross open access networks, two layers of approved commercial cryptography are required. One of these layers will be an Internet Protocol Security (IPsec) Virtual Private Network (VPN), which establishes a secured path between the User Equipment and the Enterprise Mobility Infrastructure. The other layer may depend on the particular applications and application-layer protocols being used and is specified elsewhere in this Mobility Security Guide.

- For any sensitive information on the device and not in use (aka “at rest”), there must be two layers of approved data-at-rest (DAR) protection. One of these layers may be provided by the operating system in a platform-wide data encryption mechanism. The other layer will depend on the particular applications being used to process sensitive information. For instance, a thin-client application would not expose data to the device and therefore would not require a second layer of approved DAR. However, a thick-client application will need to carry an additional layer of DAR protection in addition to whatever is provided by the native operating system.
- The implementation of the two layers must be independent. Using two independent layers reduces the potential for compromise of classified or sensitive information in case of implementation errors in a single commercial product.
- Government-issued Public Key Infrastructure (PKI) credentials should be used for mutual authentication in both layers.
- Suite B cryptography will be used for protecting classified data. For more information about the algorithms in Suite B, refer to CNSSP-15 and the National Institute of Standards and Technology (NIST) publications listed in the Consolidated Reference section.

2 User Equipment

The User Equipment portion of this document describes the commercial cellular and wireless devices used to access classified enterprise data and voice services. Commercial mobile devices, such as smartphones, tablets, and laptop computers, support multiple cellular and Wi-Fi connectivity options. This release of the Mobility Security Guide describes the smartphone cellular and data capability containing projections for the Next Generation Handset desired by USG. Future releases of the Mobile Access CP and other CPs will include other mobile device capabilities, such as laptops and tablets, using other transport mechanisms.

The Next Generation Handset Requirements consist of requirements for the mobile device endpoint (MDE), encompassing the mobile platform (operating system, kernel, firmware, and hardware), the VPN client, any possible MDM client and all associated application-programming interfaces (API). To implement this security guide successfully, the using agency must meet all USG requirements. The USG requirements include all other requirements in this Mobility Security Guide, the National Information Assurance Partnership (NIAP) PPs specified below, any compliance drivers such as NIST 800-53, and importantly NIST SP 800-164.

NSA will test commercial products for the next generation phone against the PPs (below) for compliance. The NIAP PPs that are applicable to the current architecture include the following.

- [Draft] Security Requirements for Email Application
- [Final] Protection Profile for Mobile Device (MD) Fundamentals
- [Final] Protection Profile for Mobile Device Management (MDM)
- [Draft] Security Requirements for Web Browser Application
- [Final] Protection Profile for IPsec Virtual Private Network (VPN) Clients
- [Final] Protection Profile for Voice over IP Application
- [Withdrawn] Security Requirements for Mobile Operating Systems

To assist in a successful accreditation decision, the appendices to this security guide specify requirements that may meet or partially meet NIST SP 800-53 control requirements. While NIAP PPs must be used to evaluate various components/sub-components of a secure solution, authorization to operate will depend on meeting any tailoring of controls for the composed solution and any other requirements levied by the authorizing official.

Because the Mobility Security Guide contains architectural and other requirements for components (in addition to the handset), the use of the entirety of the Mobility Security Guide is essential for any composed solution intended to process classified information in a NSS.

To gain access to draft or unpublished PPs (for example the MDM, email, web browser, and MD PPs) please consider joining the technical community at NIAP. Vendors, Integrators, and Original Equipment Manufacturers (OEMs) who join a technical community can obtain draft circulations of PPs for review and comment. Contact NIAP directly for more information about joining a technical community at www.niap-ccevs.org.

2.1 Smartphone

This section describes the security services and capabilities needed on a commercial smartphone and its resident operating system for use in the Enterprise Mobility capability using cellular networks.

Commercial smartphones are essentially computers integrated with radio components in a small package. They are not a trusted platform and do not yet provide all of the security mechanisms and levels of assurance that are desired. Enterprise Mobility will use the commercially available protections that currently exist, compensating for device limitations within the overall Mobility architecture by using secure Government enterprise services. To be clear, some of the protections afforded by mobile platforms are better than those on fixed systems but the risk associated with mobile processing of sensitive data requires additional desired assurance levels.

The User Equipment is a commercial smartphone that is configured to provide secure data connections to the Enterprise Mobility Infrastructure and secure communications (voice, video, and data) with other User Equipment.

- For secure voice communications, the User Equipment communicates with the commercial cellular network, as well as the VPN Gateway and SIP Server in the Enterprise Mobility Infrastructure in order to connect to the other User Equipment. Once the session is established, the User Equipment communicates across the cellular network and VPN Gateway with the other User Equipment to pass voice traffic. Two layers of encryption and authentication are used to protect communications across the commercial cellular network: call set-up is initiated using TLS over IPsec, while voice traffic uses SRTP over IPsec. See Section 3.1 for more information about protected secure voice communications.
- For secure web-based non-resident data services, the User Equipment communicates with the commercial cellular network, the VPN Gateway, and Web Server in the Enterprise Mobility Infrastructure. Two layers of encryption are used to protect communications across the commercial cellular network; data traffic uses TLS over IPsec. See Section 3.2 for more information about protected web-based non-resident data communications.

The operating system of the User Equipment is responsible for providing the following security functions to enable secure connections to the Enterprise Mobility Infrastructure for secure voice and data communications and to ensure that the device operates under known, authorized conditions.

- Protecting the Device (system configuration, device monitoring, authentication, updates, etc)
- Protecting Data (VPN client, DAR)
- Protecting the Keys (key/certificate management for the VPN client/other applications)

2.1.1 Device Protection

In order to ensure that only authorized users can use the User Equipment and that the User Equipment stays in a known secure configuration, the user equipment must be properly configured.

- **System Configuration:** The initial provisioning of the User Equipment reduces exposure to risk by removing or disabling non-essential services and applications. Interfaces (such as Wi-Fi and Bluetooth) should be configured so that no communications in or out of the User Equipment are permitted, except through the VPN/cellular connection to the Enterprise Mobility Infrastructure. Note that this also currently includes disallowing standard cellular services, such as voice calls (except emergency 911) and cellular messaging services. This provisioning must be completed before the User Equipment is distributed to users. Provisioning could also be executed by a security monitoring service (see Device Monitoring below) on the User Equipment each time it is

turned on, specifically to disable services/interfaces that could not be removed or disabled during initial provisioning. Applications shall be limited to those that have verified integrity and shall be approved by a vetting process by the host enterprise. The MDE shall enforce an application white list to prevent the installation and running of unapproved applications. The MDE shall verify the integrity of applications at application launch.

- **Device Monitoring:** A monitoring service must be available on the User Equipment in order to ensure that it operates under known, authorized conditions. Computer system faults are a common occurrence. Responding to a category of fault in a consistent way, based on risk aversion, is a basic way to ensure policy enforcement mechanisms are working as expected while protecting against potential abuse of the fault. Three factors must be considered when developing a device monitoring practice for systems built within this security guide.
    - **Security Enforcement:** For any fault management and security enforcement solution, we predicate the selection of responses for severity thresholds on the basic principle that we can categorize each computer system fault based on severity. The judgment of severity implies a risk decision. The MDM and MD PPs provide additional information on Fault Management and Security Enforcement.
    - **Continuous Operation:** The device monitoring service must be initiated when the User Equipment is turned on and continuously monitor the device to ensure that it stays in a secure state. The service checks at each boot to ensure that no unauthorized software has been installed and that all configuration settings are correct. It does so by monitoring the operating system, processes, applications, files, and interface port activities.
    - **Alerting and Logging:** The monitoring service must alert the user when issues are found and log the information both locally to the User Equipment and to a logging service within the enterprise. Initial deployments may have no provision for remote logging however eventually it would be desired to centrally log any issues inside the enterprise. Central logging and alerting will allow a more systematic response for any category of fault.
- **Event Response:** When an unauthorized event is detected, the monitoring service also prevents secure operation of the User Equipment with the enterprise and requires the device operator or an authorized enterprise service to determine a course of action (reboot, shut down, or continue to operate in an untrusted state) for the detected event. Upon detection of a severe fault, the monitoring service zeroizes the device, rendering it inoperable for secure use. The NSA Mobility definitions for each reaction (and even the naming scheme used) are implementation specific and can serve as analogy against which to build a fault management and security enforcement monitoring and auditing service. Currently, the monitoring service rides on top of the operating system which itself rides on the hardware platform. Monitoring service vendors should work to enable their products to use monitoring functionality implemented in system firmware. If the hardware and operating system are trusted then the monitoring service is expected to be trusted as well.
- **Local authentication:** The user must first authenticate to the User Equipment in order to use it. A password, passphrase, or other secure method is used to authenticate the user to the User Equipment. Periodic re-authentication is also required (screen lock). This partially addresses the threat of a lost or stolen device. Failed authentication attempts incur time-outs or other penalties based on organizational policy in order to deter rapid, repeated guessing of credentials. The corresponding authentication information (hash value) that is stored on the

User Equipment also needs to be protected (either by credentials or by full disk encryption) in order to prevent retrieval of that information for offline guessing.

- **Secondary authentication:** An additional authentication (password or passphrase) to the User Equipment may be required to protect secure credential storage (such as VPN certificates and private keys). The corresponding authentication information (as implemented, e.g. hash value) stored on the User Equipment also needs to be protected (either by credentials or by full disk encryption) in order to prevent retrieval of that information for offline guessing. Other authentication methods may be supported including biometrics. It is important to consider how many passwords (including their length and complexity) users will be willing to enter to use a given system, in order to appropriately balance security and usability.
- **Updates:** The organization shall deliver application, operating system, and firmware updates Over the Air (OTA) to the User Equipment by means under the control of the using organization. The organization shall deliver OTA updates via the dual layer encrypted connection between the User Equipment and the enterprise. The using organization may employ Device Management services to securely deploy signed updates to the User Equipment within the VPN tunnel from the Enterprise Mobility Infrastructure.
- **Radio Interface Behavior:** To enable access to the carrier network, the carrier may provide OTA updates to the radio interface software on the User Equipment. These updates should be limited to configuration policies, parameters, etc. required to access the carrier network. The User Equipment must block all non-essential updates to the radio interface.

2.1.2 Data Protection

A critical feature of the solution is data protection. Two layers of encryption will be used to protect all data carried over the carrier network. Similarly, two layers of DAR protection along with appropriate application isolation are required to protect sensitive data in processing and storage. This section outlines at a high level these requirements.

2.1.2.1 Data-in-Transit

All data between User Equipment and the Enterprise Mobility Infrastructure is protected in a VPN tunnel. Within this tunnel, application traffic is encrypted to provide an additional layer of protection.

The operating system of the User Equipment must provide an integrated VPN client or support a third party VPN client, which will use the IPsec protocol with Suite B algorithms, including Advanced Encryption Standard (AES) for data encryption. FIPS 140-2 level 1 certification is required for all encryption system components for which a NIAP certification is anticipated. Within IPsec/Internet Key Exchange (IKE), the VPN client will use public key certificates for mutual authentication with the VPN Gateway in the Enterprise Mobility Infrastructure. The VPN must be configurable to force all IP data communications to/from the User Equipment through the tunnel to the VPN Gateway in the Enterprise Mobility Infrastructure; no split-tunneling is allowed. If a basic firewall-like capability within the operating system exists, it must be configured to only allow IPsec/IKE VPN communications.

2.1.2.2 Data-at-Rest

If sensitive data is stored resident on the device, it must be protected by appropriate cryptographic controls for DAR as outlined in the draft Mobile Device PP. The Client Application requirements in this security guide specify additional requirements for DAR. Additional physical security hardening may be required depending on the use case. For instance, the handset should be protected with tamper evident seals (more below).

2.1.2.3 Data-in-Process

Protecting data being processed through appropriate application isolation is a key requirement of this solution. The requirements for application isolation can be found in the draft Mobile Device PP and in the draft Application on Operating System PP.

2.1.3 Local Key and Certificate Management

Public key certificates and their corresponding private keys are used to provide user and system authentication before establishing each of the two layers of encryption. The operating system must provide a secure storage capability for these credentials. The system must allow the user to decrypt sensitive materials (such as private keys) using an authentication (password or passphrase) mechanism separate from the screen lock. The decrypted private key-material or any ephemeral keys must not be stored on non-volatile memory and never written to log files in plaintext.

2.1.4 Other Security Considerations

2.1.4.1 Provisioning

In the event that User Equipment incorporating secure device management services is not available as a commercial capability, the using organization may harden the user device, operating system, and certain application by disallowing software update except by full reprovisioning of the User Equipment.

2.1.4.2 Supply Chain

A critical aspect of the U.S. Government's effectiveness is the dependability, trustworthiness, and availability of the information and communication technology (ICT) components embedded in the systems and networks upon which the ability to perform their missions rely. The supply chains for those ICT components are the underpinnings of those systems and networks. Supply chain attacks are proactive attempts to compromise those underpinnings.

Unfortunately, the supplier cannot always provide guarantees of a safe delivery of a first class component; they are only able to provide assurances based on their reliance on established procedures and processes they have developed. In a single change of hands, the component may be introduced to potential threats and compromises on many levels.

The supply chain threat refers to an adversary gaining access to a vendor, shipper, or retailer and then attempting to insert or install a modification or a counterfeit piece of hardware into a component that is destined for a U.S. Government customer in an effort to gain information or cause operational issues. This threat also includes the installation of malicious software on components of the solution. This threat is hard to identify and verify. This threat is increasingly harder to prevent or protect against since vendors build products using subcontracts with other companies to make certain parts of components. Additionally, it is often difficult to tell precisely where in the supply chain different pieces of components have been are built and installed.

Threat actions include manufacturing faulty or counterfeit parts or components that can be used to disrupt system or network performance, leaving open back doors in hardware that allow attackers easy ways to attack and evade monitoring, as well as easy ways to steal data or tamper with the integrity of

existing/new data. Supply chain attacks may occur during development and production, updates, distribution, shipping, at a warehouse, in storage, or during disposal.

To reduce the risks associated with the aforementioned threat of unauthorized device modification within the supply chain, each component shall go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's (Delegated Authorizing Official) DAO approved Product Supply Chain Threat Assessment process.

2.1.4.3 Tamper Protection

In order to provide additional protection to the User Equipment, the using organization may remove or disable some applications and services, to run a monitoring service, and to add physical/logical tamper detection measures. This security hardening must be achieved before the User Equipment is provided to a user. The User Equipment must allow the using organization the ability to place tamper-indicating seals on key items, such as the batteries and screw heads. Any removable memory must have the possibility to be glued or otherwise permanently affixed into the User Equipment to prevent its removal or replacement. Anti-tamper measures do not have to prevent tampering, but should make any attempt to tamper with User Equipment evident to a user.

3 Mobile Applications and Services

This section describes the applications and services that the mobile User Equipment will use. These capabilities have components that are resident on the User Equipment and that run as services within the Enterprise Mobility Infrastructure or within the Enterprise itself. In this section, the high-level service design and configuration guidance for client applications and the infrastructure components are covered.

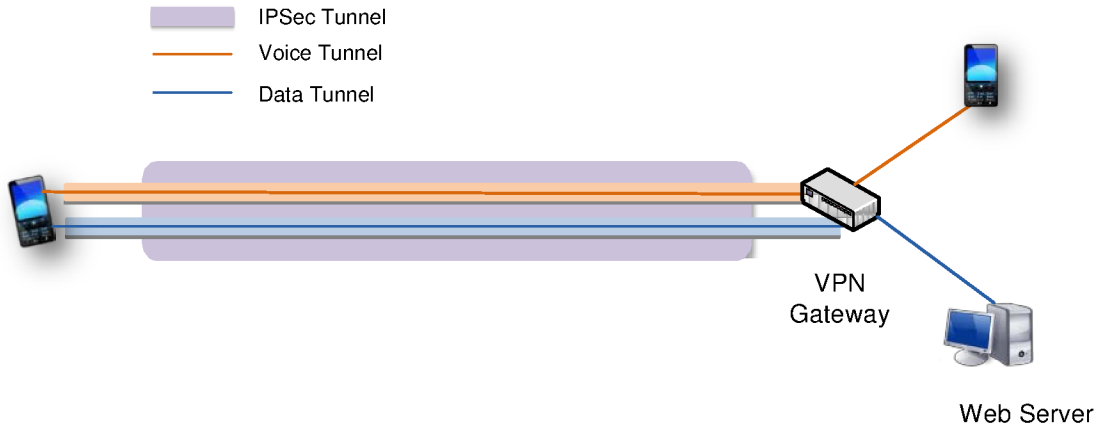

Figure 3-1. Two Tunnels of the Enterprise Mobility Solution

The mobile User Equipment connects to the enterprise (using data plans only) with layered encryption and authentication according to the following principles.

- All data between User Equipment and the Enterprise Mobility Infrastructure is protected in an IPsec VPN tunnel. The IPsec VPN connection must be established before connections to enterprise services are permitted. The VPN Gateway serves as the main entry point into the Enterprise Mobility Infrastructure and authenticates requested VPN associations using the IKE protocol. A VPN client that cannot be identified or authenticated is denied access to the Enterprise Mobility Infrastructure and to all enterprise services. See Section 3.1.2 and Section 5.2.2 for more information about the VPN.
- Within the VPN tunnel, application traffic is encrypted to provide an additional layer of protection. The inner layer may depend on the applications or services being used and is specified in the following sections.

In addition to the requirements in this security guide, commercial products must be tested against the PPs (below) for compliance. The NIAP PPs that are applicable to the current architecture include the following.

- [Draft] Security Requirements for Email Application
- [Draft] Security Requirements for Web Browser Application
- [Final] Network Device (NDPP) Extended Package SIP Server
- [Final] Network Device (NDPP) Extended Package VPN Gateway
- [Final] Protection Profile for IPsec Virtual Private Network (VPN) Clients
- [Final] Protection Profile for Voice over IP Application

3.1 Secure Voice over Internet Protocol (SVoIP) Capability

This section describes a Secure Voice over Internet Protocol (SVoIP) capability to enable secure voice communications between User Equipment. Threshold requirements for the SVoIP capability found in Appendix A and functional requirements in Appendix C must be met for the system to process classified data as a NSS. To assist the using agency's accrediting officials, test criteria for the SVoIP capability requirements are found in Appendix 0.

3.1.1 Security-Relevant Components

User Equipment uses a SVoIP client application configured to use the existing VPN tunnel for the outer layer of encryption. An inner TLS tunnel to a SIP Server residing in the Enterprise Mobility Infrastructure protects call control traffic, and an inner SRTP tunnel to another endpoint protects Real Time Services media streams. All SRTP traffic between User Equipment is routed through the Enterprise Mobility Infrastructure.

The following cryptographic protections are deployed as part of the SVoIP capability.

- **SIP over TLS:** SIP is used for registration of User Equipment, call setup, and call termination. TLS with Suite B compliant cryptography is used to protect SIP signaling traffic between the User Equipment and the SIP Server in the Enterprise Mobility Infrastructure. Although mutual authentication in TLS with public key certificates is preferred, the SIP Server may authorize users based on a USERID and password supplied in the TLS-protected session.
- **SVoIP Media Streams:** SRTP is used to protect media streams between secure voice systems. The Security Descriptions (SDES) [IETF RFC 4568] for media streams key transport of Session Description Protocol (SDP) must be used to initially negotiate the key for SRTP.

The following components are deployed as part of the SVoIP capability.

- **SVoIP Client:** The SVoIP Client on the User Equipment is configured to only connect to authorized SIP Servers.
- **SIP Server:** All secure mobile call requests are handled by a SIP Server within the Enterprise Mobility Infrastructure. The SIP Server acts as a SIP Registrar/Proxy to provide device registration and coordination of calls between User Equipment. Additionally, the SIP Server provides a SIP redirect service from one client in an enterprise to another client in a different enterprise to achieve interoperability between enterprises. All SIP traffic with User Equipment is protected using TLS with Suite B compliant cryptography. When SDES-SRTP is used, the master session keys are exposed to the SIP Server, and the server must be protected accordingly. Although mutual authentication in TLS with public key certificates is preferred for user authentication, the SIP Server may authorize users based on a USERID and password supplied in the TLS-protected session. The SIP Server may consult an Authentication, Authorization and Accounting (AAA) Server on the Enterprise Mobility Infrastructure for this user authentication/authorization.
- **Secure Voice Gateway:** Secure Voice Gateways provide the means to connect secure mobility solutions to other secure voice systems, terminating the mobility solution's protected channel and providing a secure voice gateway bridge to the interfacing system. The exact capabilities of the Secure Voice Gateway will depend on the networks and secure voice systems to which it is connected. Interoperability between secure systems will be more fully discussed in the Mobile Access CP.

3.1.2 Other Security Considerations

The following gaps have been identified.

- **Performance**: The multiple layers of encryption used and the lack of control over cellular data connection Quality of Service (QoS), especially for pre-4G networks, may affect the ability to make and maintain acceptable QoS voice calls. Secure voice gateways will be needed to extend commercial secure mobility solutions to interoperate with many existing secure voice systems. For use cases where secure voice gateways are used and additional layers of encryption and decryption are introduced, the call quality must be carefully analyzed as part of the implementation design and test.
- **Key Management:** SDES–SRTP requires exposure of key material on the SIP Server. However, the use of SIP over a mutually authenticated TLS connection protects the confidentiality of exchanged key material while in transit.

3.2 Web-Based Non-Resident Data Capability

This section describes a web-based capability to enable secure access to enterprise data and services from User Equipment. The web browser client is a single presentation layer that can attach to multiple existing enterprise services, with those services responsible for required authentication and authorization. Threshold requirements for the Web-Based Non-Resident Data Capability found in Appendix A and functional requirements in Appendix C must be met for the system to process classified data as a NSS.

3.2.1 Security-Relevant Components

The User Equipment uses a web browser that is configured to work within the existing VPN tunnel for the outer layer of encryption and the inner TLS tunnel to a web server residing in the Enterprise Mobility Infrastructure. Having a separate TLS tunnel provides a clean segregation between the web traffic and all other traffic to other client applications on the User Equipment. The web server provides an interface to Enterprise Network data without requiring the ability to store data on the User Equipment. The organization may choose to expose any data or applications (such as internal web sites, email, chat) that it wishes to the user, as long as the connection is through the web server and browser.

The following cryptographic protection is deployed as part of the Web-Based Non-Resident Data Capability.

- **TLS Connection:** For establishing the inner TLS tunnel, both the web server and the web browser on the User Equipment must be configured to support only TLS using Suite B cryptography. In particular, implementations must not allow Secure Sockets Layer (SSL) protocols (which have less security than TLS), nor unencrypted connections. Although mutual authentication in TLS with public key certificates is preferred, the web server may authorize users based on a USERID and password supplied in the TLS-protected session.

The following components are deployed as part of the Web-Based Non-Resident Data Capability.

- **Web Browser:** The web browser on the User Equipment is configured to prohibit the storing or caching of any data in non-volatile memory. Additionally, the web browser should be configured to access only specified web servers, authorized by the enterprise. This may be accomplished through server-side certificates or comparable mechanisms (such as IP white listing). Finally, the client (web browser) and the server (web server) perform mutual authentication.
- **Web Server:** The web server acts as the endpoint for TLS connections from User Equipment. It offers web-based application services directly to the User Equipment and may also act as a

gateway to other enterprise servers, such as an email server, which would provide web-based email services to User Equipment indirectly via the web server. If the web server authorizes users based on credentials supplied in the TLS-protected session, it may consult an AAA Server in the Enterprise Mobility Infrastructure for this user authentication/authorization. The enterprise web server must also be configured to require the user to re-authenticate to it no less than every 24 hours.

4 Access Networks

The Access Networks portion of this document discusses the methods and features that enable the User Equipment to interface with the Enterprise Mobility Infrastructure. Common access methods are cellular and Wi-Fi, though this release will focus exclusively on cellular services. Threshold requirements for Carrier Service Integration found in Appendix A must be met for the system to process classified data as a NSS. To assist DAOs, test criteria for Carrier Service Integration are found in Appendix B.6.

4.1 Cellular Services

This section describes the interactions between the Enterprise Mobility Infrastructure and a commercial cellular network. For this document's purposes, cellular networks consist of Radio Access Networks (RANs) using Code Division Multiple Access – 2000 (CDMA-2000), Universal Mobile Telephone Service (UMTS), High Speed Packet Access (HSPA)/Evolved HSPA or Long Term Evolution (LTE) connected to packet core networks. While the Enterprise Mobility solution tunnels through these networks, and the mobile devices rely on them for availability of data services, this section will not discuss the detailed functionality of the cellular networks.

The Enterprise Mobility architecture has little control of the cellular carrier services. It is advised that an integrator of an Enterprise Mobility implementation have expert knowledge in cellular systems in order to understand the system engineering issues, options, and tradeoffs.

The areas that will be discussed are

- connection between the cellular data network and the enterprise,
- service-level expectations of the carrier connection,
- mobile device dependencies on the carrier and User Equipment manufacturer, and
- disabling voice and SMS services.

4.1.1 Cellular to Enterprise Connection

Connections between the cellular carrier and the enterprise may be via a carrier's private network or over the public Internet. Using the carrier's private network is preferred, since the User Equipment need not expose a network interface to the Internet.

Not all carriers' RANs may be connectable to a carrier's private network. This is typically the case in roaming scenarios. In this case, it is necessary to use the Internet for the connection between the cellular provider and the enterprise. Since the user device will have an IP address routable over the Internet, the user device will require additional protections such as an internal firewall to protect against malicious traffic originating on the Internet.

4.1.2 Service-Level Expectations

LTE systems define different levels of QOS for different types of traffic. (For example, best effort for web traffic and guaranteed bit rate for streaming media.) The use of a single IPsec VPN for all traffic precludes differentiated treatment of traffic within the tunnel. An integrator should be aware of this issue and negotiate services with the carrier appropriately.

4.1.3 User Equipment Dependencies on Carrier and Manufacturer

The User Equipment contains the baseband processor, which is the signal processor to connect to theRAN. The baseband processor was built according to a wireless standard, such as GSM, UMTS, or LTE. The mobile device, and specifically the baseband processor, operates according to specifications set by the carrier.

The carrier, often in partnership with the manufacturer of the mobile device, has a deployed architecture to configure and manage the software for any mobile devices on the network. It is important for the integrator to understand the software update process employed by the carrier. It is also important to understand whether the software is cryptographically signed, whether that signature uses an approved cryptographic algorithm, and whether the user equipment verifies the signature on installation and/or boot.

4.1.4 Disabling Voice and SMS

The Enterprise Mobility architecture requires that the only commercial network service allowed for use by the User Equipment be the data connection that carries the tunneled encrypted sessions. Therefore, carrier-provided voice, SMS, and other value-added services should not be made available to the mobile client. While it is possible to purchase commercial mobile devices with just a "data plan", this does not mean that the cellular voice and SMS capabilities are not present, but rather that the carrier will bill differently for using them. It might be difficult or even impossible to completely disable the cellular voice functionality on a commercial mobile device, but it may be possible to disable user access to that functionality. The situation for SMS is similar. The desired outcome is that the device cannot use incoming or outgoing carrier voice services while the device is connected to the Enterprise. However, given the threat environment posed by SMS services, these functionalities should not be made available to the mobile client even when disconnected from the Enterprise. The device management capability should restrict the use of carrier services other than the data connection to the enterprise.

5 Enterprise Mobility Infrastructure

The Enterprise Mobility Infrastructure mediates the access of mobile devices to protected Enterprise Services. The Enterprise Mobility Infrastructure follows the principle of defense-in-depth by providing multiple layers of protection mechanisms and has responsibility for the following primary functions:

- **Networking & Enterprise Boundary Protection.** This includes the deployment of firewall and Intrusion Detection System/Intrusion Protection System (IDS/IPS) capabilities to protect the Enterprise from Access Networks.
- **Layered Data-In-Transit Protection.** Two layers of encryption are used across open Access Networks and authentication and authorization is an integral part of setting up an encrypted session with User Equipment.
- **Mobility Application Services.** Mobility-specific services are provided exclusively to mobile devices. An example is direct mobile-to-mobile routing of voice calls without relying on an intermediate network within the Enterprise.
- **Mobility Gateways.** These gateways mediate the exchange of information between User Equipment and resources within the Enterprise.
- **Provisioning and Management.** User Equipment and associated components within the Enterprise Mobility Infrastructure must be configured and provisioned with security credentials to enable secure operations.

Where used, components must be tested against the following PPs.

- [Draft] Protection Profile for Certificate Authority (CA)
- [Draft] Protection Profile for Intrusion Prevention Systems (IPS)
- [Final] Network Device (NDPP) Extended Package SIP Server
- [Final] Network Device (NDPP) Extended Package Stateful Traffic Filter Firewall
- [Final] Network Device (NDPP) Extended Package VPN Gateway
- [Final] Protection Profile for IPsec Virtual Private Network (VPN) Clients

5.1 Objective Enterprise Mobility Infrastructure Architecture

Figure 5-1 depicts a high-level view of the objective Enterprise Mobility Infrastructure architecture.

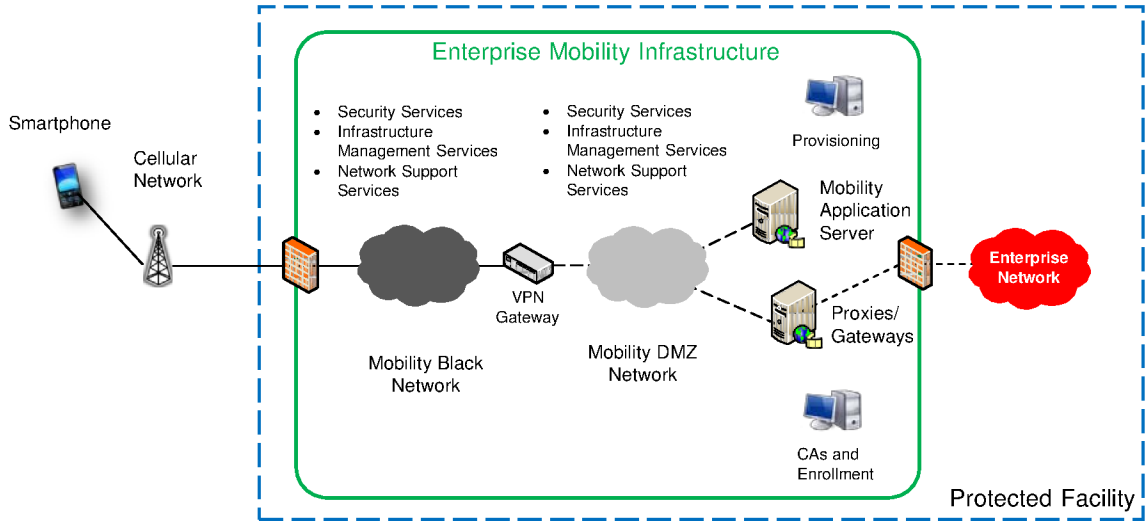

Figure 5-1. Objective Enterprise Mobility Infrastructure Architecture

The objective architecture supports either a standalone Enterprise Mobility Infrastructure serving a pilot set of mobile users or an infrastructure integrated with other existing Enterprise Services and supporting connection to other (non-mobile) users. The goal is full integration with Government Enterprise Services, networks, and infrastructure support. Implementations may initially be limited while capability development, policy, and certification for interconnection issues are addressed.

5.2 Prototype Enterprise Mobility Infrastructure Architecture

Figure 5-2 shows a more detailed view of a prototype Enterprise Mobility Infrastructure for SVoIP and Web-based Non-Resident Data services over a cellular Access Network.

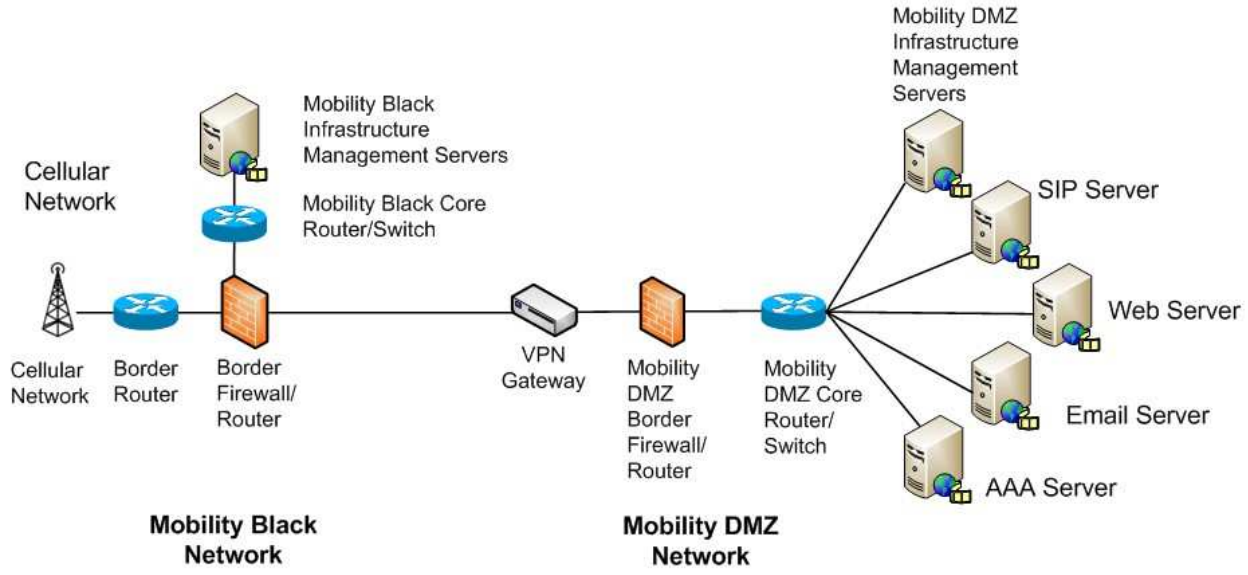

Figure 5-2. Enterprise Mobility Infrastructure Architecture

A brief description of the components follows with more detailed architecture and configuration requirements provided in Appendix A and functional requirements in Appendix BC. There are protection profiles for each class of product identified including routers, firewalls, VPN gateway, switches, SIP and other servers. Common Criteria labs must evaluate (for PP compliance) any products intended for use in a composed solution. Requirements specific to performance, scalability, availability, and reliability are not included within the component requirements in the appendices, but should be addressed as part of a given solution implementation.

5.2.1 Mobility Black Network Components

The following components are deployed as part of the Mobility Black Network which connects directly to the unclassified network.

- **Border Router:** The Border Router acts as the entry point to the Mobility Black Network from the carrier network. The router is configured to only allow IPsec/IKE traffic with the carrier network. The Border Router is required to perform Network Address Translation (NAT) unless

the cellular carrier is able to statically or dynamically assign IP black addresses to Government User Equipment from a private Government address space, and such an address space will be isolated from any other IP address spaces used by the carrier. Threshold requirements for the Infrastructure found in Appendix A.7 and functional requirements in Appendix C.6 must be met for the system to process classified data as a NSS. To assist the using agency's accrediting officials, test criteria for the Infrastructure are found in Appendix 0.

- **Border Firewall/Router:** The Border Firewall/Router supplements the Border Router in ensuring that only IPsec/IKE traffic is exchanged between the carrier network and the VPN Gateway. The Border Firewall/Router permits the exchange of non-IPsec/IKE traffic to and from the Mobility Black Core Switch Router for network management purposes. Threshold requirements for the Infrastructure found in Appendix A.7 and functional requirements in Appendix C.6 must be met for the system to process classified data as a NSS. To assist the using agency's accrediting officials, test criteria for the Infrastructure are found in Appendix 0.
- **Mobility Black Core Switch/Router:** The Mobility Black Core Switch/Router provides access to Mobility Black Network support services, which are described in Section 5.2.3.

5.2.2 Mobility Demilitarized Zone (DMZ) Network Components

The following components may be deployed as part of the Mobility DMZ Network, which is a bastion network between the Mobility Black Network and the Enterprise network.

- **VPN Gateway:** The VPN Gateway authenticates the User Equipment as part of establishing the IPsec encrypted session and authorizes access to the Mobility DMZ Network. The VPN Gateway uses IPsec in tunnel mode to protect the data stream and IKE with mutual public key certificate authentication with Suite B compliant cryptography. Although the use of Certificate Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP) is preferred for determining certificate validity, the VPN Gateway may use a preconfigured list ("white list") of authorized certificates and rely on the removal of invalid certificates from its white list. Threshold requirements for the VPN Gateway found in Appendix A and functional requirements in Appendix C must be met for the system to process classified data as a NSS. To assist the DAOs, test criteria for the VPN Capability are found in Appendix B.3.
- **SIP Server:** All secure mobile call requests are handled by SIP Server within the Enterprise Mobility Infrastructure. The SIP Server acts as a SIP Registrar/Proxy to provide device registration and coordination of calls between User Equipment. All SIP traffic with User Equipment is protected using TLS with Suite B compliant cryptography. When SDES-SRTP is used, the master session keys are exposed to the SIP Server and the server must be protected accordingly. Although mutual authentication in TLS with public key certificates is preferred, the SIP Server may authorize users based on a USERID and password supplied in the TLS-protected session. The SIP Server may consult an AAA Server on the Enterprise Mobility Infrastructure for this user authentication/authorization. More information on SVoIP capabilities may be found in Section 3.1. Threshold security requirements in Appendix A and functional requirements in Appendix C must be met for the system to process classified data as a National Security System. To assist the using DAOs, test criteria for the, test criteria for the SVoIP capability are found in Appendix 0.
- **Web Server:** The web server offers web-based application services directly to the User Equipment and also acts as a gateway to a separate email server. More information on Web-based Non-Resident Data capabilities may be found in Section 3.2. Threshold requirements in Appendix A and functional requirements in Appendix C must be met for the system to process

classified data as a NSS. To assist the using DAOs, test criteria for the web capability are found in Appendix 0.

- **Email Server:** The email server indirectly provides web-based email services to User Equipment via the web server. See Section 3.2 for more details on the Web-based Non-Resident Data capability.
- **AAA Server:** The AAA Server is responsible for performing authentication, authorization, and accounting on behalf of other components such as the VPN Gateway, SIP Server, and web server. These components are not required to use the AAA Server, but doing so may allow centralization of account management and reduction of effort. Threshold requirements for the Infrastructure found in Appendix A.7 and functional requirements in Appendix C.6 must be met for the system to process classified data as a NSS. To assist the using DAOs, test criteria for the Infrastructure are found in Appendix 0.
- **Mobility DMZ Border Firewall/Router:** The Mobility DMZ Network Border Firewall/Router controls access to the VPN tunnel. It only allows passage of SIP-over-TLS traffic to and from the SIP Server, and Hyper Text Transfer Protocol (HTTP)-over-TLS traffic to and from the Web Server. Mobile-to-mobile voice traffic, encoded using SRTP, is looped back by the VPN Gateway and never transits the Mobility DMZ Border Firewall/Router. Threshold requirements for the Infrastructure found in Appendix A.7 must be met for the system to process classified data as a National Security System. To assist the using agency's accrediting officials, test criteria for the Infrastructure are found in Appendix 0.
- **Mobility DMZ Core Switch/Router:** The Mobility DMZ Core Switch/Router provides access to Mobility DMZ Network applications and support services, which are as described in Section 5.2.3.
- **Mobile Device Management/Mobile Application Store services:** The MDM services manages policies to be enforced by the device management solution, and reports and alerts the state of compliance of managed devices to the enterprise network operations capability. The mobile application store makes approved and vetted applications available to mobile devices.

5.2.3 Infrastructure Management Services

Infrastructure Management Services components manage and monitor components in the Enterprise Mobility Infrastructure, but do not directly handle user data or manage User Equipment. The services provided by these components include network, host, and security (anti-virus, IDS/IPS, etc.) management, as well as monitoring and backups. Within each network, Infrastructure Management Services operate over their own Virtual Local Area Network (VLAN) to maintain logical separation between management and operational traffic. A managed component should be managed by the Infrastructure Management Services running on the network that matches the highest classification of data handled by the component.

The following components are independently deployed in both the Mobility Black Network and the Mobility DMZ Network:

- **Infrastructure AAA Service:** The Infrastructure AAA Service supports authentication and authorization of administrative users.
- **Intrusion Detection System (IDS):** The Mobility Black Network IDS passively monitors traffic from the carrier network to detect any signs of intrusion. The Mobility DMZ Network IDS passively monitors traffic exiting the VPN Gateway to detect any signs of intrusion.
- **Configuration Management Service:** This service provides a patch management solution for the Mobility infrastructure. The service is manually updated with approved patch sets, and infrastructure endpoint agents are queried for patch deployment on a pre-determined schedule.

Threshold requirements for the Infrastructure found in Appendix A.7 must be met for the system to process classified data as a National Security System. To assist the using agency's accrediting officials, test criteria for the Infrastructure are found in Appendix 0.

- **Host Service:** This service is responsible for the management and monitoring of host-based protection capabilities (anti-virus, host-based firewall, and host-based IDS) deployed on infrastructure components.
- **Networking Service:** This service is responsible for management and monitoring of networking hardware (switches and routers). This includes configuration of router access control and firewall policies. Threshold requirements for the Infrastructure found in Appendix A.7 must be met for the system to process classified data as a National Security System. To assist the using agency's accrediting officials, test criteria for the Infrastructure are found in Appendix 0.
- **Backup Service:** This service is used to back up infrastructure components, but not User Equipment.
- **Certificate Service:** This service is responsible for generating and processing certificates, specifically to: generate X.509 v3 format certificates; process PKCS #7 and #10 messages; generate device certificates and accept a common specified field (e.g., International Mobile Equipment Identity, IMEI) as part of the Distinguished Name for device certificates. To do this successfully it is necessary that an interoperability standard is developed by the using agency, ensuring that infrastructure generating and using PKI information implements a common certificate profile and a standard update process.

Additional network support services (such as Domain Name Service (DNS), Network Time Protocol (NTP) Servers, and Dynamic Host Configuration Protocol (DHCP) Servers) do not play a direct role in maintaining network security, but are essential for the operation of the network. As such, they will be properly configured and protected from unauthorized access.

5.2.4 Provisioning Components

Components (not depicted in Figure 5-2) that primarily provide provisioning functions include certificate and trust management systems, and capabilities used to configure and initialize User Equipment for secure operations. The following provisioning components are deployed in the Enterprise Mobility Infrastructure:

- **Outer (VPN) Certificate Authority and Enrollment Workstation:** The goal is to use Government Enterprise Public Key Infrastructures (PKIs) for the installation of root key certificates (trust anchors) and checking certificate validity. The Enterprise Mobility Infrastructure includes a Certificate Authority with an associated Enrollment Service for the issuance of device certificates to the VPN Gateway and to each User Equipment for use by the VPN client software. These certificates are used for mutual authentication when User Equipment establishes an IPsec association with the VPN Gateway using the Internet Key Exchange (IKE) protocol. Suite B compliant cryptography is to be used. Threshold requirements for the PKI components found in Appendix 0 and functional requirements in Appendix C must be met for the system to process classified data as a National Security System. To assist the using agency's accrediting officials, test criteria for the PKI components are found in Appendix B.10.
- **Inner (User) Certificate Authority and Enrollment Workstation:** The goal is to use Government PKIs for the installation of root key certificates (trust anchors) and checking certificate validity. The prototype Enterprise Mobility PKI Components includes a Certificate Authority with an associated Enrollment Service for the issuance of certificates to users and gateway systems or servers (such as the SIP Server and Web Server). These certificates are used for TLS authentication between a gateway/server and a client user. Suite B compliant cryptography is

to be used. Threshold requirements for the Infrastructure found in Appendix 0 and functional requirements in Appendix C must be met for the system to process classified data as a National Security System. To assist the using agency's accrediting officials, test criteria for the PKI components are found in Appendix B.10.

- **Provisioning Capability:** The provisioning capability will enable an authorized Systems Administrator to configure the User Equipment, install required applications, establish user accounts, register the device, and associate the device with the user. Threshold requirements for the Provisioning Capability found in Appendix A and functional requirements in Appendix C must be met for the system to process classified data as a National Security System. To assist the using accrediting officials, test criteria for the provisioning components are found in Appendix B.10.

6 Mobility Threats, Risks, and Mitigations

The use of cellular mobile devices, commercial carriers, layered commercial products, and voice and data services entails a number of risks to address. These risks include actions taken by an adversary or by an authorized user, under both malicious and accidental motivations. There are a number of ways to mitigate the risks posed to secure mobility, and most of them work in concert with one another. In particular, the Enterprise Mobility Infrastructure and existing Enterprise capabilities provide strong security features to protect the User Equipment and user traffic.

6.1 Risks

Some principal risks to be prevented or mitigated include:

- Exfiltration or monitoring (via Bluetooth, infrared, Wi-Fi, or other covert channels) of sensitive voice or data communications
- Malware and Advanced Persistent Threat (APT) on user equipment or within Enterprise Mobility Infrastructure, or other unauthorized modifications of user equipment or infrastructure components
- Sensitive data being stored unprotected on user equipment
- Loss of authentication credentials such as passwords or private keys for certificates
- Disruption of services
- Software flaws, out-of-date Operating Systems (OSes), and 3rd party firmware to gain access to device features that are locked by default
- Magnetic field induction – inductive coupling, threat from eavesdropping, improperly configured near-field configuration (NFC)
- Exposure of mobile phone number to prevent Vishing and Phishing
- Improper disposal of old cell phones with sensitive configurations and/or data
- Use of social media applications contrary to policy
- Excessive power consumption, battery drain DoS

6.2 Threats

Some principal threat areas to address are:

- Attacks on user equipment from rogue cellular systems or other users of the cellular carriers
- Unauthorized device modification, including changing the hardware or software of the User Equipment either remotely, with physical access, or within the supply chain
- Lost or stolen user equipment attempting to access the Enterprise Mobility Infrastructure or masquerade as authorized users
- Unauthorized users and devices attempting to access or disrupt the Enterprise Mobility Infrastructure
- Authorized equipment users attempting to misuse their privileges, such as by trying to use disallowed services/applications or trying to connect directly to commercial services
- Enterprise Mobility Infrastructure network operators attempting to misuse their privileges
- Untrusted apps stores that repackage versions of popular apps that include malware

The following recommended references that provide more information on threats to mobile security:

- Department of Homeland Security (DHS) Federal Mobile Security Reference Architecture
- US-CERT Technical Information Paper – TIP-10-105-01, Cyber Threats to Mobile Devices
- NIST Special Publication 800-124 “Guidelines on Cell Phone and PDA Security”

6.3 Mitigation Considerations

6.3.1 User Equipment

Current commercial smartphones and their operating systems and applications do not yet provide all the security mechanisms and levels of assurance that are desired; however, by limiting initial use to voice and non-resident data applications (reducing the need to securely store data), shutting off unneeded processes and interfaces (reducing threat exposure), adding monitoring and control capability, and controlling the allowed connectivity, the risks can be managed at the User Equipment end.

- Mobile devices provide a unique opportunity for an adversary to target individual users. Remote attacks against the User Equipment, other than via the carrier network, are limited by closing down a number of potential ingress paths (such as Wi-Fi or Bluetooth) via the device configuration and monitoring services. Stealing or modifying user equipment would seem to be an attractive attack plan since user credentials are stored on the device and both layers of encryption terminate on the device. However, the level of effort required by an adversary to attack a single User Equipment may not be worth it unless the targeted user is of particularly high value.
- It is important to note that the only security critical information stored on the User Equipment is limited to the credentials used for authentication to the VPN Gateway, SIP Server, and Web Server. An adversary who recovers a user equipment – even an active one – does not obtain any information that would help the attacker decrypt any past voice or data communications. Since the device is only used for voice and non-resident data applications, there is also no sensitive data (documents, email, etc.) stored on the User Equipment.
- See CNSSD 505 Supply Chain Risk Management (SCRM) for additional guidance on reducing supply chain risk.
- In the event that an adversary acquires an active User Equipment that was lost or stolen, that adversary would be able to access the organization's network or impersonate a user for some period of time (without modifying the mobile device in any way), until either the user reports the device as lost (at which time certificate revocation will prevent any future network access) or the system requires re-authentication (which the adversary might not be able to provide). Loss reporting responsiveness is critical.
- The credentials on the User Equipment would allow the adversary to connect to the VPN Gateway in the Enterprise Mobility Infrastructure; this access into the network can allow the adversary to try to send traffic of his choosing further into the network in order to attempt to attack infrastructure components, or to send data to other User Equipment in order to attempt to attack them. Again, the adversary would not obtain any information that would help the adversary decrypt any past voice or data communications.
- An adversary who obtains temporary possession of User Equipment could attempt to modify it and return it to the user. Although additional endpoint hardening (i.e., tamper detection) provides some assurance that the user equipment has not been physically modified, some attempts by the adversary to modify the device may not be detected if it were returned to the user. An adversary with physical access to the User Equipment may want to delete existing software and/or install malicious code on the device. In initial deployments, the User Equipment is configured to disallow the installation of any software except at initial

provisioning; later deployments will include Device Management Services that should detect these changes. If an adversary were to succeed, he could expose calls to and from that particular User Equipment, exfiltrate audio in the proximity of the device, exfiltrate data, or attempt to attack the internal network (as above).

- Monitoring provides indicators of the operational status and health of the User Equipment.

Other mitigations include stronger vigilance/control of User Equipment to limit their exposure to adversaries, use of Device Management Services in order to detect software or configuration changes and do updates, more rigorous provisioning methods, and spot-checking of devices in order to circumvent supply chain threats.

6.3.2 Enterprise Mobility Infrastructure

The Enterprise Mobility Infrastructure and existing enterprise capabilities provide strong security features to protect the User Equipment and user traffic. These compensate for the lack of strong security on the User Equipment and allow the use of commercial devices, software, and Access Networks. Layered security services (encryption, authentication, authorization, boundary protection) protect both the enterprise resources and the mobile users from the majority of external threats.

- In order to prevent unauthorized devices from accessing the Enterprise Mobility Infrastructure networks and services, the VPN Gateway authenticates the Government provisioned identification of the device (PKI credentials) and checks that the device is authorized. The SIP Server and Web Server also independently check that the user is authorized.
- Techniques such as periodic re-authentication, inactivity timeouts, and loss reporting responsiveness help limit the potential damage from lost or stolen devices.
- Since Mobile Applications come from a variety of sources potentially of unknown provenance, validation of mobile applications should be considered a potential mitigation for implementation within the Enterprise.

Monitoring and auditing can provide indicators of the operational status and health of mobility operations. Denial of service due to malicious insider actions, unintentional actions, and system failures could be detected by monitoring systems, resulting in notifications to multiple operators.

6.3.3 Cellular Carrier Networks

A commercial cellular Access Network is a very large attack surface that could potentially attempt to access Government resources. The first lines of defense that can be provided by a commercial cellular Access Network include: only authenticated authorized devices and only data traffic are routed to the Government, the IP address of the entrance point to the Enterprise Mobility Infrastructure is not publicized, and the carrier interface controls what data is passed.

The rogue base station threat could be mitigated through use of mutual authentication in the cellular radio network.

Appendix A Architecture and Configuration - Enterprise Mobility Requirements

This appendix contains requirements applicable to Enterprise Mobility components. This does not include Enterprise Services; hence no requirements are identified for fixed devices and external gateways. The requirement priorities are specified based on guidance contained in the Defense Acquisition Guidebook. Based on this guidance, the "Threshold or Objective" column in each table means the following:

- An objective (O) requirement specifies a feature or function that the Government desires and expects.
- A threshold (T) requirement specifies a minimum acceptable feature or function that, in the Government's judgment, still provides the needed capabilities if the corresponding objective requirement cannot reasonably be met (e.g., due to lack of technology maturity, cost or time constraints).

In many cases, the threshold requirement also serves as the objective requirement (T=O). Where both a Threshold requirement and a related Objective requirement exist, the Objective requirement complements the Threshold requirement rather than replaces it. Several different kinds of requirements are provided: Architectural, Functional, and Configuration Guidance. Each requirement is intended to be testable, resulting in a yes/no answer of whether the requirement was met. The security functional requirements in this appendix were designed to create a high level of assurance without referencing the NIST SP 800-53 control set (revision 4). However, there are a number of requirements which meet, partially meet, or enhance NIST 800-53 controls and enhancements. A mapping is provided for convenience. This mapping is not complete and is subject to future modifications.

Table 2: Appendix A Requirement Designators

Designator	Requirements Addressed
BSP	Requirements for **B**asic **S**ecurity **P**olicy
CAR	**C**lient **A**pplication **R**equirements
CSI	Requirements for **C**arrier **S**ervice **I**ntegration
ECA	Requirements for **E**lectronic **C**ertificate **A**uthority
EWS	Requirements for **E**nrollment **W**ork**S**tation operation
HRT	Requirements for **H**ardware **R**oot of **T**rust
IFA	Requirements for **I**n**F**rastructure host **A**rchitecture
IFB	Requirements for **I**n**F**rastructure host **B**oundary protection
IFH	Requirements for **I**n**F**rastructure **H**ost systems
IFM	Requirements for **I**n**F**rastructure host **M**anagement
IFN	Requirements for **I**n**F**rastructure host **N**etworking
IFS	Requirements for **I**n**F**rastructure host **S**ecurity services
MOB	Overarching **MOB**ility requirements that solutions fielded using this MSG should implement
PSS	Requirements for **P**rotected **S**torage **S**ervices
SVP	Requirements for the overall **SV**o**I**P infrastructure
SVS	Requirements for the **SV**oIP and SIP **S**ervers

Designator	Requirements Addressed
UEA	Requirements for the **U**ser **E**quipment **A**udit, monitoring and fault handling
UEP	Requirements for **U**ser **E**quipment **P**rovisioning
UES	Overall requirements for configuring the **U**ser **E**quipment, **Smartphone**
VPG	Requirements applicable to the **VPN Gateway**
VPN	Requirements for designing and implementing the **VPN** solution
WNC	**W**eb Arbitrated **N**on-Resident Data User Equipment **C**lient requirements
WND	**W**eb Arbitrated **N**on-Resident **D**ata
WNS	**W**eb Arbitrated **N**on-Resident Data **S**erver requirements

A.1 Overarching Solution Requirements

Table 3: Overarching Mobility Requirements

Requirement Number	Requirement Description	Threshold/ Objective	Architecture/ Configuration / Guidance (A/C/G)	NIST 800-53 Control Mapping
MOB.00	**Overarching Mobility Requirements**			
MOB.01	All network traffic across an untrusted transport medium shall be protected by a minimum of two layers of encryption.	T=O	A	IA7, SC11, SC13, SC8(1/2), SC9(3)
MOB.02	The Mobility components providing the outer layer of encryption and inner layer of encryption shall use non-proprietary standards based protocols.	T=O	A	SC29, SC27
MOB.03	Products for each layer of network encryption shall be from different vendors.	T=O	A	SA12(5), SC37(1), SC29
MOB.04	The software for each layer of network encryption shall not use the same software cryptographic libraries or depend on the same services.	T=O	A	SA12(5), SC37(1), SC29
MOB.05	The Mobility components providing the outer layer of encryption and inner layer of encryption in the Enterprise Mobility Infrastructure shall be run on separate hardware platforms.	T=O	A	SA12(5), SC37(1), SC29

Requirement Number	Requirement Description	Threshold/ Objective	Architecture/ Configuration / Guidance (A/C/G)	NIST 800-53 Control Mapping
MOB.06	The Mobility components providing the outer layer of encryption and inner layer of encryption in the Enterprise Mobility Infrastructure shall not utilize the same OS for critical IA security functionality. Differences between Service Packs (SP) and version numbers for a particular vendor's OS do not provide adequate diversity.	T=O	A	SA12(5), SC37(1), SC29
MOB.07	Each layer of cryptography protecting network traffic across an untrusted transport medium shall be of sufficient strength to protect the highest classification of the data in accordance with CNSSP-15.	T=O	A	SA13(2)
MOB.08	Every device/component shall be issued unique certificates and corresponding private keys for authentication.	T=O	A	AC4(13), SC17, IA5, IA3
MOB.09	The authentication certificates for each layer of network encryption shall be issued by different Certificate Authorities.	T=O	A	SA12(5), SC29
MOB.10	All components of the system shall have been approved via National Information Assurance Partnership (NIAP) and NSA's Commercial Solutions for Classified	T=O	A	SA14
MOB.11	If single factor authentication is used (e.g., password, passphrase, or PIN), then at least two independent user authentication steps shall be required to enable classified access. (i.e., two steps may be device unlock and password to decrypt stored keys and certificates).	T	A	IA4, IA5
MOB.12	All cryptographic algorithms shall conform to the Suite B standard or the Suite B transitional standard as documented in CNSSP-15.	T	A	SC8, SC9
MOB.13	All cryptographic algorithms shall conform to the full Suite B standard as documented in CNSSP-15.	O	A	SC8, SC9

Requirement Number	Requirement Description	Threshold/ Objective	Architecture/ Configuration / Guidance (A/C/G)	NIST 800-53 Control Mapping
MOB.14	Each system shall be configured to protect certificates along with their corresponding private keys and security critical profiles stored on the system in accordance with protection guidance for the highest level of classification of the system.	T=O	C	SC12
MOB.15	All systems and services shall be configured in accordance with NIST 800-53, applicable DoD guidance, or applicable using-agency guidance except where configuration requirements in this document state differently	T=O	C	SC1
MOB.16	The using agency will develop and use a Certification Practice Statement (CPS) that will include information required by applicable DoD or using agency guidance and the requirements enumerated in this document	T=O	C	(RFC3647)

A.2 VPN Requirements

Table 4: VPN Requirements

Requirement Number	Requirement Description	Threshold/ Objective	Architecture/ Configuration / Guidance (A/C/G)	NIST 800-53 Control Mapping
VPN.00	**Overarching VPN Requirements**			
VPN.01	The VPN shall be a standards-based IPsec solution.	T=O	A	
VPN.02	The VPN Gateway and client shall use IPsec in tunnel-mode.	T=O	A	SC7, AC4
VPN.03	*Depreciated into VPN.04*			
VPN.04	The VPN Gateway and client shall use IKEv2.	T=O	A	SC7, AC4
VPN.05	The VPN Gateway and client shall be configured to use the cipher suites specified in IETF RFC 6380 “Suite B Profile for Internet Protocol Security (IPsec)”	T=O	C	SC8, SC9
VPN.06	The VPN Gateway and client shall be configured to prohibit split-tunneling.	T=O	C	SC7(7)

Requirement Number	Requirement Description	Threshold/ Objective	Architecture/ Configuration / Guidance (A/C/G)	NIST 800-53 Control Mapping
VPN.07	The VPN Gateway and client shall be configured to maintain the tunnel even if applications are not transmitting data.	O	C	SC7, AC4
VPN.08	The VPN client shall automatically reconnect the VPN upon unexpected disconnect.	O	A	SC11
VPG.00	**VPN Gateway Requirements**			
VPG.01	The VPN Gateway shall audit and report all unsuccessful attempts to establish a security association.	T=O	C	AU2, AU3, SI4
VPG.02	The VPN Gateway shall audit and report successful attempts to establish a security association in accordance with applicable DoD or using agency guidance	T=O	C	AU2, AU3, SI4
VPG.03	The VPN Gateway shall audit and report all integrity check failures.	T=O	C	AU2, AU3, SI4
VPG.04	The VPN Gateway shall be configured in accordance with applicable DoD or using organization guidance.	T=O	C	SC1
VPG.05	The VPN Gateway shall be configured to assign an internal network private IP address to a VPN client upon successful establishment of a security association.	T=O	C	SC7
VPG.06	The VPN Gateway shall be configured to request re-authentication for security associations that have been inactive for a configurable period of time.	T=O	C	SC7, AC4
VPG.07	The VPN Gateway shall be configured to terminate security associations that have been inactive for a configurable period of time.	T=O	C	SC7, AC4
VPG.08	The VPN Gateway shall perform certificate path validation.	T=O	C	IA5, AC4, SC11
VPG.09	The VPN Gateway shall check for revoked certificates.	T=O	C	IA5, AC4, SC11
VPG.10	The VPN Gateway shall check for invalid certificates.	T=O	C	IA5, AC4, SC11
VPG.11	The VPN Gateway shall be configured to consult an external white or black list to authorize certificates presented by the User Equipment client before access to the protected network is granted	T	C	AI5

Requirement Number	Requirement Description	Threshold/ Objective	Architecture/ Configuration / Guidance (A/C/G)	NIST 800-53 Control Mapping
VPG.12	The VPN Gateway shall be configured to use OCSP or equivalent to authorize certificates presented by the User Equipment client before access to the protected network is granted	O	C	IA5, AC4

A.3 Secure Voice over Internet Protocol (SVoIP) Requirements

Table 5: SVoIP Requirements

Requirement Number	Requirement Description	Threshold/ Objective	Architecture/ Configuration/ Guidance (A/C/G)	NIST 800-53 Control Mapping
SVP.00	**Overarching SVoIP Requirements**			
SVP.01	The Enterprise Mobility Solutions shall use the Suite B cryptosuite.	T=O	A	SC8, SC9
SVP.02	The User Equipment SVoIP Client and Mobility SIP Server shall use SIP over TLS for registration of the User Equipment, call setup, and call termination.	T=O	A	SC11
SVP.03	The User Equipment SVoIP Client shall use the SDES-SRTP Protocol.	T=O	A	SC11
SVP.04	The Enterprise Mobility System shall provide the capability for User Equipment to communicate with another User Equipment operating at the same classification level in the same enterprise.	T=O	A	SC11, AC4
SVP.05	The Enterprise Mobility System shall provide the capability for User Equipment to communicate with another User Equipment operating at the same classification level but in a different enterprise.	O	A	SC11, AC4
SVP.06	The Enterprise Mobility System shall provide the capability for User Equipment to communicate with fixed enterprise VoIP devices operating at the same classification level.	O	A	SC11, AC4

Requirement Number	Requirement Description	Threshold/ Objective	Architecture/ Configuration/ Guidance (A/C/G)	NIST 800-53 Control Mapping
SVP.07	The Enterprise Mobility System, in conjunction with the existing Enterprise Gateways, shall provide the capability for User Equipment to communicate with devices operating on non-IP networks at the same classification level.	O	A	SC11, AC4
SVP.08	Within the Enterprise Mobility System, the User Equipment SVoIP client and Mobility SIP Server shall perform mutual public key authentication using only the keys and certificates issued by the designated SVoIP Certificate Authority.	T=O	C	SC11, AC4, IA5
SVP.09	The Enterprise Mobility Solution shall use the SRTP Protocol in compliance with IETF RFC 3711 "Secure Real-Time Transport Protocol" to transmit secure voice traffic. Within the Enterprise Mobility System, the User Equipment shall use SRTP and SRTCP to transmit secure voice traffic.	T=O	C	SC11
SVP.10	The Enterprise Mobility System and User Equipment client shall be configured to use a password for client authentication for SIP REGISTER function requests.	T=O	C	SC23, IA2, IA5, SA4
SVP.11	The Enterprise Mobility System shall be configured to automatically notify the operator of User Equipment of the highest level classification supported by the connection to another device.	O	C	AC4(13), AC3, AC21, AC4(20)
SVS.00	**SVoIP Server Requirements**			
SVS.01	The Enterprise Mobility System shall be able to interface to a SIP Trunking Gateway that enables voices calls between User Equipment authorized to operate at the unclassified level and an unsecured VoIP device accessible via an external IP network. (Note: This includes packet-switched cellular voice communications.)	T=O	A	AC21
SVS.02	The SVoIP Server shall be configured to have two User Equipment send SRTP traffic directly to one another via the Enterprise Mobility Infrastructure network and their respective VPN Gateway tunnels, instead of having them use the SVoIP	T=O	C	AC4(8)

Requirement Number	Requirement Description	Threshold/ Objective	Architecture/ Configuration/ Guidance (A/C/G)	NIST 800-53 Control Mapping
	Server as an intermediary.			
SVS.03	The Mobility SIP Server in the “home” enterprise and the Mobility SIP Server in the far-end enterprise shall exchange the caller IDs of the User Equipment.	T=O	C	IA3
SVS.04	For communication between User Equipment and a fixed enterprise VoIP device, the Mobility SIP Server and Secure Voice Gateway shall use SIP over TLS for transmitting call setup and call termination messages used by the User Equipment.	T=O	C	IA3, SC11
SVS.05	For communication between User Equipment and a fixed enterprise VoIP device, the User Equipment and Secure Voice Gateway shall use SRTP and Secure Real Time Control Protocol (SRTCP) to transmit secure voice traffic.	T=O	C	SC11, AC4
SVS.06	For communication between User Equipment and a fixed enterprise VoIP device, the Secure Voice Gateway shall exchange the caller ID of the User Equipment and Fixed VoIP Device between the Mobility SIP Server and the Enterprise SIP Server and vice versa.	T=O	C	SC11, IA3, AC4
SVS.07	The SIP Server shall be configured to securely contain a unique public key certificate and corresponding private key, which will be used to provide authentication of the SIP Server to the user equipment, in order to establish the TLS channel for SIP messages.	T=O	C	IA5, AC4

A.4 Web Based Non-Resident Data Requirements

Table 6: Web Based Non-Resident Data Requirements

Requirement Number	Requirement Description	Threshold/ Objective	Architecture/ Configuration / Guidance (A/C/G)	NIST 800-53 Control Mapping
WND.00	**Overarching Web Browser Non-Resident Data Requirements**			
WND.01	The inner TLS tunnel shall be used for all traffic between the web browser and the web server.	T=O	A	AC3, SC3(6)
WND.02	The web browser shall be included in any permitted applications white list.	T=O	A	CM2, CM6
WND.03	The web browser shall be able to pass user identity certificates as application credentials.	O	C	IA5, IA9, IA11
WNC.00	**Web Browser Non-Resident Data Client Requirements**			
WNC.01	The web browser shall be configured to disallow the storing of any data in non-volatile memory.	T=O	C	AC19(6), AC3
WNC.02	The web browser shall be configured to connect to only authorized web servers.	T=O	C	CM2, CM6
WNC.03	The web browser shall be configured to use the existing outer VPN tunnel for network access.	T=O	C	SC11
WNC.04	The web browser shall be configured to disable any encryption protocol that is not Suite B compliant.	T=O	C	SC8, SC9
WNC.05	Web browser history shall only be maintained in volatile memory on the User Equipment.	T=O	C	AC19(6), AC3
WNC.06	The web browser shall be configured to disable the use of all versions of the Secure Sockets Layer (SSL) protocol.	T=O	C	SC8, SC9
WNC.07	The web browser shall use a Suite B compliant Transport Layer Security (TLS) protocol 1.2 or later.	T=O	C	SC8, SC9
WNC.08	The web browser shall disable all browser plug-ins, extensions, and other third party software that has not specifically been approved for use by the DAO.	T=O	C	CM2, CM6
WNC.09	The web browser on the User Equipment shall be configured to require the user to authenticate to the web server at least every 24 hours.	T=O	C	IA12

Requirement Number	Requirement Description	Threshold/ Objective	Architecture/ Configuration / Guidance (A/C/G)	NIST 800-53 Control Mapping
WNS.00	**Web Browser Non-Resident Data Server Requirements**			
WNS.01	The web server shall be configured to allow only TLS and Suite B cryptosuite options	T=O	A	SC8, SC9
WNS.02	The web server shall be configured to reject SSL encryption handshakes	T=O	C	SC8, SC9
WNS.03	The web server shall be able to re-authenticate user equipment.	O	C	IA3, IA5, IA12
WNS.04	The web server shall be able to be configured to use user identity certificates to authenticate users.	O	C	IA5, AC4

A.5 Carrier Service Integration

Table 7: Carrier Service Integration Requirements

Requirement Number	Requirement Description	Threshold/ Objective	Architecture/ Configuration/ Guidance (A/C/G)	NIST 800-53 Control Mapping
CSI.00	**Carrier Service Integration**			
CSI.01	The Enterprise Mobility Infrastructure Integrator shall negotiate with the carrier QoS of IPsec VPN traffic from/to user equipment providing users with the lowest amount of network latency that is cost effective	T=O	A	
CSI.02	The using agency shall be cognizant of supply chain compromise attacks and build contingency plans in response	T=O	A	SA12, CP1
CSI.03	The using agency shall be cognizant of rogue carrier threats and build contingency plans in response	T=O	A	CP1, RA1, RA3
CSI.04	The Enterprise Mobility Infrastructure Integrator shall use Suite B compliant cryptosuites	T=O	C	SC8, SC9
CSI.05	The Enterprise Mobility Infrastructure shall have a documented plan to detect and mitigate rogue base stations	T=O	C	SI4(14)

A.6 User Equipment Requirements

Table 8: User Equipment Requirements

Requirement Number	Requirement Description	Threshold/ Objective	Architecture/ Configuration / Guidance (A/C/G)	NIST 800-53 Control Mapping
UES.00	**Smartphone User Equipment Requirements**			
UES.01	The User Equipment shall provide a hardware root of trust, trusted boot, and attestation that interoperates with the infrastructure to support remote assessment of integrity and compliance status.	O	A	SA12, SI4, CM2, AC16(8)
UES.02	The User Equipment screen lock password shall be configured for length and complexity in according with DoD or using agency policy on mobile security.	T=O	C	AC11, IA5, CA1, RA5, SA4, AT1?
UES.03	*Withdrawn*			
UES.04	The User Equipment shall be configured to allow the Universal Serial Bus (USB) cable to be used only to charge the device.	T=O	C	AC11, PE20, SC18, MP7
UES.05	The User Equipment shall be configured to disable processing of incoming cellular messaging services.	T=O	C	SC11, CM7, SI4(11), MP5, MP7, SC7(19)
UES.06	*Withdrawn*			
UES.07	*Withdrawn*			
UES.08	*Withdrawn*			
UES.09	*Withdrawn*			
UES.10	The User Equipment shall be configured to disable Bluetooth.	T=O	C	CM7, SI4(11), AC18,MP7
UES.11	The User Equipment shall be configured to disable Wireless-Fidelity (Wi-Fi).	T=O	C	CM7, MP7, SC5(1), SI4(11), AC18(3)
UES.12	*Withdrawn*			
UES.13	*Withdrawn*			
UES.14	*Withdrawn*			
UES.15	The User Equipment shall be configured to disable all transmitted Global Positioning System (GPS) and location services except Enhanced 9-1-1 (E911) or those authorized by the DAO.	T=O	C	CM7, CM6, MP7
UES.16	*Withdrawn*			
UES.17	*Withdrawn*			

Requirement Number	Requirement Description	Threshold/ Objective	Architecture/ Configuration / Guidance (A/C/G)	NIST 800-53 Control Mapping
UES.18	*Withdrawn*			
UES.19	*Withdrawn*			
UES.20	*Withdrawn*			
UES.21	*Withdrawn*			
UES.22	*Withdrawn*			
UES.23	*Withdrawn*			
UES.24	*Withdrawn*			
PSS	**Protected Storage Services**			
PSS.1	A device shall have the capability to allow multiple authentication and authorization factors (including device integrity evidence) in combination to govern use of a DEK or KEK	T	A	SC12, SC13
CAR	**Client Application Requirements**			
CAR.1	The email client shall employ Secure/Multipurpose Internet Mail Extensions (S/MIME)	T	C	IA5(11)
CAR.2	The email client shall meet all key protection requirements in the [final] MD F PP, otherwise specified in this MSG, and shall adhere to FIPS 140-2 Level1	T	C	SC13
CAR.3	The email client shall employ TLS Mutual Authentication (for user certificate verification)	T	C	IA2, IA3(2)
CAR.4	All DAR layers (application provided or native) must meet the DAR requirements in the [final] MD F PP	T	A	AC19
CAR.5	If the email client is a thin client – all enterprise data (for example, temporary files, history, etc. shall only be saved to RAM	T	C	AC19
CAR.6	If the email client is a thick client – the application must provide a DAR layer independent of the platform DAR layer	T	A	AC19
CAR.7	If the email client is a thick client – the application must meet the Application PP (in progress)	T	A	AC19
CAR.8	If the email client is a thick client – the application must meet all isolation requirements in the MD F PP	T	A	AC19

BSP	Basic Security Policy			
BSP.1	The User Equipment shall employ physical tamper protection that is visually inspectable by the user	O	A	PE3(5), SA18, SA19, AC19(9), MP7,
BSP.2	The User Equipment shall prevent Over the Air (OTA) software/firmware updates from non-authorized sources	T	C	PL9, AC19, CM7, SI2, AC3, MA1, MP7
BSP.3	The User Equipment shall employ active electronic/logical tamper indicating technology	O	A	SA18, MP7, AC19(9), PE3(5), SA19
BSP.4	The User Equipment shall be configured to disable Over the Air (OTA) carrier commands that are not required for the phone to access the carrier network.	O	C	AC19, CM7, SI2, AC3, MA1, MP7
BSP.5	The User Equipment shall be configurable to trigger a wipe process	T	C	PS4, MP8, DM2, SC4, AC19, SI4
HRT	**Hardware Root of Trust[1]**			
HRT.1	The User Equipment shall generate integrity measurements of critical software prior to execution and on demand	T	A	AC19, AC16(8)
HRT.2	The User Equipment shall provide protected storage and authorized access to and use of critical integrity measurements for enterprise assertions[2]	T	C	AC19, AC16(8)
HRT.3	The User Equipment shall provide identity information rooted in hardware to enable authentic and non-repudiable enterprise assertions	T	A	AC19, AC16(8)

[1] Hardware Root of Trust requirements listed in this section are intended to be part of a set of recommendations eventually included in NIST SP 800-164. When NIST SP 800-164 recommendations are finalized, they will be included in this Mobility Security Guide by reference.

[2] Protection Profile requirements are interpreted to require CNSSP 15 approved algorithms for integrity measurements, digital signature verification, authenticity, and verification functions. Therefore all hardware root of trust functions will be expected to meet CNSSP 15 standards.

UEA.00	User Equipment Monitoring Service Requirements			
UEA.01	*Withdrawn*			
UEA.02	*Withdrawn*			
UEA.03	*Withdrawn*			
UEA.04	*Withdrawn*			
UEA.05	*Withdrawn*			
UEA.06	*Withdrawn*			
UEA.07	*Withdrawn*			
UEA.08	*Withdrawn*			
UEA.09	*Withdrawn*			
UEA.10	*Withdrawn*			
UEA.11	*Withdrawn*			
UEA.12	*Withdrawn*			
UEA.13	*Withdrawn*			
UEA.14	*Withdrawn*			
UEA.15	*Withdrawn*			
UEA.16	*Withdrawn*			
UEA.17	The User Equipment shall adhere to [final] PP for MD F Requirement[3] FTP_TST_EXT.2.1 (INT-5)	T	A	AC16(8), CM6
UEA.18	The User Equipment shall alert the MDM Agent following [final] PP for MD F Requirement FPT_NOT_EXT.1.1 when a TSF software integrity verification failure has occurred.	T	C	
UEA.19	The MDM Agent shall transmit alert to the MDM Server under [draft] MDM PP FAU_ALT_EXT.1.1 Assignment: “Transmit all critical software integrity measurements”.	T	C	
UEA.20	The MDM Agent shall query the operating system using [draft] MDM PP FMT_SMF.1(2) Assignment: “Query integrity of critical software”.	T	C	
UEA.21	The MDM Server shall submit a request to the MDM Agent using [draft] MDM PP FMT_SMF.1.1(1) Assignment: “Query integrity of critical software”.	T	C	
UEA.22	*Withdrawn*			
UEA.23	*Withdrawn*			

[3] This requirement (both for boot verification and for integrity checking for AP and BP software/firmware) reflects the spirit of requirements expected to be included in NIST SP 800-164 at some future date. Adherence to NIST SP 800-164 as well as all applicable PPs, is a requirement of this security guide.

UEA.24	The device shall alert on and log any attempt to circumvent [final] PP for MD F Requirement FDP_IFC_EXT.1.1 (IFC-1) as represented in UEA.28	O	C	CA3
UEA.25	*Withdrawn*			
UEA.26	*Withdrawn*			
UEA.27	The device shall provide the user and administrator with the ability to view the public parts of any certificates stored on the device	T=O	C	SC17
UEA.28	The User Equipment shall adhere to [final] PP for MD F Requirement FDP_IFC_EXT.1.1 (IFC-1)	T	C	CA3

A.7 Enterprise Mobility Infrastructure Requirements

Table 9: Infrastructure Requirements

Requirement Number	Requirement Description	Threshold/ Objective	Architecture/ Configuration/ Guidance (A/C/G)	NIST 800-53 Control Mapping
IFB.00	**Enterprise Mobility Infrastructure Boundary Protection Requirements**			
IFB.01	The Enterprise Mobility Infrastructure shall implement Border Routers at public network boundaries to perform network address translation (NAT).	T=O	A	IA11, CA3, SC2, SC3, SC20, SC7
IFB.02	The Enterprise Mobility Infrastructure shall implement Network IDS/IPS in accordance with applicable DoD or using agency policy and guidance.	T=O	A	CM6, SA18, SC26
IFB.03	The Enterprise Mobility Infrastructure shall implement Network Firewalls in accordance with applicable Department of Defense (DoD) or using agency policy and guidance.	T=O	A	SC7, AC4, SA18
IFH.00	**Enterprise Mobility Infrastructure Host Systems Requirements**			
IFH.01	Each host system in the Enterprise Mobility Infrastructure shall report platform status in accordance with applicable DoD or using agency policy and guidance.	T=O	C	SI2, CA7
IFH.02	An Infrastructure Host System shall authenticate users in accordance with applicable DoD or using agency policy and guidance.	T=O	C	IA6, SC23, IA2, AC14, IA5
IFH.03	An Infrastructure Host System shall prohibit unauthorized users from accessing resources.	T=O	C	AC14

Requirement Number	Requirement Description	Threshold/ Objective	Architecture/ Configuration/ Guidance (A/C/G)	NIST 800-53 Control Mapping
IFH.04	An Infrastructure Host System shall maintain separation of user roles.	T=O	C	IA11, PL4, AC5, SC4
IFH.05	An Infrastructure Host System shall audit actions taken by users (types of actions and content of audit record are configurable) in accordance with applicable DoD or using agency policy and guidance.	T=O	C	AU1, AU2, AU3, SI4, AU5, AU6, AU13
IFH.06	An Infrastructure Host System shall perform anti-malware detection or have an anti-malware service installed and configured in accordance with applicable DoD or using agency policy and guidance.	T=O	C	SC38, SI3, SI2
IFH.07	An Infrastructure Host System shall have a host-based firewall installed and configured in accordance with applicable DoD or using agency policy and guidance.	T=O	C	IR4, CA3, SI3
IFH.08	An Infrastructure Host System shall have a host-based IDS/IPS installed and configured in accordance with applicable DoD or using agency policy and guidance.	T=O	C	CM6, SA18, SC26
IFH.09	An Infrastructure Host System shall verify the integrity of its software environment.	T	C	SI1-SI7
IFH.10	An Infrastructure Host System shall implement hardware roots of trust for performing integrity verification and reporting (attestation).	O	C	SA10(3), SA12, SA14
IFM.00	**Enterprise Mobility Infrastructure Management Requirements**			
IFM.01	The Enterprise Mobility Infrastructure Management Services shall provide scheduled virus signature updates automatically to infrastructure components running anti-virus software in accordance with applicable DoD or using agency policy and guidance.	T=O	A	SI2, SI3
IFM.02	The Enterprise Mobility Infrastructure Management Services shall be configured to receive, authenticate, and validate software updates received indirectly via the Internet (e.g., via the Internet Download Server) or directly from applicable vendors in accordance with applicable DoD or using agency policy and guidance.	T=O	A	CM11, CM5, SI3, SI2

Requirement Number	Requirement Description	Threshold/ Objective	Architecture/ Configuration/ Guidance (A/C/G)	NIST 800-53 Control Mapping
IFM.03	The Enterprise Mobility Infrastructure Management Services shall track the Configuration Management status of infrastructure components in accordance with applicable DoD or using agency policy and guidance.	T=O	A	CM2, CM6, CM8, CM9
IFM.04	The Enterprise Mobility Infrastructure Management Services shall provide scheduled intrusion detection signature updates automatically to infrastructure components running host-based IDS/IPS software in accordance with applicable DoD or using agency policy and guidance.	T=O	A	CM6, SA18, SC26
IFM.05	The Enterprise Mobility Infrastructure Management Services shall create and distribute firewall policies to infrastructure components running host-based firewall software in accordance with applicable DoD or using agency policy and guidance.	T=O	A	SI3, CA3, IR4, SC7, AC4, SC3(6)
IFM.06	The Enterprise Mobility Infrastructure Management Services shall create and distribute firewall policies to network-based firewall components in accordance with applicable DoD or using agency policy and guidance.	T=O	A	SI3, CA3, IR4, SC7, AC4, SC3(6)
IFM.07	The Enterprise Mobility Infrastructure Management Services shall be configured to receive, authenticate, and validate virus and IDS/IPS signatures received indirectly via the Internet (e.g., via the Internet Download Server) or directly from applicable vendors in accordance with applicable DoD or using agency policy and guidance.	T=O	A	CM6, SA18, SC26, CP9
IFM.08	The Enterprise Mobility Infrastructure Management Services shall securely configure, manage, and monitor all networking components (e.g., switches, routers, firewalls) in accordance with applicable DoD or using agency policy and guidance.	T=O	A	CM3, CM6, CA7, SI4, SI3

Requirement Number	Requirement Description	Threshold/ Objective	Architecture/ Configuration/ Guidance (A/C/G)	NIST 800-53 Control Mapping
IFM.09	The Enterprise Mobility Infrastructure Management Services shall remotely install software updates on infrastructure components in accordance with applicable DoD or using agency policy and guidance.	T=O	A	AC17, CM6, CM2, CM5, CM11, SI2
IFM.10	The Enterprise Mobility Infrastructure Management Services shall be configured in accordance with applicable DoD or using agency policy and guidance.	T=O	C	CM6
IFM.11	The Enterprise Mobility Infrastructure Management Services shall be configured to provide mobile application vetting to support application whitelisting efforts.	0	A	CM7(4), CM7(5)
IFS.00	**Security Services Requirements Enterprise Mobility Infrastructure**			
IFS.01	The Enterprise Mobility Infrastructure Security Services shall record audit events reported by infrastructure components.	T=O	A	AU2, AU3, SI4
IFS.02	The Enterprise Mobility Infrastructure Security Services shall provide integrity protection of audit records in transit from infrastructure components.	T=O	A	AU9
IFS.03	The Enterprise Mobility Infrastructure Security Services shall provide integrity protection of audit records at rest.	T=O	A	AU9
IFS.04	The Enterprise Mobility Infrastructure Security Services shall support Windows Domain authentication if the infrastructure includes components running Microsoft Windows.	T=O	A	IA2, IA3
IFS.05	The Enterprise Mobility Infrastructure Security Services shall support Kerberos authentication if the infrastructure includes components running Linux.	T=O	A	IA2, IA3
IFS.06	The Enterprise Mobility Infrastructure Security Services shall support RADIUS authentication if required by the system design (e.g., to support the SIP Service).	T=O	A	IA2, IA3
IFS.07	The Enterprise Mobility Infrastructure Security Services shall require the authentication of users based on USERID and password.	T=O	C	IA2

Requirement Number	Requirement Description	Threshold/ Objective	Architecture/ Configuration/ Guidance (A/C/G)	NIST 800-53 Control Mapping
IFS.08	The Enterprise Mobility Infrastructure Security Services shall authorize access using role-based access control.	T=O	C	IA4
IFS.09	The Enterprise Mobility Infrastructure Security Services shall audit all authentication and authorization failures.	T=O	C	AU2, AU3, SI4
IFS.10	The Enterprise Mobility Infrastructure Security Services shall be configured to audit selected authentication and authorization successes in accordance with applicable DoD or using agency guidance.	T=O	C	AU2, AU3, SI4
IFS.11	The Enterprise Mobility Infrastructure Security Services shall require authentication and authorization for users to view, modify, delete, or backup audit records.	T=O	C	AU9
IFA.00	**Enterprise Mobility Infrastructure Architecture Requirements**			
IFA.01	The Enterprise Mobility Infrastructure shall implement Directory Services.	T=O	A	CM6, SI2, SI8, AU3, AC19
IFA.02	The Enterprise Mobility Infrastructure shall implement audit and logging for all network systems and hosts in accordance with applicable DoD or using agency policy and guidance.	T=O	A	AU2, AU3, SI4
IFA.03	The Enterprise Mobility Infrastructure shall provide Domain Name System Security Extensions (DNSSEC) Servers within the infrastructure networks.	O	A	SC20
IFA.04	The Certificate Validation Service shall validate X.509 certificates.	T=O	C	SC23, SA12(5), SC29
IFA.05	The Enterprise Mobility Infrastructure shall require authentication and authorization of users to stop, start, or change configuration for servers or services.	T=O	C	RA5, SI3, AC3, AC17, AC3, AU2, AC6, IA2
IFA.06	The Enterprise Mobility Infrastructure Security Services shall be configured to enable posting of full Certificate Revocation Lists (CRLs) to the Directory Service.	O	C	SI2, SI8, CM6, AU3, AC19

Requirement Number	Requirement Description	Threshold/ Objective	Architecture/ Configuration/ Guidance (A/C/G)	NIST 800-53 Control Mapping
IFA.07	The Enterprise Mobility Infrastructure Security Services shall be configured to enable posting of delta CRLs to the Directory Service.	O	C	SI2, SI8, CM6, AU3, AC19
IFA.08	The Enterprise Mobility Infrastructure Security Services shall include a Certificate Validation Service.	O	C	SA12(5), SC23, SC29
IFN.00	**Enterprise Mobility Infrastructure Networking Services Requirements**			
IFN.01	If implemented, the Enterprise Mobility Infrastructure shall provide DNS Servers within the infrastructure networks.	T	A	SC20, SC25, SC21
IFN.02	If implemented, the Enterprise Mobility Infrastructure shall provide Network Time Servers that provide time synchronization within the infrastructure networks.	T=O	A	SC12, AU8, CM6
IFN.03	The Enterprise Mobility Infrastructure Directory Service shall require user authentication and authorization to perform creation, deletion, or modification of directory entries or attributes.	T=O	C	AC2, AC3, IA2, AC5, RA5, SI3, AC17, AC14
IFN.04	The Enterprise Mobility Infrastructure Directory Services shall be configured to require user authentication and authorization to read directory entries or attributes.	T=O	C	AC2, AC3, IA2, AC5, RA5, SI3, AC17, AC14
IFN.05	The Enterprise Mobility Infrastructure Directory Services shall be configured to allow storage of X.509 certificates.	T=O	C	SC23, SC29, SA12(5)
IFN.06	The Enterprise Mobility Infrastructure Directory Services shall be configured to allow storage of X.509 CRLs.	T=O	C	SC23, SC29, SA12(5)
IFN.07	The Enterprise Mobility Infrastructure shall require authentication and authorization of a user to stop, start, or change configuration for servers or services.	T=O	C	RA5, SI3, AC2, AC17, AC6, AC3, IA2

A.8 PKI Requirements

Table 10: PKI Requirements

Requirement Number	Requirement Description	Threshold/ Objective	Architecture/ Configuration/ Guidance (A/C/G)	NIST 800-53 Control Mapping
ECA.00	**Certificate, Key, and Trust Management**			
ECA.01	The Certificate Authority cryptomodule shall be FIPS 140-2 compliant.	T=O	C	SC28, SC42, IA7, SC13
ECA.02	A Certificate Authority service shall be configured to generate user certificates.	T=O	C	SC23, SA12(5), SC29
ECA.03	A Certificate Authority service shall be configured to accept a common specified field (e.g., DoD Electronic Data Interchange Personnel Identifier, (DODEDIPI) as part of the Distinguished Name for user certificates.	T=O	C	SC20
ECA.04	The Certificate Authority service shall maintain a data store of all certificates it has issued including date of issuance and current status.	T=O	C	SC23, SA12(5), SC29
ECA.05	The Certificate Authority service shall maintain a Certificate Revocation List (CRL).	T=O	C	AC3, SC23
ECA.06	The Certificate Authority service shall process certificate revocation requests.	T=O	C	AC3, SC23
ECA.07	The Certificate Authority service shall be configured to process PKCS #7 and #10 messages.	T=O	C	SC23
ECA.08	The Certificate Authority shall be capable of generating certificates for the digital signature algorithms as defined in CNSSP-15, Annexes B and C.	O	C	SC23

A.9 Provisioning Requirements

Table 11: Provisioning Requirements

Requirement Number	Requirement Description	Threshold/ Objective	Architecture/ Configuration/ Guidance (A/C/G)	NIST 800-53 Control Mapping
EWS.00	**Enrollment Work Station Requirements**			
EWS.01	The Enrollment Workstation shall be able to accept entry of requests for device certificates.	T=O	C	MA2?
EWS.02	The Enrollment Workstation shall be configurable to define and enforce complexity policies for the secret value (passphrase or password) used to protect sensitive key material.	T=O	C	MA4, SC23, IA2, IA3, IA4, IA5
EWS.03	The Enrollment Workstation shall be able to accept entry of requests for user certificates.	T=O	C	MA2
EWS.04	The Enrollment Workstation shall be able to interface to non-secure removable media.	T=O	C	MA2, MA3
EWS.05	The Enrollment Workstation shall generate certificates for the digital signature algorithms defined in CNSSP-15, Annex C.	T	C	SC23
EWS.06	The Enrollment Workstation shall generate certificates for the digital signature algorithms defined in CNSSP-15, Annex B.	O	C	SC23
UEP.00	**User Equipment Provisioning Requirements**			
UEP.01	During provisioning any applications, processes, and files that are not essential for operation of the User Equipment shall be removed.	T=O	C	AC6, CM7
UEP.02	During provisioning of the User Equipment any functionality that would allow an ordinary user of the User Equipment to attain administrative user privileges shall be removed.	T=O	C	AC6, CM7
UEP.03	During provisioning and updates of the User Equipment the administrative user shall clear the contents of the cache in order to remove any data associated with the applications that were removed during provisioning or updating the User Equipment.	T=O	C	AC3, AC5

Requirement Number	Requirement Description	Threshold/ Objective	Architecture/ Configuration/ Guidance (A/C/G)	NIST 800-53 Control Mapping
UEP.04	After provisioning or updating of the User Equipment the administrative user shall reboot the User Equipment in order to have a fresh initialization of the kernel and the applications remaining, as well as a fresh load of the boot image.	T=O	C	MA2

Appendix B Test Criteria - Enterprise Mobility

This appendix contains test criteria for requirements applicable to Enterprise Mobility components. This appendix does not include requirements applicable for Enterprise Services. As a result, no requirements are identified for fixed devices and external gateways. The test criterion were written to make it easier for project management, accrediting officials, system administrators, and vendors/integrators to determine whether a given component was successful at meeting the security requirements outlined in Appendix A .

This appendix is not intended to replace any security testing performed as part of the certification activities by the local accrediting official but is intended to augment and support these activities. Each requirement is intended to be testable and provide an analysis of the solution to result in a yes/no answer of whether the requirement was met. A test protocol should make it possible to quickly determine whether the mobility solution has met the security requirements of this security guide.

B.1 Designators for the Overarching Mobility Requirements

Table 12: Appendix B Requirements Designators

Designator	Requirements Addressed
CSI	Requirements for **C**arrier **S**ervice **I**ntegration
ECA	Requirements for **E**lectronic **C**ertificate **A**uthority
EWS	Requirements for **E**nrollment **W**ork**S**tation operation
IFA	Requirements for **I**n**F**rastructure host **A**rchitecture
IFB	Requirements for **I**n**F**rastructure host **B**oundary protection
IFH	Requirements for **I**n**F**rastructure **h**ost systems
IFM	Requirements for **I**n**F**rastructure host **M**anagement
IFN	Requirements for **I**n**F**rastructure host **N**etworking
IFS	Requirements for **I**n**F**rastructure host **S**ecurity services
MOB	Overarching **MOB**ility reqts that a solution fielded using this MSG should implement
SVC	Requirements for the **SV**oIP **c**lient running on the User Equipment
SVP	Requirements for the overall **SV**o**I**P infrastructure
SVS	Requirements for the **SV**oIP and SIP **s**ervers
UEA	Requirements for the **U**ser **E**quipment **A**udit, monitoring and fault handling
UEP	Requirements for **U**ser **E**quipment **P**rovisioning
UES	Overall requirements for configuring the **U**ser **E**quipment, **Smartphone**
VPG	Requirements applicable to the **VP**N **G**ateway
VPN	Requirements for designing and implementing the **VPN** solution
WNC	**W**eb Arbitrated **N**on-Resident Data User Equipment **C**lient requirements
WND	**W**eb Arbitrated **N**on-Resident **D**ata
WNS	**W**eb Arbitrated **N**on-Resident Data **S**erver requirements

B.2 Test Criteria for Overarching Mobility Requirements

Table 13: Overarching Mobility Test Criteria

Requirement Number	Test Criteria
	Overarching Mobility Requirements
MOB.01	All network traffic across an untrusted transport medium shall be protected by a minimum of two layers of encryption.
	1. Identify the untrusted transport link 2. Determine how the traffic on the link is encrypted 3. Verify the data on the link is encrypted twice using an authorized encryption standard. a. How is the original data first encrypted? b. How is the once encrypted data encrypted a second time?
MOB.02	The Mobility components providing the outer layer of encryption and inner layer of encryption shall use non-proprietary standards based protocols.
	1. Identify which encryption standards are used to protect the inner and outer layers of encryption 2. Verify that the encryption algorithms are based on non-proprietary standards-based protocols
MOB.03	Products for each layer of network encryption shall be from different vendors.
	1. Determine which vendors provide the products used for the inner and outer layers of encryption 2. Verify that the vendors are not the same
MOB.04	The software for each layer of network encryption shall not use the same software cryptographic libraries or depend on the same services.
	1. Identify the cryptographic libraries and services used by each encryption activity 2. Identify any libraries or service routines that are used by both encryption layers 3. Verify that there are no common libraries or service routines used between encryption layers
MOB.05	The Mobility components providing the outer layer of encryption and inner layer of encryption in the Enterprise Mobility Infrastructure shall be run on separate hardware platforms.
	1. Identify the hardware responsible for encrypting the outer and inner layers of encryption 2. Verify the hardware that encrypts the outer layer encryption is physically separate from the hardware that encrypts the inner layer
MOB.06	The Mobility components providing the outer layer of encryption and inner layer of encryption in the Enterprise Mobility Infrastructure shall not utilize the same OS for critical IA security functionality. Differences between Service Packs (SP) or version numbers for a particular vendor's OS do not provide adequate diversity.
	1. Identify all Mobility components providing encryption for inner and outer layers 2. Identify the operating systems used in each critical IA security function 3. Verify that each critical IA security function does not use the same OS
MOB.07	Each layer of encryption protecting network traffic across an untrusted transport medium shall be of sufficient strength to protect the highest classification of the data in accordance with CNSSP-15.

Requirement Number	Test Criteria
	1. Identify all encryption algorithms used to protect data at every layer for transmission across an untrusted communications link 2. Identify the classification of the data being transmitted 3. Verify all algorithms meet the required strength for the classification in accordance with CNSSP-15 a. Ensure encryption algorithms for Top Secret data meet the CNSSP-15 requirements b. Ensure encryption algorithms for Secret data meet the CNSSP-15 requirements
MOB.08	Every device/component shall be issued unique certificates and corresponding private keys for authentication.
	1. Identify all the devices/components that make up the system 2. Compare all the digital certificates 3. Verify that each device/component has a certificate and it is unique a. Ensure no two certificates share the same issuer/serial number field b. Ensure each certificate has a corresponding private key
MOB.09	The authentication certificates for each layer of network encryption shall be issued by different Certificate Authorities.
	1. On each UE, identify the authentication certificates for each layer of network encryption 2. Compare the digital certificates 3. On each UE, verify the two certificates do not share the same Certificate Authority
MOB.10	All components of the system shall have been approved via NIAP and NSA's Commercial Solutions for Classified
	1. Identify each component in the system 2. Verify each component is on the NIAP approval list 3. Verify each component is approved for use by NSA's Commercial Solutions for Classified
MOB.11	If single factor authentication is used (e.g., password, passphrase, or PIN), then at least two independent user authentication steps shall be required to enable classified access. (i.e., two steps may be device unlock and password to decrypt stored keys and certificates).
	1. Connect the device to the authorized classified network 2. Access classified data on the network using single-factor authentication 3. Verify that in accessing the network the device required two independent single-factor user authentication steps a. The user must enter a different password, passphrase or PIN on two separate occasions.
MOB.12	All cryptographic algorithms shall conform to the Suite B standard or the Suite B transitional standard as documented in CNSSP-15.

Requirement Number	Test Criteria
	1. Identify all encryption algorithms used to protect data at every layer for transmission across an untrusted communications link 2. Identify the classification of the data being transmitted 3. Verify all algorithms meet the required strength for the classification in accordance with Suite B and Suite B Transitional as stated in CNSSP-15 a. Ensure encryption algorithms for Top Secret data meet the CNSSP-15 requirements b. Ensure encryption algorithms for Secret data meet the CNSSP-15 requirements
MOB.13	All cryptographic algorithms shall conform to the full Suite B standard as documented in CNSSP-15.
	1. Identify all encryption algorithms used to protect data at every layer for transmission across an untrusted communications link 2. Identify the classification of the data being transmitted 3. Verify all algorithms meet the required strength for the classification in accordance with Suite B as stated in CNSSP-15 a. Ensure encryption algorithms for Top Secret data meet the CNSSP-15 requirements b. Ensure encryption algorithms for Secret data meet the CNSSP-15 requirements
MOB.14	Each system shall be configured to protect certificates along with their corresponding private keys and security critical profiles stored on the system in accordance with protection guidance for the highest level of classification of the system.
	1. Identify all system components that store/process certificates or private keys 2. Identify all system components that are configured with security critical profiles 3. Review all protection guidance associated with the system 4. Verify all identified system components properly protect security areas in accordance with the protection guidance a. Ensure digital certificates are protected to the classification level of the network b. Ensure private keys are protected to the classification level of the network c. Ensure security critical profiles are protected to the classification level of the network
MOB.15	All systems and services shall be configured in accordance with NIST 800-53, applicable DoD guidance, or applicable using-agency guidance except where configuration requirements in this document state differently.
	1. Identify all guidance applicable to the network system and components 2. Verify the network is configured in accordance with all applicable guidance to include NIST 800-53
MOB.16	The using agency shall develop and use a Certification Practice Statement (CPS) that will include information required by applicable DoD or using agency guidance and the requirements enumerated in this document.
	1. Identify the Certification Practice Statement (CPS) for the network system 2. Verify the CPS includes applicable DoD or using agency guidance

B.3 Test Criteria for Overarching VPN Requirements

Table 14: VPN Test Criteria

Requirement Number	Test Criteria
	Overarching VPN Requirements
VPN.01	The VPN shall be a standards based IPsec solution.
	1. Identify the IPsec standards used by the VPN 2. Verify the IPsec solution is standards-based a. The VPN IPsec implementation follows applicable IETF RFCs b. The VPN IPsec implementation is public domain and not protected by trademark, patent or copyright
VPN.02	The VPN Gateway and client shall use IPsec in tunnel-mode.
	1. Identify the VPN Gateway and client platforms 2. Configure the VPN Gateway to accept VPN connections in tunnel-mode 3. Configure the VPN client to connect to the gateway using tunnel-mode 4. On the VPN client, initiate a connection to the gateway 5. Verify the connection was established and that tunnel-mode was used
VPN.03	*Requirement withdrawn IFO VPN.04*
VPN.04	The VPN Gateway and client shall use IKEv2.
	1. Identify the VPN Gateway and client platforms 2. Configure the VPN Gateway's IPsec protocol to use IKEv2 3. Configure the VPN client's IPsec protocol to use IKEv2 4. Verify both the VPN Gateway and client settings are configured for IKEv2
VPN.05	The VPN Gateway and client shall be configured to use the cipher suites specified in IETF RFC 6380 "Suite B Profile for Internet Protocol Security (IPsec)"
	1. Identify the VPN Gateway and client platforms 2. Review the encryption configuration of each platform a. Identify what cipher suite is used by the VPN Gateway b. Identify what cipher suite is used by the VPN client 3. Verify that the cipher suite used by the VPN Gateway and client is specified in IETF RFC 6380 under "Suite B Profile for Internet Protocol Security (IPsec)"
VPN.06	The VPN Gateway and client shall be configured to prohibit split-tunneling.
	1. Identify the VPN Gateway and client platforms 2. In the setting in the VPN Gateway, disable split-tunneling 3. In the setting in the VPN client, disable split-tunneling 4. Verify that split-tunneling was disabled on both the gateway and client
VPN.07	The VPN Gateway and client shall be configured to maintain the tunnel even if applications are not transmitting data.

Requirement Number	Test Criteria
	1. Identify the VPN Gateway and client configuration settings for maintaining the IPsec tunnel 2. Ensure the gateway's IPsec tunnel settings for "time-out" are disabled or set to "never" 3. Ensure the device's IPsec tunnel settings for "time-out" are disabled or set to "never" 4. Ensure the device's sleep/power down settings are set appropriately 5. Connect device to network using the VPN tunnel 6. Place device in a quiescence state a. Exit applications b. Monitor network interface card to ensure zero network activity (other than VPN tunnel keep-alive messages) 7. Verify the device maintained the VPN tunnel after an extended period of no network activity a. Launch an app that requires access to the network through the VPN tunnel to test connectivity
VPN.08	The VPN client shall automatically reconnect the VPN upon unexpected disconnect.
	1. Review the VPN client configuration settings 2. Enable the setting for VPN automatic reconnect 3. Connect the VPN client to the VPN Gateway 4. On the VPN Gateway, perform an action that resets/disconnects the VPN connection 5. Verify the VPN client disconnected and automatically reconnected to the VPN Gateway
	VPN Gateway Requirements
VPG.01	The VPN Gateway shall audit and report all unsuccessful attempts to establish a security association.
	1. Identify the VPN Gateway and bring up the audit and report settings 2. Configure the VPN Gateway to log all failed attempts to make a VPN connection 3. Configure a device to make a connection to the VPN Gateway 4. Using the device, attempt a connection to the VPN Gateway and deliberately fail a. Use a device with an invalid digital certificate 5. Verify the VPN Gateway audited and reported the failed connection attempt a. Ensure the auditing and reporting is in accordance with applicable guidance
VPG.02	The VPN Gateway shall audit and report successful attempts to establish a security association in accordance with applicable DoD or using agency guidance.
	1. Identify the VPN Gateway and bring up the audit and report settings 2. Configure the VPN Gateway to log all successful VPN connections 3. Configure a device to make a connection to the VPN Gateway 4. Using the device, successfully connect to the VPN Gateway 5. Verify the VPN Gateway audited and reported the successful connection a. Ensure the auditing and reporting is in accordance with applicable guidance

VPG.03	The VPN Gateway shall audit and report all integrity check failures.
	1. Identify the VPN Gateway and bring up the audit and report settings 2. Configure the VPN Gateway to log all integrity check failures a. Ensure IPsec/Encapsulating Security Protocol (ESP) is enabled b. Ensure IPsec/Header Authentication (HA) is enabled c. Ensure the digital signature algorithm used to ensure integrity is selected in accordance with applicable DoD or using agency guidance 3. Verify the VPN Gateway is configured to audit and report integrity check failures
VPG.04	The VPN Gateway shall be configured in accordance with applicable DoD or using organization guidance.
	1. Identify the VPN Gateway and bring up the audit and report configuration settings 2. Identify applicable DoD or using organization guidance 3. Ensure the VPN Gateway is configured in accordance with the identified DoD or using organization guidance
VPG.05	The VPN Gateway shall be configured to assign an internal network private IP address to a VPN client upon successful establishment of a security association.
	1. Identify the VPN Gateway DHCP configuration settings 2. Configure the VPN Gateway for DHCP address assignment a. Set the DHCP assignable IP address range in accordance with organization guidance 3. Configure a device to successfully connect to the VPN Gateway 4. Upon successful connection of the device to the VPN Gateway, identify the device's IP address 5. Verify the assigned IP address is within the range of DHCP addresses configured on the VPN Gateway
VPG.06	The VPN Gateway shall be configured to request re-authentication for security associations that have been inactive for a configurable period of time.
	1. Identify the VPN Gateway and client configuration settings for maintaining the IPsec tunnel 2. Ensure the gateway's IPsec tunnel setting for idle-traffic "time-out" is enabled 3. Ensure the VPN Gateway's IPsec re-authentication setting is enabled a. Set the period between re-authentications in accordance with organizational policy 4. Ensure the device's sleep/power down settings are set appropriately 5. Connect device to the network using the VPN tunnel 6. Allow the VPN tunnel to remain idle for longer than the defined re-authentication period 7. Verify the VPN Gateway forced a re-authentication of the security association between the VPN tunnel connection and client

VPG.07	The VPN Gateway shall be configured to terminate security associations that have been inactive for a configurable period of time.
	1. Identify the VPN Gateway and client configuration settings for maintaining the IPsec tunnel 2. Ensure the gateway's IPsec tunnel setting for idle-traffic "time-out" is enabled 3. Ensure the device's sleep/power down settings are set appropriately 4. Connect device to the network using the VPN tunnel 5. Allow the VPN tunnel to remain idle for longer than the defined "time-out" period 6. Verify the VPN Gateway terminates the security association between the VPN tunnel connection and client
VPG.08	The VPN Gateway shall perform certificate path validation.
	1. Identify the VPN Gateway configuration settings for certificate acceptance and path validation 2. Enable settings for accepting Certificate Authority (CA) subordinate certificates 3. On the UE, employ a certificate that uses subordinate certificates and requires a certificate path discovery to the root CA 4. Connect the UE to the VPN Gateway and use the subordinate certificate for authentication 5. Verify the UE successfully connected to the VPN Gateway using the subordinate certificate
VPG.09	The VPN Gateway shall check for revoked certificates.
	1. Configure a device using a digital certificate 2. On the network infrastructure, revoke the device's digital certificate 3. Attempt to connect the device with revoked certificate to the network through the VPN Gateway 4. Verify the device's connection was rejected due to a revoked certificate
VPG.10	The VPN Gateway shall check for invalid certificates
	1. Configure a device using an invalid digital certificate 2. Attempt to connect the device with invalid certificate to the network through the VPN Gateway 3. Verify the device's connection was rejected due to an invalid certificate
VPG.11	The VPN Gateway shall be configured to consult an external white or black list to authorize certificates presented by the User Equipment client before access to the protected network is granted.

	1. Identify the VPN Gateway configuration settings for verifying certificate validity
	2. Ensure the VPN is configured for a certificate revocation using a white or black list (e.g. CRL)
	3. Configure a UE using a digital certificate
	4. Revoke the device's digital certificate
	  a. Add it to the black list (e.g. CRL)
	  b. Remove it from the white list
	5. Attempt to connect the UE with revoked certificate to the network through the VPN Gateway
	6. Verify the UE's connection was rejected due to the certificate being on the black list or absent from the white list

VPG.12	The VPN Gateway shall be configured to use OCSP or equivalent to authorize certificates presented by the User Equipment client before access to the protected network is granted
	1. Identify the network equipment that uses OSCP to verify the status of certificates a. Ensure OCSP is enabled b. Disable CRLs 2. Identify the Certificate Authority (CA) that maintains the revocation status of certificates 3. On the CA, revoke a certificate 4. Attempt to connect the device with revoked certificate to the network Verify the connection attempt failed due to revoked certificate

B.4 Test Criteria for Overarching SVoIP Requirements

Table 15: SVoIP Test Criteria

Requirement Number	Test Criteria
	Overarching SVoIP Requirements
SVP.01	The Enterprise Mobility Solutions shall use the Suite B cryptosuite.
	1. Identify all encryption algorithms used to protect data at every layer for transmission across an untrusted communications link 2. Identify the classification of the data being transmitted 3. Verify all algorithms meet the required strength for the classification in accordance with Suite B and Suite B Transitional as stated in CNSSP-15 c. Ensure encryption algorithms for Top Secret data meet the CNSSP-15 requirements a. Ensure encryption algorithms for Secret data meet the CNSSP-15 requirements
SVP.02	The User Equipment SVoIP Client and Mobility SIP Server shall use SIP over TLS for registration of the User Equipment, call setup, and call termination.
	1. Identify the SIP Server configuration settings for protecting User Access Client (e.g. User Equipment) connections 2. Enable TLS 3. Connect a device with a valid digital certificate to the Mobility SIP Server 4. Verify the SIP Server connection was successful using TLS
SVP.03	The User Equipment SVoIP Client shall use the SDES-SRTP Protocol.
	1. On the client device, review the Voice over Internet Protocol (VoIP) security settings for SDP/SRTP/SRTCP 2. Enable the SDES crypto attribute appropriate for the level of classification 3. Connect a device to the SIP Server using a valid digital certificate 4. Verify the SIP Server connection was successful using the SDES protocol
SVP.04	The Enterprise Mobility System shall provide the capability for User Equipment to communicate with another User Equipment operating at the same classification level in the same enterprise.

Requirement Number	Test Criteria
	1. Identify the phone number for the first classified User Equipment 2. Identify the phone number of the second User Equipment at the same classification and on the same enterprise as the first User Equipment 3. Connect both UEs to the Enterprise Mobility System 4. Using the first User Equipment, call the second User Equipment 5. Verify the first User Equipment connects to the second User Equipment through the Enterprise Mobility System a. Ensure the first User Equipment rings the second User Equipment b. Ensure the first User Equipment properly transmits voice data to the second User Equipment c. Ensure the second User Equipment properly transmits voice data to the first User Equipment
SVP.05	The Enterprise Mobility System shall provide the capability for User Equipment to communicate with another User Equipment operating at the same classification level but in a different enterprise.
	1. Identify the phone number for the first classified User Equipment 2. Identify the phone number of the second User Equipment at the same classification but on a different enterprise than the first User Equipment 3. Connect both UEs to their respective Enterprise Mobility Systems 4. Using the first User Equipment, call the second User Equipment 5. Verify the first User Equipment connects to the second User Equipment through both Enterprise Mobility Systems a. Ensure the first User Equipment rings the second User Equipment b. Ensure the first User Equipment properly transmits voice data to the second User Equipment c. Ensure the second User Equipment properly transmits voice data to the first User Equipment
SVP.06	The Enterprise Mobility System shall provide the capability for User Equipment to communicate with fixed enterprise VoIP devices operating at the same classification level.
	1. Connect a User Equipment to the Enterprise Mobility System 2. Identify the phone number of a fixed enterprise VoIP device at the same classification 3. Using the User Equipment, call the fixed enterprise VoIP device 4. Verify the User Equipment connects to the fixed enterprise VoIP device a. Ensure the User Equipment rings the fixed enterprise VoIP device b. Ensure the User Equipment properly transmits voice data to the fixed enterprise VoIP device c. Ensure the fixed enterprise VoIP device properly transmits voice data to the User Equipment
SVP.07	The Enterprise Mobility System, in conjunction with the existing Enterprise Gateways, shall provide the capability for User Equipment to communicate with devices operating on non-IP networks at the same classification level.

Requirement Number	Test Criteria
	1. Connect User Equipment to the Enterprise Mobility System 2. Identify the phone number of a device operating on a non-IP network at the same classification 3. Using the User Equipment, call the non-IP network device 4. Verify the User Equipment connects to the non-IP network device a. Ensure the User Equipment rings the non-IP network device b. Ensure the User Equipment properly transmits voice data to the non-IP network device c. Ensure the non-IP network device properly transmits voice data to the User Equipment
SVP.08	Within the Enterprise Mobility System, the User Equipment SVoIP client and Mobility SIP Server shall perform mutual public key authentication using only the keys and certificates issued by the designated SVoIP Certificate Authority.
	1. Install an authorized SVoIP digital certificate on the UE 2. Install an authorized SVoIP digital certificate on the Mobility SIP Server 3. Connect the UE to the Enterprise Mobility System and connect to the Mobility SIP Server 4. Verify the UE connected to the Mobility SIP Server through mutual authentication of the certificates 5. Invalidate the UE certificate 6. Attempt to reconnect the UE to the Mobility SIP Server 7. Verify the attempt failed due to invalid UE certificate 8. Validate the UE certificate and invalidate the SIP Server certificate 9. Attempt to reconnect the UE to the Mobility SIP Server 10. Verify the attempt failed due to invalid SIP Server certificate 11.
SVP.09	The Enterprise Mobility Solution shall use the SRTP Protocol in compliance with IETF RFC 3711 to transmit secure voice traffic. Within the Enterprise Mobility System, the User Equipment shall use SRTP and SRTCP to transmit secure voice traffic.
	1. On the Enterprise Mobility System SIP Server, review the VoIP security settings 2. Enable SRTP/SRTCP 3. On the User Equipment, review the VoIP client security settings 4. Enable SRTP/SRTCP 5. Connect the User Equipment to the Enterprise Mobility System 6. Verify the User Equipment connection to the SIP Server was successful using SRTP/SRTCP
SVP.10	The Enterprise Mobility System and User Equipment client shall be configured to use a password for client authentication for SIP REGISTER function requests.
	1. Attempt to register the User Equipment with the Enterprise Mobility System SIP Server 2. Ensure that a password is requested to register a. This is separate from the password to break the screen lock 3. Enter an invalid password 4. Verify the registration request was rejected due to invalid password 5. Enter a valid password 6. Verify registration was successful

Requirement Number	Test Criteria
SVP.11	The Enterprise Mobility System shall be configured to automatically notify the operator of User Equipment of the highest level classification supported by the connection to another device.
	1. Identify two test UEs of different classification 2. Identify another UE to initiate calls with the test UEs 3. Verify the Enterprise Mobility System is configured to report the classifications of each device making a connection 4. Initiate a connection with the test UE of highest classification 5. Verify upon connection, the initiator UE's classification is correctly displayed on the test UE and the test UE's classification is correctly displayed on the initiator UE 6. Initiate a connection with the test UE of lowest classification 7. Verify upon connection, the initiator UE's classification is correctly displayed on the test UE and the test UE's classification is correctly displayed on the initiator UE
	SVoIP Server Requirements
SVS.01	The Enterprise Mobility System shall be able to interface to a SIP Trunking Gateway that enables voice calls between User Equipment authorized to operate at the unclassified level and an unsecured VoIP device accessible via an external IP network. (Note: This includes packet-switched cellular voice communications.)
	1. Connect User Equipment authorized to operate at the unclassified level to the Enterprise Mobility System 2. Identify the phone number of a an unsecured VoIP device operating on an external IP network 3. Using the User Equipment, call the unclassified VoIP device 4. Verify the User Equipment connects to the unclassified VoIP device through the SIP Trunking Gateway a. Ensure the User Equipment rings the unclassified VoIP device b. Ensure the User Equipment properly transmits voice data to the unclassified VoIP device c. Ensure the unclassified VoIP device properly transmits voice data to the User Equipment
SVS.02	The SVoIP Server shall be configured to have two User Equipment send SRTP traffic directly to one another via the Enterprise Mobility Infrastructure network and their respective VPN Gateway tunnels, instead of having them use the SVoIP Server as an intermediary.

Requirement Number	Test Criteria
	1. On the SVoIP Mobility System, configure the SIP Server to connect VoIP traffic directly between UEs via the VPN Gateway after the SIP Server has established the VoIP connection a. Enable the SRTP setting 2. Connect the User Equipment to the SVoIP Mobility System SIP Server 3. Call User Equipment that is also connected to the SVoIP Mobility System 4. Verify the User Equipment to User Equipment SVoIP connection bypasses the SIP Server and connects only through the VPN Gateway using SRTP a. Ensure the User Equipment properly transmits voice data to distant User Equipment b. Ensure the distant User Equipment properly transmits voice data to the User Equipment
SVS.03	The Mobility SIP Server in the "home" enterprise and the Mobility SIP Server in the far-end enterprise shall exchange the caller IDs of the User Equipment.
	1. Connect the "home" and "far-end" UEs to their respective Enterprise Mobility Systems 2. Using the "home" User Equipment, call the "far-end" User Equipment to establish a SVoIP connection 3. Verify the Caller-ID messages on each phone are correct a. The "home" User Equipment displays the Caller-ID of the "far-end" User Equipment on its display b. The "far-end" User Equipment displays the Caller-ID of the "home" User Equipment on its display
SVS.04	For communication between User Equipment and a fixed enterprise VoIP device, the Mobility SIP Server and Secure Voice Gateway shall use SIP over TLS for transmitting call setup and call termination messages used by the User Equipment.
	1. On the SVoIP Mobility System, configure the SIP Server to require User Equipment connections using SIP over TLS 2. On the Secure Voice Gateway, configure the gateway to require connections to the SIP Server using SIP over TLS a. Enable SIP over TLS between the fixed enterprise VoIP device and the Secure Voice Gateway if supported 3. Identify the phone number for a fixed enterprise VoIP device 4. Connect User Equipment to the Enterprise Mobility System and call the fixed enterprise VoIP device 5. Verify the User Equipment connects to the fixed enterprise VoIP device through the Secure Voice Gateway using SIP over TLS d. Ensure the User Equipment rings the fixed enterprise VoIP device e. Ensure the User Equipment properly transmits voice data to the fixed enterprise VoIP device f. Ensure the fixed enterprise VoIP device properly transmits voice data to the User Equipment

SVS.05	For communication between User Equipment and a fixed enterprise VoIP device, the User Equipment and Secure Voice Gateway shall use SRTP and SRTCP to transmit secure voice traffic.
	1. On the Enterprise Mobility System, configure the SIP Server to require User Equipment connections using SRTP and SRTCP 2. On the Secure Voice Gateway, configure the gateway to require connections to the SIP Server using SRTP and SRTCP a. Enable SRTP/SRTCP between the fixed enterprise VoIP device and the Secure Voice Gateway/SIP Server if supported 3. Identify the phone number for a fixed enterprise VoIP device 4. Connect the User Equipment to the Enterprise Mobility System and call the fixed enterprise VoIP device 5. Verify the User Equipment connects to the fixed enterprise VoIP device through the Secure Voice Gateway using SRTP and SRTCP a. Ensure the User Equipment rings the fixed enterprise VoIP device b. Ensure the User Equipment properly transmits voice data to the fixed enterprise VoIP device c. Ensure the fixed enterprise VoIP device properly transmits voice data to the User Equipment
SVS.06	For communication between User Equipment and a fixed enterprise VoIP device, the Secure Voice Gateway shall exchange the caller ID of the User Equipment and Fixed VoIP Device between the Mobility SIP Server and the Enterprise SIP Server and vice versa.
	1. Connect the User Equipment to the Enterprise Mobility System SIP Server 2. Connect the fixed VoIP device to the Enterprise SIP Server 3. Using the User Equipment, call the fixed VoIP device through the Secure Voice Gateway and establish a SVoIP connection 4. Verify the Enterprise Mobility System SIP Server recorded the Caller-ID of the fixed VoIP device a. Review the SIP Server logs to determine the Caller-ID 5. Verify the Enterprise SIP Server recorded the Caller-ID of the User Equipment a. Review the SIP Server logs to determine the Caller-ID
SVS.07	The SIP Server shall be configured to securely contain a unique public key certificate and corresponding private key, which will be used to provide authentication of the SIP Server to the user equipment, in order to establish the TLS channel for SIP messages.
	1. On the SIP Server, identify the storage location of the public certificates and private keys 2. Verify that any activity within the certificate store requires administrative privileges a. Deleting public certificates or private keys b. Adding public certificates or private keys c. Altering public certificates or private keys d. Viewing private keys

B.5 Test Criteria for Web Based Non-Resident Data Requirements

Table 16: Web Based Non-Resident Data Test Criteria

Requirement Number	Requirement Description
	Overarching Web Browser Non-Resident Data Requirements
WND.01	The inner TLS tunnel shall be used to transit all traffic between the web browser and the web server.
	1. Connect User Equipment to the Enterprise Mobility Infrastructure a. Ensure the outer tunnel is established 2. Connect to the web server using the device's browser 3. Review the browser connection details for the encryption used 4. Verify the connection is protected using TLS
WND.02	The web browser shall be included in any permitted applications white list.
	1. Review the User Equipment's application white list 2. Verify that a web browser is included as a permitted application on the white list
	Web Browser Non-Resident Data Client Requirements
WNC.01	The web browser shall be configured to disallow the storing of any data in non-volatile memory.

	1. On the User Equipment, review privacy settings such as those for:
	  a. Offline storage
	  b. Caching
	  c. Downloads
	  d. History
	2. Verify that storage settings do not use non-volatile memory
	  a. Offline storage location uses volatile memory or is disabled
	  b. Caching uses volatile memory
	  c. Downloads are disabled
	  d. History is not preserved

WNC.02	The web browser shall be configured to connect to only authorized web servers.

	1. Review the web browser's proxy connection settings
	2. Review the operating system DNS settings
	3. Ensure the web browser points to a proxy server or the operating system points to a DNS Server that specifies authorized web servers
	4. Ensure the list of web server addresses in the DNS or proxy server are authorized
	5. Connect the User Equipment to the Enterprise Mobility Infrastructure
	6. Verify the web browser connects to the appropriate web servers
	  a. Connections to authorized web servers are allowed
	  b. Connections to unauthorized web servers are disallowed

WNC.03	The web browser shall be configured to use the existing outer VPN tunnel for network access.
	1. Connect User Equipment to the Enterprise Mobility Infrastructure a. Ensure the outer tunnel is established 2. Connect to a web server using the device's web browser 3. Verify the web browser connection is tunneled through the outer VPN tunnel 4. Disconnect the outer VPN tunnel 5. Attempt a connection to a web server using the device's web browser 6. Verify the connection attempt failed

WNC.04	The web browser shall be configured to disable any encryption protocol that is not Suite B compliant.
	1. Review the connection settings for the User Equipment's browser 2. Disable all encryption algorithm settings that are not Suite B compliant 3. Connect the User Equipment through the Enterprise Mobility Infrastructure to a web server using the device's web browser 4. Review the browser connection details for the encryption used 5. Verify the connection is protected using a Suite B algorithm
WNC.05	Web browser history shall only be maintained in volatile memory on the User Equipment.
	1. On the User Equipment, review the browser history settings 2. Verify the history settings disable history storage or use only volatile memory
WNC.06	The web browser shall be configured to disable the use of all versions of the Secure Sockets Layer (SSL) protocol.
	1. Review the connection settings for the User Equipment's browser connection 2. Disable all SSL settings 3. Connect the User Equipment to a web server 4. Review the connection details for the encryption used 5. Verify the connection does not use SSL
WNC.07	The web browser shall use a Suite B compliant Transport Layer Security (TLS) protocol 1.2 or later, or another approved cryptographic protocol.
	1. Review the connection settings for the User Equipment's browser connection 2. Enable TLS 1.2 or later or another approved cryptographic protocol 3. Connect the User Equipment to a web server using the device's web browser 4. Review the browser connection details for the encryption used 5. Verify the connection is protected using TLS 1.2 or another approved cryptographic protocol
WNC.08	The User Equipment web browser shall disable all browser plug-ins, extensions, and other third party software that has not specifically been approved for use by the DAO.
	1. On the User Equipment web browser, identify the installed plug-ins and extensions 2. Verify the installed plug-ins and extensions have been approved for use on the device by the DAO
WNS.00	**Web Browser Non-Resident Data Server Requirements**
WNS.01	The web server shall be configured to allow only TLS and Suite B cryptosuite options
	1. Review the connection settings for the web server connection 2. Review the web browser's connection protocol settings a. Ensure that TLS has been enabled b. Ensure all other connection protocols (e.g. SSL) have been disabled 3. Review the web browser's encryption settings a. Ensure the encryption settings are compliant with Suite B and for the classification level of the system 4. Connect User Equipment to the web server using the device's web browser 5. Review the browser connection details for the encryption used 6. Verify the connection is protected using TLS and a Suite B algorithm that is appropriate for the classification level of the system

WNS.02	The web server shall be configured to reject SSL encryption handshakes
	1. On the web server, review the connection settings 2. Ensure SSL settings are disabled 3. On the UE, disable all protocols except SSL 4. Attempt a User Equipment connection to the web server using a SSL protocol 5. Verify the connection was rejected because the web server prohibits SSL connections 6. On the UE, disable all SSL settings and re-enable TLS 7. Using the UE, connect to the web server 8. Verify the UE connected to the web server not using SSL
WNS.03	The web browser on the User Equipment shall be configured to require the user to authenticate to the web server at least every 24 hours.
	1. Review the connection settings of the web browser for connection re-authentication 2. Ensure the connection requires re-authentication at least every 24 hours 3. On the User Equipment, connect the web browser to the web server 4. Ensure the UE is authenticated to the web server 5. Remain connected to the server for more than 24 hours 6. Verify the connection re-authenticated after being connected for more than 24 hours

B.6 Test Criteria for Carrier Service Integration

Table 17: Carrier Service Integration Test Criteria

Requirement Number	Requirement Description
CSI.00	**Carrier Service Integration**
CSI.01	The Enterprise Mobility Infrastructure Integrator shall negotiate with the carrier QoS of IPsec VPN traffic from/to user equipment providing users with the lowest amount of network latency that is cost effective
	1. Reconcile the user latency requirements with the service cost and determine the required QoS 2. Contract for the required QoS with the carrier 3. During operation of the service, collect user experience statistics 4. Verify the user experience is acceptable
CSI.02	The using agency shall be cognizant of supply chain compromise attacks and build contingency plans in response
	1. Identify the contingency plan used in case of a suspected supply chain compromise 2. Verify the plan has been approved by the organization
CSI.03	The using agency shall be cognizant of rogue carrier threats and build contingency plans in response
	1. Identify the contingency plan used in case a rogue carrier is suspected 2. Verify the plan has been approved by the organization

CSI.04	The Enterprise Mobility Infrastructure Integrator shall use Suite B compliant cryptosuites
	1. Identify all the cryptographic algorithms used in the Enterprise Mobility Infrastructure 2. Verify the cryptographic algorithms use Suite B compliant cryptosuites
CSI.05	The Enterprise Mobility Infrastructure shall have a documented plan to detect and mitigate rogue base stations
	1. Identify the plan used to detect and mitigate the threat and use of rogue base stations 2. Verify the plan has been approved by the organization

B.7 Test Criteria for User Equipment Requirements

Table 18: User Equipment Test Criteria

Requirement Number	Test Criteria
User Equipment Requirements	
UES.01	The User Equipment shall provide a hardware root of trust, trusted boot, and attestation that interoperates with the infrastructure to support remote assessment of integrity and compliance status.
	1. On the UE, identify the trusted platform module(s) that perform trusted operations 2. Identify what trusted operations are performed 3. Verify the UE contains a hardware root of trust and utilizes a trusted boot sequence 4. Identify what trusted assessments are reported to the infrastructure 5. On the infrastructure, configure a network device to request attestation information from the UE 6. Using a UE with trusted reporting, connect to the network 7. Verify the network requested and obtained trusted device information 8. Verify the UE assessment data passed to the infrastructure is current and accurately reflects the UE's disposition.
UES.02	The User Equipment screen lock password shall be configured for length and complexity in accordance with DoD or using agency policy on mobile security.
	1. As administrator, configure the User Equipment screen lock password complexity and length to meet applicable security documentation requirements 2. As user, attempt to set the screen lock password to a value that does not meet the length and complexity requirements 3. Verify the User Equipment rejects the password change and prompts the user to reenter a password that meets the requirements 4. Enter a password value that meets the length and complexity requirements 5. Verify the User Equipment accepts the password change
UES.03	*Withdrawn*

UES.04	The User Equipment shall be configured to allow the USB cable to be used only to charge the device.
	1. Find device's USB driver/service settings 2. Disable USB data connection capability a. Remove USB drivers that are not needed for provisioning 3. Connect device to a computer through the USB port 4. Verify device does not establish a data connection 5. Connect device to a power source through the USB 6. Verify the device's battery charges
UES.05	The User Equipment shall be configured to disable processing of incoming cellular messaging services.
	1. Configure the firmware, operating system or app settings to prevent the User Equipment from processing incoming cellular messages 2. From a commercial cellular phone, send a text message to the User Equipment's phone 3. Verify the device does not accept, process or acknowledge receipt of a text message
UES.06	*Withdrawn*
UES.07	*Withdrawn*
UES.08	*Withdrawn*
UES.09	*Withdrawn*
UES.10	The User Equipment shall be configured to disable Bluetooth.

	1. Configure the firmware, operating system or app settings to disable the User Equipment's Bluetooth communication capability
	  a. Remove Bluetooth drivers and software
	  b. Disable settings
	2. Attempt to connect the User Equipment to a Bluetooth transceiver
	3. Verify the User Equipment does not make a Bluetooth connection

UES.11	The User Equipment shall be configured to disable Wi-Fi.

	1. Configure the firmware, operating system or app settings to disable the User Equipment's Wi-Fi communication capability
	  a. Remove Wi-Fi drivers and software
	  b. Disable settings
	2. Attempt to connect the User Equipment to a Wi-Fi wireless access point
	3. Verify the User Equipment does not make a Wi-Fi connection

UES.12	*Withdrawn*
UES.13	*Withdrawn*
UES.14	*Withdrawn*
UES.15	The User Equipment shall be configured to disable all GPS and location services except E911.
	1. On the UE, ensure there are no apps that provide location services 2. Configure the firmware, operating system or app settings to disable the User Equipment's location and GPS settings 3. Verify the User Equipment has no apps providing GPS or location information and UE GPS and location service settings are disabled.
UES.16	*Withdrawn*
UES.17	*Withdrawn*

UES.18	*Withdrawn*
UES.19	*Withdrawn*
UES.20	*Withdrawn*
UES.21	*Withdrawn*
UES.22	*Withdrawn*
UES.23	*Withdrawn*
UES.24	*Withdrawn*
PSS	**Protected Storage Services**
PSS.1	A device shall allow multiple authentication and authorization factors to govern use of a DEK or KEK
	There are no test requirement criteria for PSS.1
PSS.2	A device shall allow device integrity evidence to be one authorization factor for use of DEK and KEKs
	1. Identify what authorization factors permitted to access the UE's DEK and/or KEK 2. Identify the UE's mechanism for attesting to the device's integrity 3. Verify that the UE uses or will allow the mechanism for assuring the device's integrity to be used as one of the authorization factors for accessing the DEK and/or KEK
CAR	**Client Application Requirements**
CAR.1	The web mail replacement shall employ Secure/Multipurpose Internet Mail Extensions (S/MIME)
	1. Connect a UE to the network 2. Login into the web mail service 3. Review the web mail service options and find the S/MIME setting 4. Ensure the S/MIME module has been installed 5. Send a digitally signed and encrypted email to yourself 6. Verify you received the email encrypted and with verified signature
CAR.2	The web mail replacement shall meet all key protection requirements (refer to the Cryptographic Security Policy section, above)
	There are no test requirement criteria for CAR.2
CAR.3	The web mail replacement shall employ TLS Mutual Authentication (for user certificate verification)
	1. On the web mail server, review the authentication settings 2. Ensure that settings for TLS authentication have been enabled 3. Ensure that TLS using the user's PKI certificate is the only authentication method permitted 4. On the UE, review the browser authentication settings 5. Ensure the browser supports TLS authentication and the proper TLS version 6. From a UE, attempt to access web mail using an invalid user certificate 7. Verify the attempted access failed 8. From a UE, attempt to access web mail using a valid user certificate 9. Verify the attempted access succeeded
CAR.4	All DAR layers (application provided or native) must meet the DAR requirements in the [draft] MD PP
	1. Review the DAR requirements in the MD PP 2. Identify all the DAR layers used on the UE 3. Verify all the UE DAR layers meet the requirements as specified in the MD PP

CAR.5	If the web mail replacement is a thin client – all enterprise data (for example, temporary files, history, etc.) shall only be saved to RAM
	1. On the UE's browser, review the settings for browsing privately (i.e. web activity is not saved to local nonvolatile storage.) a. Note that some browsers and versions may not support this function 2. Enable the setting that forces the browser into private browsing each time the browser is launched 3. Close/relaunch the browser and verify the browser launched automatically into private browsing mode
CAR.6	If the web mail replacement is a thick client – the application must provide a DAR layer independent of the platform DAR layer
	1. On the UE, identify the mail application and determine how and where the files and other data are stored 2. Ensure the mail application or other application encrypts the stored mail application data 3. Verify the mail data encryption process is independent of any other encryption process (i.e. the mail encryption process is not used by any other process). 4. Exit the web mail application or browser and review the local directory where the mail data are stored 5. Verify the mail files are encrypted/inaccessible
CAR.7	If the web mail replacement is a thick client – the application must meet the Application PP (in progress)
	1. Review the requirements in the Application PP 2. Identify the mail client 3. Verify the mail client meets the requirements as specified in the Application PP
CAR.8	If the web mail replacement is a thick client – the application must meet all isolation requirements in the MD PP
	1. Review the requirements in the MD PP 2. Identify the mail client 3. Verify the mail client meets the requirements as specified in the Isolation PP
BSP	**Basic Security Policy**
BSP.1	The User Equipment shall employ physical tamper protection that is visually inspectable by the user
	1. Identify the physical tamper protections employed to protect the UE 2. Inspect the physical tamper protections 3. Identify how the physical tamper protections would appear if physical tampering were to occur 4. Verify the UE employs physical tamper protections and that there is no evidence of physical tampering
BSP.2	The User Equipment shall be configurable to disable Over the Air (OTA) software/firmware updates from non-authorized sources

	1. Identify what authorized sources are allowed to update software/firmware OTA 2. On the UE, identify what entities the device trusts 3. Remove from the device those trusted entities that are not authorized sources of updates a. Remove update agents b. Remove digital certificates c. Remove applications d. Disable configuration settings 4. Verify all unauthorized trust relationships are removed from the UE
BSP.3	The User Equipment shall employ active electronic/logical tamper indicating technology
	1. Identify what active electronic/logical tamper indicating technologies are employed by the UE 2. Identify the notifications generated by each of the active electronic/logical tamper indicating technologies 3. Identify actions the UE takes to mitigate compromise when an active electronic/logical tamper indicating technology flags a suspicious event 4. Verify the technologies implemented and the actions taken provide the necessary amount of protections required
BSP.4	The User Equipment shall be configurable to disable Over the Air (OTA) carrier commands that are not required for the phone to access the carrier network.
	1. Identify what OTA commands are necessary for the UE to access the carrier's network 2. On the UE, review the list of available commands enabling the UE to connect to the carrier's network 3. Remove from the UE any commands not required for connecting to the carrier's network
BSP.5	The User Equipment shall be configurable to trigger a wipe process
	1. Identify what trigger events will cause the UE's memory to be wiped 2. Ensure the UE's settings are enabled to wipe the memory when a trigger occurs 3. On the UE, trigger an event that will wipe the memory 4. Verify the UE's memory was wiped upon triggering a memory wiping event
HRT	**Hardware Root of Trust[4]**
HRT.1	The User Equipment shall generate integrity measurements of critical software prior to load and on demand

[4] Hardware Root of Trust requirements listed in this section are intended to be part of a set of recommendations eventually included in NIST SP 800-164. When NIST SP 800-164 recommendations are finalized, they will be included in this Mobility Security Guide by reference.

	1. Identify how the UE generates integrity measurements 2. Identify how software is loaded onto the UE and registered as trusted 3. Identify the database containing the integrity measurements of trusted code 4. Load trusted code onto the UE 5. Execute the code 6. Verify the UE executes the code without error 7. Load untrusted code onto the UE 8. Execute the untrusted code 9. Verify the untrusted code does not execute and generates a warning/error stating the code is untrusted 10. On the UE, select a program and generate an integrity report without attempting to execute the code 11. Verify an integrity report is generated stating whether the code is trusted
HRT.2	The User Equipment shall provide protected storage and authorized access to and use of critical integrity measurements for enterprise assertions[5]
	1. Identify what integrity measurements are generated by the UE for enterprise assertion 2. Identify how the generated integrity measurements are used for enterprise assertion 3. Identify where the UE stores the generated integrity measurements 4. As a user of the UE, attempt to access the location where the integrity measurements are stored 5. Verify users do not have access to the integrity measurements storage location
HRT.3	The User Equipment shall provide identity information rooted in hardware to enable authentic and non-repudiable enterprise assertions
	1. Identify the UE hardware (e.g. TPM) that contains its identity information 2. Identify how the UE identity information is used to enable authentic and non-repudiable enterprise assertion. 3. Attempt to connect the UE to the enterprise using the identity information that is rooted in the UE hardware 4. Verify the connection was successful using the UE's hardware identity information

B.8 Test Criteria for User Equipment Monitoring Service Requirements

Table 19: User Equipment Monitoring Service Requirements Test Criteria

Requirement Number	Test Criteria
	User Equipment Monitoring Service Requirements
UEA.01	*Withdrawn*
UEA.02	*Withdrawn*
UEA.03	*Withdrawn*

[5] Protection Profile requirements are interpreted to require CNSSP 15 approved algorithms for integrity measurements, digital signature verification, authenticity, and verification functions. Therefore all hardware root of trust functions will be expected to meet CNSSP 15 standards.

Requirement Number	Test Criteria
UEA.04	*Withdrawn*
UEA.05	*Withdrawn*
UEA.06	*Withdrawn*
UEA.07	*Withdrawn*
UEA.08	*Withdrawn*
UEA.09	*Withdrawn*
UEA.10	*Withdrawn*
UEA.11	*Withdrawn*
UEA.12	*Withdrawn*
UEA.13	*Withdrawn*
UEA.14	*Withdrawn*
UEA.15	*Withdrawn*
UEA.16	*Withdrawn*
UEA.17	The User Equipment shall adhere to [final] PP for MD F Requirement[6] FTP_TST_EXT.2.1 (INT-5) 1. Review the FTP_TST_EXT.2.1 (INT-5) requirement in the MD F PP 2. Identify how the UE adheres to the FTP_TST_EXT.2.1 (INT-5) requirement 3. Verify the UE meets the FTP_TST_EXT.2.1 (INT-5) requirements as specified in the MD PP
UEA.18	The User Equipment shall alert the MDM Agent following [final] PP for MD F Requirement FPT_NOT_EXT.1.1 (INT-3) when a TSF software integrity verification failure has occurred. 1. Identify the UE's critical software used to generate integrity measurements 2. Make an alteration/corruption to a critical piece of software 3. Reboot the UE and/or connect it to the enterprise 4. Verify the UE generated an alert based on the software change in accordance with MD F PP FPT_NOT_EXT.1.1 (INT-3) requirements
UEA.19	The MDM Agent shall transmit alert to the MDM Server under [draft] MDM PP FAU_ALT_EXT.1.1 Assignment: "Transmit all critical software integrity measurements". 1. Identify the UE's critical software used to generate integrity measurements 2. Confirm the MDM Agent and MDM Server and the communication between them 3. Connect the UE to the enterprise and, if necessary, initiate a transmission of integrity information over the MDM channel 4. Review the UE integrity data captured by the MDM Server 5. Verify the MDM Server captured the UE's integrity data and the data meets the requirements of the MDM PP
UEA.20	The MDM Agent shall query the operating system using [draft] MDM PP FMT_SMF.1(2) Assignment: "Query integrity of critical software".

[6] This requirement (both for boot verification and for integrity checking for AP and BP software/firmware) reflects the spirit of requirements expected to be included in NIST SP 800-164 at some future date. Adherence to NIST SP 800-164 as well as all applicable PPs, is a requirement of this security guide.

Requirement Number	Test Criteria
	1. Identify the UE's critical software used to generate integrity measurements 2. Confirm the MDM Agent and MDM Server and the communication between them 3. Connect the UE to the enterprise and, if necessary, force the MDM Server to request integrity information from the UE over the MDM channel 4. Review the UE integrity data captured by the MDM Server 5. Verify the MDM Server captured the UE's integrity data and the data meets the requirements of the MDM PP
UEA.21	The MDM Server shall submit a request to the MDM Agent using [draft] MDM PP FMT_SMF.1.1(1) Assignment: "Query integrity of critical software".
	1. Identify the UE's critical software used to generate integrity measurements 2. Confirm the MDM Agent and MDM Server and the communication between them 3. Connect the UE to the enterprise and, if necessary, force the MDM Server to request integrity information from the UE over the MDM channel 4. Review the UE integrity data captured by the MDM Server 5. Verify the MDM Server captured the UE's integrity data and the data meets the requirements of the MDM PP
UEA.22	*Withdrawn*
UEA.23	The Enterprise Mobility System shall be capable of automatically notifying the operator of User Equipment of the highest-level classification supported by the connection to another device.
	Same as SVP.11
UEA.24	The device shall alert on and log any attempt to circumvent [final] PP for MD F Requirement FDP_IFC_EXT.1.1 (IFC-1) as represented in UEA.28
	1. Attempt to circumvent FDP_IFC_EXT.1.1 (IFC-1). 2. Verify that the device logs the attempt 3. Verify that the device alerts on the attempt 4. Verify that the device alert is transmitted to the enterprise
UEA.25	*Withdrawn*
UEA.26	*Withdrawn*
UEA.27	The device shall provide the user and administrator with the ability to view certificates stored on the device.
	1. Identify where on the device are stored the digital certificates 2. As administrator log into the device and review each certificate's information 3. As user, log into the device and review each certificate's information 4. Verify each certificate was viewable by both user and administrator roles
UEA.28	The User Equipment shall adhere to [final] PP for MD F Requirement FDP_IFC_EXT.1.1 (IFC-1)
	1. Test cases will be released in a later version of this document.

B.9 Test Criteria for Infrastructure Requirements

Table 20: Infrastructure Test Criteria

Requirement Number	Test Criteria
	Enterprise Mobility Infrastructure Boundary Protection Requirements
IFB.01	The Enterprise Mobility Infrastructure shall implement Border Routers at public network boundaries to perform network address translation (NAT).
	1. Identify the locations the Enterprise Mobility Infrastructure network interfaces with a public network 2. Verify a NAT enabled border router exists between that Enterprise Mobility Infrastructure and public networks a. Review the border router's network configuration file b. Ensure the router is configured for NAT
IFB.02	The Enterprise Mobility Infrastructure shall implement Network IDS/IPS in accordance with applicable DoD or using agency policy and guidance.
	1. Identify the network IDS/IPS platform in the Enterprise Mobility Infrastructure 2. Identify applicable DoD or using agency policy and guidance 3. Review the IDS/IPS configuration 4. Verify the IDS/IPS implements applicable DoD or using agency policy and guidance
IFB.03	The Enterprise Mobility Infrastructure shall implement Network Firewalls in accordance with applicable DoD or using agency policy and guidance.
	1. Identify the network firewall platforms in the Enterprise Mobility Infrastructure 2. Identify applicable DoD or using agency policy and guidance 3. Review the firewall configurations 4. Verify the firewalls implement applicable DoD or using agency policy and guidance
	Enterprise Mobility Infrastructure Host System Requirements
IFH.01	Each host system in the Enterprise Mobility Infrastructure shall report platform status in accordance with applicable DoD or using agency policy and guidance.
	1. Identify to where each host system reports a. Ensure each host generates a report 2. Identify applicable DoD or using agency policy and guidance 3. Review the host reports a. What is reported b. Report frequency c. Report format d. Classification markings 4. Verify reporting meets the guidance specified in applicable DoD or using agency policy

IFH.02	An Infrastructure Host System shall authenticate users in accordance with applicable DoD or using agency policy and guidance.
	1. Identify the host systems on the Enterprise Mobility Infrastructure 2. Identify applicable DoD or using agency policy and guidance 3. Attempt to log onto the host system 4. Verify the host authentication meets applicable DoD or using agency policy and guidance
IFH.03	An Infrastructure Host System shall prohibit unauthorized users from accessing resources.
	1. On an Infrastructure Host System, log in using valid user credentials 2. Attempt to perform a system administrator action 3. Verify the action was rejected due to insufficient privileges 4. Suspend user account access 5. Log out of the account 6. Attempt to log back in with now suspended account credentials 7. Verify user login was rejected due to invalid login credentials
IFH.04	An Infrastructure Host System shall maintain separation of user roles.
	1. On an Infrastructure Host System, enter valid user credentials 2. Determine what actions are permitted for the user 3. Perform an action for which the user is not authorized a. System admin actions b. Webpage access c. Command line execution 4. Verify the user received a rejection message stating the action was not authorized
IFH.05	An Infrastructure Host System shall audit actions taken by users (types of actions and content of audit record are configurable) in accordance with applicable DoD or using agency policy and guidance.
	1. Identify the host systems on the Enterprise Mobility Infrastructure 2. Configure the host systems to audit user actions a. Follow applicable DoD or using agency policy and guidance for what actions are auditable 3. Log onto the host system a. User account b. Admin account 4. Perform an auditable action 5. Review the audit log 6. Verify auditable activities were logged by the host system in accordance with applicable DoD or using agency policy and guidance

IFH.06	An Infrastructure Host System shall perform anti-malware detection or have an anti-malware service installed and configured in accordance with applicable DoD or using agency policy and guidance.

	1. On the host system, identify the anti-malware service
	  a. Resident on the host using a local service
	  b. Remote service through a network connection
	2. Identify applicable DoD or using agency policy and guidance
	3. Scan the host system using the anti-malware service
	  a. Open the local service anti-malware interface and start a scan
	  b. Connect the host to the network and from the remote scanning service launch a scan of the host
	4. Verify the host was successfully scanned by the service in accordance with applicable DoD or using agency policy and guidance

IFH.07	An Infrastructure Host System shall have a host-based firewall installed and configured in accordance with applicable DoD or using agency policy and guidance.
	1. Identify the firewall service on the host system 2. Configure the host firewall in accordance with applicable DoD or using agency policy and guidance 3. Change the firewall configuration to block a required service to the host 4. Verify the required service fails to work properly 5. Change the firewall configuration to restore the required service 6. Verify all required services are working properly and the firewall is configured in accordance with applicable DoD or using agency policy and guidance
IFH.08	An Infrastructure Host System shall have a host-based IDS/IPS installed and configured in accordance with applicable DoD or using agency policy and guidance.
	1. Identify the IDS/IPS service on the host system 2. Configure the host IDS/IPS in accordance with applicable DoD or using agency policy and guidance 3. On the host, perform an action that will be captured by the IDS/IPS 4. Review the IDS/IPS audit report 5. Verify the IDS/IPS captured the incident and that the IDS/IPS is configured in accordance with applicable DoD or using agency policy and guidance
IFH.09	An Infrastructure Host System shall verify the integrity of its software environment.
	1. Identify the host service that verifies installed software 2. Ensure software installation and changes requires administrative privileges 3. Ensure software installation requires digital certificate integrity checks 4. Download an approved and unapproved software package onto the host 5. Attempt to install the approved and unapproved software programs 6. Verify the approved package was accepted for install and the unapproved package was rejected

IFH.10	An Infrastructure Host System shall implement hardware roots of trust for performing integrity verification and reporting (attestation).
	1. For each Infrastructure Host, identify the hardware root of trust 2. Review how the Infrastructure Host performs integrity verification measurements 3. Review how the Infrastructure Host performs integrity reporting 4. Identify where the Infrastructure Hosts sends its integrity reports 5. Verify that each Infrastructure Host performs and reports integrity verification measurements
	Enterprise Mobility Infrastructure Management Requirements
IFM.01	The Enterprise Mobility Infrastructure Management Services shall provide scheduled virus signature updates automatically to infrastructure components running anti-virus software in accordance with applicable DoD or using agency policy and guidance.
	1. Identify Enterprise Mobility Infrastructure Host Security Manager for antivirus distribution 2. Configure the Host Security Manager to automatically update network clients a. Set the update scheduling in accordance with applicable DoD or using agency policy and guidance 3. Identify the client infrastructure components and ensure they are running antivirus software 4. Configure the clients to receive the automatic antivirus signature updates from the distribution server 5. Push an updated anti-virus signature file 6. Verify the clients were automatically updated with the most recent signatures
IFM.02	The Enterprise Mobility Infrastructure Management Services shall be configured to receive, authenticate, and validate software updates received indirectly via the Internet (e.g., via the Internet Download Server) or directly from applicable vendors in accordance with applicable DoD or using agency policy and guidance.

	1. Download an approved and unapproved software package to the Enterprise Mobility Infrastructure Management Services system
	  a. Use vendor signed packages for approved software
	  b. Use unsigned or unapproved vendor for unapproved software
	2. Scan the software packages for malware
	3. Launch the unapproved software package
	4. Verify the system rejects the software due to the system's inability to authenticate the package
	5. Launch the approved software package
	6. Verify the system is able to authenticate the package and accepts the software

IFM.03	The Enterprise Mobility Infrastructure Management Services shall track the Configuration Management status of infrastructure components in accordance with applicable DoD or using agency policy and guidance.
	1. Identify the Enterprise Mobility Infrastructure Management Services system 2. Configure the system to receive configuration management reports from infrastructure hosts 3. Configure infrastructure hosts to send configuration management information to the Enterprise Mobility Infrastructure Management Services system 4. Review the configuration management reports received by the Enterprise Mobility Infrastructure Management Services system 5. Verify hosts are reporting their configuration management status to the Enterprise Mobility Infrastructure Management Services system in accordance with applicable DoD or using agency policy and guidance
IFM.04	The Enterprise Mobility Infrastructure Management Services shall provide scheduled intrusion detection signature updates automatically to infrastructure components running host-based IDS/IPS software in accordance with applicable DoD or using agency policy and guidance.
	1. Identify Enterprise Mobility Infrastructure Host Security Manager for IDS/IPS signature distribution 2. Configure the Host Security Manager to automatically update network clients a. Set the update scheduling in accordance with applicable DoD or using agency policy and guidance 3. Identify the client infrastructure components and ensure they are running IPS/IDS software 4. Configure the clients to receive the automatic IDS/IPS signature updates from the distribution server 5. Push an updated anti-virus signature file 6. Verify the clients were automatically updated with the most recent signatures
IFM.05	The Enterprise Mobility Infrastructure Management Services shall create and distribute firewall policies to infrastructure components running host-based firewall software in accordance with applicable DoD or using agency policy and guidance.
	1. Identify Enterprise Mobility Infrastructure Host Security Manager for firewall policy distribution 2. Configure the Host Security Manager to automatically update network clients a. Set the update scheduling in accordance with applicable DoD or using agency policy and guidance 3. Identify the client infrastructure components and ensure they are running a host-based firewall 4. Create a firewall policy in accordance with applicable DoD or using agency policy and guidance 5. Configure the clients to receive the automatic firewall policy updates from the distribution server 6. Push an updated firewall policy file 7. Verify the clients were automatically updated with the most recent policy

IFM.06	The Enterprise Mobility Infrastructure Management Services shall create and distribute firewall policies to network-based firewall components in accordance with applicable DoD or using agency policy and guidance.
	1. Identify Enterprise Mobility Infrastructure Host Security Manager for firewall policy distribution 2. Configure the Host Security Manager to automatically update network-based firewall appliances a. Set the update scheduling in accordance with applicable DoD or using agency policy and guidance 3. Identify the network-based firewall components 4. Create a firewall policy in accordance with applicable DoD or using agency policy and guidance 5. Configure the network-based firewall components to receive the automatic firewall policy updates from the distribution server 6. Push an updated firewall policy file 7. Verify the network-based firewall components were automatically updated with the most recent policy
IFM.07	The Enterprise Mobility Infrastructure Management Services shall be configured to receive, authenticate, and validate virus and IDS/IPS signatures received indirectly via the Internet (e.g., via the Internet Download Server) or directly from applicable vendors in accordance with applicable DoD or using agency policy and guidance.

	1. Acquire virus and IDS/IPS signature update packages from an approved source
	  a. Download from vendor's Internet website
	  b. Media provided by the vendor
	2. Configure the Enterprise Mobility Infrastructure Management Services system to receive, authenticate and validate IPS/IDS signature packages
	3. Verify the signatures from approved sources are accepted by the Enterprise Mobility Infrastructure Management Server

IFM.08	The Enterprise Mobility Infrastructure Management Services shall securely configure, manage, and monitor all networking components (e.g., switches, routers, firewalls) in accordance with applicable DoD or using agency policy and guidance.
	1. Identify all networking components in the Enterprise Mobility Infrastructure 2. Configure Management Services to configure, manage and monitor the identified components 3. Create a configuration file and push the configuration to the appropriate network component 4. Verify the network components implemented the newly pushed configuration 5. Review the Management Services' monitoring and management functions 6. Verify the monitoring report reflects the state and operation of the monitored and managed network components

IFM.09	The Enterprise Mobility Infrastructure Management Services shall remotely install software updates on infrastructure components in accordance with applicable DoD or using agency policy and guidance.
	1. Download an approved software update package onto the Enterprise Mobility Infrastructure Management Services system 2. Configure the Management Services system to update software packages on required infrastructure components in accordance with applicable DoD or using agency policy and guidance 3. Indentify infrastructure components requiring the software update 4. Use the Management Services system to push the software update to the infrastructure components 5. Verify the infrastructure components installed the software updates
IFM.10	The Enterprise Mobility Infrastructure Management Services shall be configured in accordance with applicable DoD or using agency policy and guidance.
	1. Identify all the Enterprise Mobility Infrastructure Management Services 2. Review the Management Services configuration 3. Verify Management Services is configured in accordance with applicable DoD or using agency policy and guidance
IFM.11	The Enterprise Mobility Infrastructure Management Services shall be configured to provide mobile application vetting to support application whitelisting efforts.
	1. Identify where on the Enterprise Mobility Infrastructure (EMI) the mobile application vetting Management Service is performed 2. Identify how the Management Service vets mobile applications and develops an application whitelist 3. Identify how the Management Service receives application information from the mobile device 4. Identify how the Management Service reports back to the mobile device and updates the application whitelist 5. Identify the application while list on the mobile device 6. Verify the mobile device uses application vetting information to restrict mobile device execution to only those applications identified on a whitelist and that the whitelist is updated by the EMI.
	Enterprise Mobility Infrastructure Security Services Requirements
IFS.01	The Enterprise Mobility Infrastructure Security Services shall record audit events reported by infrastructure components.
	1. Identify the Enterprise Mobility Infrastructure Security Services system 2. Review the infrastructure component audit records that were reported to the Enterprise Mobility Infrastructure Security Service 3. On an infrastructure component, perform an auditable event 4. Verify the infrastructure component reported the audited event to the Security Services system

IFS.02	The Enterprise Mobility Infrastructure Security Services shall provide integrity protection of audit records in transit from infrastructure components.
	1. Identify the Enterprise Mobility Infrastructure Security Services system 2. Review the connection details between the Security Services system and the infrastructure components for transferring audit records 3. Verify the connection is protected from modification a. Connection is encrypted b. Audit record is digitally signed
IFS.03	The Enterprise Mobility Infrastructure Security Services shall provide integrity protection of audit records at rest.
	1. Identify the Enterprise Mobility Infrastructure Security Services system audit records 2. Attempt to modify the records a. Delete records b. Alter records c. Add records 3. Verify actions taken to modify records require administrative privileges a. Records are read only for unprivileged users and digitally signed
IFS.04	The Enterprise Mobility Infrastructure Security Services shall support Windows Domain authentication if the infrastructure includes components running Microsoft Windows.
	1. Identify components running Microsoft Windows operating systems 2. Verify the Enterprise Mobility Infrastructure Security Services is using Windows Domain authentication for those components running Microsoft Windows
IFS.05	The Enterprise Mobility Infrastructure Security Services shall support Kerberos authentication if the infrastructure includes components running Linux.
	1. Identify components running Linux based operating systems 2. Verify the Enterprise Mobility Infrastructure Security Services is using Kerberos authentication for those components running Linux
IFS.06	The Enterprise Mobility Infrastructure Security Services shall support Remote Authentication Dial In User Service (RADIUS) authentication if required by the system design (e.g., to support the SIP Service).
	1. Determine if system design requires RADIUS authentication 2. Identify the RADIUS Remote Access Server 3. Review the configurations for the VPN, network switch and network access server 4. Ensure the RADIUS protocol is enabled 5. Verify network logon uses RADIUS for authentication a. Review the RADIUS logs for confirmation of RADIUS authentication
IFS.07	The Enterprise Mobility Infrastructure Security Services shall require the authentication of users based on user id and password.
	1. Log into an Enterprise Mobility Infrastructure component 2. Verify the logon requires a unique user id and password

IFS.08	The Enterprise Mobility Infrastructure Security Services shall authorize access by an authenticated user based on a black or white list.

	1. Identify Enterprise Mobility Infrastructure authorization services
	  a. Logon authorization
	  b. Service authorization (HTTP, File Transfer Protocol (FTP), email, group etc…)
	2. Identify a test user and remove authorization to some service for that user
	  a. Add to an unauthorized list (black list)
	  b. Remove from an authorized list (white list)
	3. As the test user, attempt to access the service
	4. Verify access to the service was rejected as unauthorized

IFS.09	The Enterprise Mobility Infrastructure Security Services shall audit all authentication and authorization failures.

	1. Configure the Enterprise Mobility Infrastructure Security Services to log authentication and authorization errors
	2. Perform actions on the network (system) that cause authentication and authorization failures
	  a. Attempt to logon to the network (system) with invalid credentials
	  b. After successful logon to the network (system) attempt to access a service to which the user is not authorized
	3. Verify the audit log captured the authentication and the authorization failures

IFS.10	The Enterprise Mobility Infrastructure Security Services shall be configured to audit selected authentication and authorization successes in accordance with applicable DoD or using agency guidance.

	1. Configure the Enterprise Mobility Infrastructure Security Services to log successful authentication and authorization activities as specified in applicable DoD or using agency guidance
	2. Perform actions on the network (system) that result in authentication and authorization successes
	  a. Logon to the network (system) with valid credentials
	  b. Access an audited authorized service
	3. Verify the audit log captured the authentication and the authorization successes

IFS.11	The Enterprise Mobility Infrastructure Security Services shall require authentication and authorization for users to view, modify, delete, or backup audit records.

	1. Identify the Enterprise Mobility Infrastructure Security Services system audit records
	2. Access audit records by logging onto the system using unique credentials
	3. Attempt to modify the records
	  a. Delete records
	  b. Alter records
	  c. Add/Backup records
	  d. View records
	4. Verify actions taken to modify records require appropriate authorization such as administrative privileges

	Enterprise Mobility Infrastructure Architecture Requirements
IFA.01	The Enterprise Mobility Infrastructure shall implement Directory Services for authentication.
	1. Identify the Enterprise Mobility Infrastructure Directory Services Server 2. Configure the Directory Services for user authentication to the Domain 3. From an Enterprise Mobility Infrastructure client, logon using valid credentials a. Ensure logon is to the Domain and not local 4. Verify successful authentication to the domain using directory services a. Ensure enterprise services are available
IFA.02	The Enterprise Mobility Infrastructure shall implement audit and logging for all network systems and hosts in accordance with applicable DoD or using agency policy and guidance.
	1. Configure Enterprise Mobility Infrastructure audit server to receive and store audit logs from systems and hosts 2. Configure the Enterprise Mobility Infrastructure systems and hosts to audit and transmit events to the audit server in accordance with applicable DoD or using agency policy and guidance 3. On a system or host, cause an auditable event 4. Verify the audit server received and stored the auditable event
IFA.03	The Enterprise Mobility Infrastructure shall provide DNSSEC Servers within the infrastructure networks.
	1. Identify the Domain Name Servers (DNS) on the Enterprise Mobility Infrastructure network 2. Ensure the DNS zones are signed by the appropriate certificates 3. Verify the DNSSEC setting is enabled a. Review the DNS Server logs to see if DNSSEC is implemented and active
IFA.04	The Certificate Validation Service shall validate X.509 certificates.
	1. Identify the certificates used by Certificate Validation Service 2. Review the properties of those certificates 3. Verify the certificates' structure and fields comply with IETF RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"
IFA.05	The Enterprise Mobility Infrastructure shall require authentication and authorization of users to stop, start, or change configuration for servers or services.
	1. Configure Enterprise Mobility Infrastructure Servers to require authentication and authorization to change configuration settings or the state of services 2. Logon to an Enterprise Mobility Infrastructure Server as a non-administrative, unauthorized user 3. Attempt to alter configuration files and services a. Delete configuration file b. Modify configuration file c. Turn off the auditing service d. Change the time e. Stop system processes 4. Verify attempts to alter configuration files and service states failed for an unauthorized user

IFA.06	The Enterprise Mobility Infrastructure Security Services shall be configured to enable posting of full CRLs to the Directory Service.
	1. Identify Enterprise Mobility Infrastructure Directory Service 2. Post a full CRL to the Directory Service 3. Identify a revoked certificate reported in the posted CRL 4. Attempt to use the revoked certificate 5. Verify that authorization/authentication was rejected due to the revoked certificate
IFA.07	The Enterprise Mobility Infrastructure Security Services shall be configured to enable posting of delta CRLs to the Directory Service.
	1. Identify Enterprise Mobility Infrastructure Directory Service 2. Post a delta CRL to the Directory Service 3. Identify a revoked certificate reported in the posted delta CRL 4. Attempt to use the revoked certificate 5. Verify that authorization/authentication was rejected due to the revoked certificate
IFA.08	The Enterprise Mobility Infrastructure Security Services shall include a Certificate Validation Service.
	1. Identify the Enterprise Mobility Infrastructure Server implementing certificate validation services 2. Identify what the certificate validation service is a. Certificate Revocation List (CRL) b. Online Certificate Status Protocol (OCSP) c. Server-based Certificate Validation Protocol 3. Verify the Enterprise Mobility Infrastructure includes a Certificate Validation Service
	Enterprise Mobility Infrastructure Networking Services Requirements
IFN.01	The Enterprise Mobility Infrastructure shall provide DNS Servers within the infrastructure networks.
	1. Identify the DNS Servers on the Enterprise Mobility Infrastructure network 2. Ensure infrastructure components are configured to use the DNS Servers 3. On an infrastructure component, perform a DNS lookup command 4. Verify the results are from the DNS Server
IFN.02	The Enterprise Mobility Infrastructure shall provide Network Time Servers that provide time synchronization within the infrastructure networks.
	1. Identify the time servers on the Enterprise Mobility Infrastructure 2. Review the configuration files on infrastructure components requiring use of the timing servers 3. Verify the configuration files point (IP address, port) to the Enterprise Mobility Infrastructure timing servers to receive their timing synchronization

IFN.03	The Enterprise Mobility Infrastructure Directory Service shall require user authentication and authorization to perform creation, deletion, or modification of directory entries or attributes.
	1. Configure Enterprise Mobility Infrastructure directory servers to require authentication and authorization to change entries or attributes 2. Logon to an Enterprise Mobility Infrastructure directory server as an unprivileged user 3. Attempt to alter directory service entries or attributes a. Create entries b. Delete entries c. Modify entries d. Modify an entry's attributes 4. Verify attempt to alter directory service entries and attributes failed for an unprivileged user
IFN.04	The Enterprise Mobility Infrastructure Directory Services shall be configured to require user authentication and authorization to read directory entries or attributes.
	1. Configure Enterprise Mobility Infrastructure directory servers to require authentication and authorization to view entries or attributes 2. Logon to an Enterprise Mobility Infrastructure host with access to directory services as an unprivileged user that is not authorized to access directory services 3. Attempt to view directory service entries or attributes 4. Verify attempt to view directory service entries and attributes failed for an unauthorized user 5. Logon to an Enterprise Mobility Infrastructure host with access to directory services as an unprivileged user that is authorized to access directory services 6. Verify attempt to view directory service entries and attributes succeeded for an authorized user
IFN.05	The Enterprise Mobility Infrastructure Directory Services shall be configured to allow storage of X.509 certificates.
	1. Identify Enterprise Mobility Infrastructure Directory Services Server 2. Load into the appropriate directory on the server an X.509 certificate 3. Verify the X.509 certificate is available to Directory Services resident on the server
IFN.06	The Enterprise Mobility Infrastructure Directory Services shall be configured to allow storage of X.509 CRLs.
	1. Identify Enterprise Mobility Infrastructure Directory Services Server 2. Load into the appropriate directory on the server an X.509 Certificate Revocation List (CRL) 3. Verify the CRL is available to Directory Services resident on the server
IFN.07	The Enterprise Mobility Infrastructure shall require authentication and authorization of a user to stop, start, or change configuration for servers or services.
	1. Same as IFA.05

B.10 Test Criteria for PKI Requirements

Table 21: PKI Test Criteria

Requirement Number	Test Criteria
	Certificate, Key, and Trust Management
ECA.01	The Certificate Authority cryptomodule shall be FIPS 140-2 compliant.
	1. Identify the Certificate Authority and the cryptomodule(s) it uses 2. Review the cryptomodule documentation and identify the FIPS-140 certificate number(s) 3. Verify the certificate numbers appear on NIST's FIPS 140-2 validation list
ECA.02	A Certificate Authority service shall be configured to generate user certificates.
	1. On the certificate authority, create a user certificate 2. Install the created certificate on a User Equipment 3. Connect the User Equipment to the Enterprise Mobility Infrastructure 4. Verify the User Equipment successfully authenticated to the network using the created certificate
ECA.03	A Certificate Authority service shall be configured to accept a common specified field (e.g., DoD Electronic Data Interchange Personnel Identifier, EDI PI) as part of the Distinguished Name (DN) for user certificates.
	1. Identify the Certificate Authority Server 2. Configure the Certificate Authority to create a Distinguished Name (DN) based on a common specified field 3. Enter the required value into the common specified field 4. Create a user certificate 5. Verify the user certificate's DN contains the required value
ECA.04	The Certificate Authority service shall maintain a data store of all certificates it has issued including date of issuance and current status.
	1. Identify the Certificate Authority Server containing stored certificates 2. Create a user certificate and place in the certificate store 3. Find the newly created certificate and review its properties 4. Verify the certificate properties contain the date of issuance and current status
ECA.05	The Certificate Authority service shall maintain a Certificate Revocation List (CRL).

	1. Identify the Certificate Authority Server
	2. Identify the CRL on the server
	  a. If a CRL does not exist create one
	3. Verify the Certificate Authority maintains CRLs
	  a. Create a user certificate
	  b. Revoke the user certificate
	  c. Verify that the revoked certificate appears on the CRL when the CRL is generated by the Certificate Authority Service

ECA.06	The Certificate Authority service shall process certificate revocation requests.
	1. Identify the Certificate Authority Server 2. Create a CRL on the server 3. Publish the CRL 4. Attempt to use a certificate that was revoked through the published CRL 5. Verify use of the certificate was rejected because it was revoked

Requirement Number	Test Criteria
ECA.07	The Certificate Authority service shall be configured to process PKCS #7 and #10 messages.
	1. Identify the Certificate Authority Server 2. Configure the Certificate Authority to handle PKCS #7 and #10 messages 3. On a local machine connected to the Certificate Authority, such as the Enrollment Workstation, create a cryptographic request a. Generate the Certificate Signing Request (CSR) (i.e. PKCS #10 message) b. Send the CSR to the Certificate Authority 4. Verify the Certificate Authority generates and returns a signed X.509 formatted public certificate with extension *.p7b
ECA.08	The Certificate Authority shall be capable of generating certificates for the digital signature algorithms as defined in CNSSP-15, Annexes B and C.
	1. Identify the Certificate Authority Server 2. Identify the algorithms in CNSSP-15 appropriate to the classification level of the data 3. Configure the server to generate certificates using the required algorithm and key strength 4. Generate a certificate 5. Review the generated certificate's properties 6. Verify the digital signature algorithm and key strength meet the requirements as specified in CNSSP-15 for the appropriate classification of the data
	Enrollment Workstation Requirements
EWS.01	The Enrollment Workstation shall be able to accept entry of requests for device certificates.
	1. On the Enrollment Workstation, create a device certificate request 2. Review the certificate that is created 3. Verify the certificate meets the requirements for device certificates a. Format b. Cryptographic strength c. Unique identification
EWS.02	The Enrollment Workstation shall be configurable to define and enforce complexity policies for the secret value (PIN, passphrase, or password) used to protect sensitive key material.
	1. Configure the Enrollment Workstation to create certificates with a PIN, passphrase, or password that meet applicable complexity policies 2. On the Enrollment Workstation, create a device certificate 3. When prompted for a PIN, passphrase, or password enter a password that does not meet the defined complexity requirements 4. Verify the invalid entry was rejected and the user is prompted to reenter another value 5. Enter a PIN, passphrase, or password that meets the defined complexity requirements 6. Verify the valid entry is accepted and the certificate is created

EWS.03	The VoIP Enrollment Workstation shall be able to accept entry of requests for user certificates.
	1. On the Enrollment Workstation, create a user certificate request 2. Review the certificate that is created 3. Verify the certificate meets the requirements for user certificates a. Format b. Cryptographic strength c. Unique identification
EWS.04	The Enrollment Workstation shall be able to interface to non-secure removable media.
	1. Identify the Enrollment Workstation and its removable media drives 2. Insert removable media into the appropriate Enrollment Workstation drive 3. Navigate to the removable media's path 4. Transfer a file to the removable media 5. Verify the file was saved to the removable media
EWS.05	The Enrollment Workstation shall generate certificates for the digital signature algorithms defined in CNSSP-15, Annex C.
	1. Identify the Enrollment Workstation Server 2. Identify the digital signature algorithms in CNSSP-15, Annex C appropriate to the classification level of the data 3. Configure the Enrollment Workstation to generate certificates using the required algorithm and key strength 4. Generate a certificate 5. Review the generated certificate's properties 6. Verify the generated certificate's digital signature algorithm and key strength meet the requirements as specified in CNSSP-15, Annex C
EWS.06	The Enrollment Workstation shall generate certificates for the digital signature algorithms defined in CNSSP-15, Annex B.
	1. Identify the Enrollment Workstation Server 2. Identify the digital signature algorithms in CNSSP-15, Annex B appropriate to the classification level of the data 3. Configure the workstation to generate certificates using the required algorithm and key strength 4. Generate a certificate 5. Review the generated certificate's properties 6. Verify the generated certificate's digital signature algorithm and key strength meet the requirements as specified in CNSSP-15, Annex B

B.11 Test Criteria for User Equipment Provisioning Requirements

Table 22: Provisioning Test Criteria

Requirement Number	Test Criteria
	User Equipment Provisioning Requirements
UEP.01	During provisioning any applications, processes, and files that are not essential for operation of the User Equipment shall be removed.
	1. Provision User Equipment in accordance with applicable policy 2. After provisioning, review the applications, processes and files on the User Equipment 3. Verify the applications, processes and files on the User Equipment are required for operation of the device and all others not necessary have been removed
UEP.02	During provisioning of the User Equipment any functionality that would allow an ordinary user of the User Equipment to attain administrative user privileges shall be removed.
	1. Provision User Equipment in accordance with applicable policy 2. After provisioning, review the applications, processes and files on the User Equipment 3. Verify that the only functionality on the User Equipment is essential for operation of the device and does not permit escalation of privileges for non-administrative users
UEP.03	During provisioning and updates of the User Equipment the administrative user shall clear the contents of the cache in order to remove any data associated with the applications that were removed during provisioning or updating the User Equipment.
	1. Provision or update the User Equipment 2. On the User Equipment, obtain administrative permissions 3. Navigate to the global setting for clearing the contents of the cache 4. Clear the contents of the cache 5. Navigate to the location where the cache is stored 6. Verify the contents of the cache were cleared
UEP.04	After provisioning or updating of the User Equipment the administrative user shall reboot the User Equipment in order to have a fresh initialization of the kernel and the applications remaining, as well as a fresh load of the boot image.
	1. Provision or update the User Equipment as required 2. Reboot the User Equipment 3. Ensure the reboot occurs without error 4. Verify the User Equipment reboots back to a known state such as the login screen or welcome screen

Appendix C Functional Requirements - Enterprise Mobility

The requirement priorities are specified based on guidance contained in section 2.1.1 of the Defense Acquisition Guidebook. Based on this guidance, the "Threshold or Objective" column in each table means the following:

- An objective (O) requirement specifies a feature or function that the Government desires and expects.
- A threshold (T) requirement specifies a minimum acceptable feature or function that, in the Government's judgment, still provides the needed capabilities if the corresponding objective requirement cannot reasonably be met (e.g., due to lack of technology maturity, cost or time constraints).

In many cases, the threshold requirement also serves as the objective requirement (T=O). Where both a Threshold requirement and a related Objective requirement exist, the Objective requirement complements the Threshold requirement rather than replaces it. These requirements are intended to provide system acquirers and integrators with guidance on selecting components that will meet the requirements of this security guide. Each requirement is intended to be testable, resulting in a yes/no answer of whether the requirement was met.

Table 23: Appendix C Requirement Designators

Designator	Requirements Addressed
FMOB	Overarching Mobility requirements that a solution fielded using this MSG should implement (**F**unctional **MOB**ility)
FECA	Requirements for PKI (**F**unctional **E**lectronic **C**ertificate **A**uthority)
FEWS	Requirements for configuration of the enrollment workstation (**F**unctional **E**nrollment **W**ork**S**tation)
FIFA	Requirements for basic system architecture (**F**unctional **I**n**F**rastructure **A**rchitecture)
FIFS	Overall requirements for selecting **F**unctional **I**n**F**rastructure **S**ecurity services
FSVC	Requirements for the SVoIP client running on the User Equipment (**F**unctional **SV**oIP **C**lient)
FSVP	Requirements for the overall SVoIP infrastructure that defines the architecture and that will apply to both the client and server (**F**unctional **SV**oI**P**)
FSVS	Requirements for SVoIP Server (**F**unctional **SV**oIP **S**erver)
FUEA	Requirements for monitoring and handling faults on the User Equipment (**F**unctional **U**ser **E**quipment **A**udit)
FUEM	Requirements for user equipment management (**F**unctional **U**ser **E**quipment **M**anagement)
FUEP	Requirements for user equipment provisioning (**F**unctional **U**ser **E**quipment **P**rovisioning)
FUES	Overall requirements for selecting the smartphone User Equipment (**F**unctional **U**ser **E**quipment **Smartphone**)
FVPC	Requirements applicable to the VPN client running on the User Equipment (**F**unctional **VP**N **C**lient)
FVPG	Requirements applicable to the VPN Gateway (**F**unctional **VPN Gateway**)
FVPN	Requirements for designing and implementing the VPN solution that defines the architecture and that will apply to both the client and server (**F**unctional **VPN**)
FWNC	**W**eb Arbitrated **N**on-Resident Data User Equipment **C**lient requirements
FWND	**W**eb Arbitrated **N**on-Resident **D**ata
FWNS	**W**eb Arbitrated **N**on-Resident Data **S**erver requirements

C.1 Overarching Mobility Requirements

Table 24: Overarching Mobility Requirements

Requirement Number	Requirement Description	Threshold/ Objective
FMOB.00	**Overarching Mobility Requirements**	
FMOB.01	Each system shall have the ability to protect certificates along with their corresponding private keys and security critical profiles stored on the system in accordance with protection guidance for the highest level of classification of the system.	T=O
FMOB.02	The system shall meet applicable security requirements and controls as identified in NIST SP 800-53 and applicable DoD (or equivalent agency) policy, directives, or instructions.	T=O
FMOB.03	Each component shall go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's DAA/AO approved Product Supply Chain Threat Assessment process. (See CNSSD 505 *Supply Chain Risk Management (SCRM)* for additional guidance.)	T=O

C.2 VPN Requirements

Table 25: VPN Requirements

Requirement Number	Requirement Description	Threshold/ Objective
FVPN.00	**Overarching VPN Requirements**	
FVPN.01	The VPN Gateway and client shall implement the cipher suites specified in IETF RFC 6379 "Suite B Cryptographic Suites for IPsec"	T=O
FVPN.02	The VPN Gateway and client shall be able to be configurable to prohibit split-tunneling.	T=O
FVPN.03	The VPN Gateway and client shall provide random bit generation services in accordance with NIST SP 800-90.	T=O
FPVN.04	The VPN client shall be capable to automatically reconnect the VPN upon unexpected disconnect.	T=O
FVPC.00	**VPN Client Requirements**	
FVPC.01	The VPN client shall run at the User Equipment operating system level, not as a separate application or service.	T=O
FVPC.02	*Withdrawn, version 2.1*	
FVPG.00	**VPN Gateway Requirements**	
FVPG.01	The VPN Gateway shall be able to audit and report all attempts to establish a security association as either successful or unsuccessful.	T=O
FVPG.02	The VPN Gateway shall support NAT.	T=O
FVPG.03	The VPN Gateway shall be able to configure and assign an internal network private IP address to a VPN client upon successful establishment of a security association.	T=O

Requirement Number	Requirement Description	Threshold/ Objective
FVPG.04	The VPN Gateway shall be configurable to request re-authentication for security associations that have been inactive for a configurable period of time.	T=O
FVPG.05	The VPN Gateway shall be configurable to terminate security associations that have been inactive for a configurable period of time.	T=O
FVPG.06	The VPN Gateway shall be able to perform certificate path validation.	T=O
FVPG.07	The VPN Gateway shall be able to check for revoked certificates using CRLs, OCSP, black lists, and other equivalent mechanism.	T=O
FVPG.08	The VPN Gateway shall be interoperable with commercially available products implementing Certificate Revocation List (RFC5280) or Online Certificate Status Protocol (RFC6277) defined protocols for checking certificate validity.	T
FVPG.09	The VPN Gateway shall be interoperable with commercially available products using Certificate Management Protocol (RFC4210) or Certificate Management over CMS (RFC6402) for the issuance of X.509v3 public key certificates.	T
FVPG.10	*Withdrawn, version 2.1*	
FVPG.11	The VPN Gateway shall be interoperable with applicable existing Public Key Infrastructures (PKIs) for the issuance of public key certificates.	O
FVPG.12	*Withdrawn into PROSE 5.2.4, version 2.2*	O
FVPG.13	*Withdrawn into PROSE 5.2.4, version 2.2*	O
FVPG.14	The VPN Gateway shall be able to check for invalid certificates by retrieving CRL information from an identified data repository within the system or by performing online status validation with a service within the system.	T=O

C.3 Secure Voice over Internet Protocol (SVoIP) Requirements

Table 26: SVoIP Requirements

Requirement Number	Requirement Description	Threshold/ Objective
FSVP.00	**Overarching SVoIP Requirements**	
FSVP.01	The SIP Server shall provide a SIP Proxy Service.	T=O
FSVP.02	The SIP Server shall provide a SIP Registration Service (Registrar).	T=O
FSVP.03	The mobility solution shall protect the SIP communication channel using TLS.	T=O
FSVP.04	The Enterprise Mobility System and User Equipment client shall implement the TLS 1.2 protocol (IETF RFC 5246) supporting Suite B (IETF RFC 6460) cipher suites, using mutual authentication with certificates.	T=O
FSVP.05	The Enterprise Mobility System and User Equipment client shall implement the Session Initiation Protocol (SIP) that complies with IETF RFC 3261.	T=O
FSVP.06	The Enterprise Mobility System and User Equipment client shall implement the SRTP protocol that complies with IETF RFC 4566.	T=O

Requirement Number	Requirement Description	Threshold/ Objective
FSVP.07	The Enterprise Mobility System and User Equipment client shall implement the Session Description Protocol (SDP) Security Descriptions for Media Streams Protocol (SDES) that complies with IETF RFC 4568.	T=O
FSVP.08	Within the Enterprise Mobility System, the User Equipment SVoIP Client and Mobility SIP Server shall provide random bit generation services in accordance with NIST SP 800-90.	T=O
FSVP.09	*Withdrawn into PROSE 3.1.1, version 2.2*	O
FSVP.10	The Enterprise Mobility System shall be capable of automatically notifying the operator of User Equipment of the highest level classification supported by the connection to another device.	O
FSVC.00	**SVoIP Client Requirements**	
FSVC.01	The SVoIP Client shall be capable of assessing credential validation status either by retrieving CRL information from an identified data repository within the SVoIP system or by performing online status validation with a service within the SVoIP system.	O
FSVS.00	**SVoIP Server Requirements**	
FSVS.01	The Mobility SIP Server in the “home” enterprise and the Mobility SIP Server in the far-end enterprise shall use public key cryptography for mutual authentication.	T=O
FSVS.02	The Mobility SIP Server in the “home” enterprise and the Mobility SIP Server in the far-end enterprise shall negotiate AES keys to protect the confidentiality and integrity of TLS traffic.	T=O
FSVS.03	Within the Enterprise Mobility System, the Mobility SIP Server in the “home” enterprise and the Mobility SIP Server in the far-end enterprise shall use SIP over TLS for transmitting call setup and call termination messages used by the UEs.	T=O
FSVS.04	For communication between User Equipment and a fixed enterprise VoIP device, the Mobility SIP Server and Secure Voice Gateway shall use public key cryptography to mutually authenticate.	T=O
FSVS.05	For communication between User Equipment and a fixed enterprise VoIP device, the Mobility SIP Server and Secure Voice Gateway shall use Suite B cryptosuite for the TLS traffic.	T=O
FSVS.06	For communication between User Equipment and a fixed enterprise VoIP device, the Mobility SIP Server and Secure Voice Gateway shall use SIP over TLS for transmitting call setup and call termination messages used by the User Equipment.	T=O
FSVS.07-10	Withdrawn	N/A
FSVS.11	The Mobility SIP Server and Secure Voice Gateway shall use public key cryptography to mutually authenticate.	O
FSVS.12	The Mobility SIP Server and Secure Voice Gateway shall negotiate AES keys to protect the confidentiality and integrity of TLS traffic.	O
FSVS.13	The Mobility SIP Server and Secure Voice Gateway shall use SIP over TLS for transmitting call setup and call termination messages used by the User Equipment.	O

Requirement Number	Requirement Description	Threshold/ Objective
FSVS.14	The Secure Voice Gateway shall use SIP for transmitting call setup and call termination messages to the Enterprise SIP Server.	O
FSVS.15	The SIP Server shall support the ability to securely contain a unique public key certificate and corresponding private key, used to provide authentication of the SIP Server to the user equipment, in order to establish the TLS channel for SIP messages.	T=O

C.4 Web Based Non-Resident Data Requirements

Table 27: Web Based Non-Resident Data Requirements

Requirement Number	Requirement Description	Threshold/ Objective
FWND.00	**Overarching Web Based Non-Resident Data Requirements**	
FWND.01	The web server and client shall support TLS 1.2 at a minimum	T=O
FWND.02	The web server and client shall support Suite B.	T=O
FWND.03	The web server and client shall be configurable to disable SSL protocols	T=O
FWND.04	The web server shall provide user access to Enterprise network data and application services	T=O
FWND.05	The web browser shall be configurable to not store any data in non-volatile memory on the User Equipment.	T=O
FWND.06	The solution shall provide means for the user to authenticate to Enterprise services	T=O
FWND.07	The solution shall trust authentication between the web server and client for a limited period of time (at most 24 hours) before requiring re-authentication	T=O
FWND.08	The web server shall accept either device certificates, user credentials, user certificates, or a combination for authentication	T=O
FWND.09	The web server and client shall be configurable to disable versions of TLS less than 1.2.	T=O

C.5 User Equipment Requirements

Table 28: User Equipment Requirements

Requirement Number	Requirement Description	Threshold/ Objective
FUES.00	**Smartphone User Equipment Requirements**	
FUES.01	The system shall not have any feature that will be capable of "Phoning home" or reporting back to a centralized vendor-managed server unless it can be disabled.	T=O
FUES.02	The administrative user shall have the ability to remove and uninstall any applications, processes, services, and files that are not essential for operation of the handset.	T=O
FUES.03	During provisioning and updates of the User Equipment the administrative user shall have the ability to terminate an identified list of processes each time the handset is provisioned or is booted	T=O

Requirement Number	Requirement Description	Threshold/ Objective
FUES.04	The User Equipment shall have the ability to notify the administrator during the provisioning process of the number of successful and unsuccessful application removals.	T=O
FUES.05	The User Equipment shall have the ability to notify the administrator during the provisioning process of the number of successful and unsuccessful file removals.	T=O
FUES.06	The User Equipment shall have the ability to notify the administrator during the provisioning process of the number of successful and unsuccessful process terminations.	T=O
FUES.07	During provisioning and updates of the User Equipment the administrative user shall have the ability to remove the functionality that would allow an ordinary user of the User Equipment to attain administrative user privileges.	T=O
FUES.08	During provisioning and updates of the User Equipment the administrative user shall have the ability to clear the contents of the cache in order to provide a clean-slate cache to begin operation of the User Equipment.	T=O
FUES.09	*Withdrawn*	
FUES.10	*Withdrawn*	
FUES.11	*Withdrawn*	
FUES.12	*Withdrawn*	
FUES.13	*Withdrawn*	
FUES.14	*Withdrawn*	
FUES.15	*Withdrawn*	
FUES.16	*Withdrawn*	
FUES.17	*Withdrawn*	
FUES.18	*Withdrawn*	
FUES.19	*Withdrawn*	
FUES.20	*Withdrawn*	
FUES.21	*Withdrawn*	
FUES.22	*Withdrawn*	
FUES.23	*Withdrawn*	
FUES.24	*Withdrawn*	
FUES.25	*Withdrawn*	
FUES.26	*Withdrawn*	
FUES.27	*Withdrawn*	
FUES.28	*Withdrawn*	
FUES.29	*Withdrawn*	
FUES.30	*Withdrawn*	
FUES.31	*Withdrawn*	
FUES.32	*Withdrawn*	
FUES.33	*Withdrawn*	
FUES.34	The User Equipment shall provide the capability to disable tethering capabilities.	T=O

Requirement Number	Requirement Description	Threshold/ Objective
FUES.35	The User Equipment shall provide the capability to prevent users from enabling tethering capabilities.	T=O
FUES.36	The User Equipment shall provide a mechanism to determine if the user has enabled tethering capabilities.	T=O
FUES.37	*Withdrawn*	
FUES.38	The User Equipment shall allow for Over the Air (OTA) updates from the carrier to be disabled.	T=O
FUES.39	*Withdrawn*	
FUES.40	The User Equipment shall provide a secure credential storage system that is usable by applications.	T=O
FUES.41	The User Equipment Certificate storage shall be protected using an auxiliary password.	T=O
FUES.42	The Certificate storage password shall have the capability to be configured for length and complexity.	T=O
FUES.43	*Withdrawn*	
FUES.44	The User Equipment shall provide a notification mechanism if the Bluetooth has been enabled by the user.	O
FUES.45	The User Equipment shall provide a notification mechanism if the Wi-Fi has been enabled by the user.	O
FUES.46	The User Equipment shall provide a mechanism to determine if the user has enabled Auto Answer.	O
FUES.47	The User Equipment shall provide a notification mechanism if the Auto Answer has been enabled by the user.	O
FUES.48	The User Equipment shall provide a mechanism to determine if the user has enabled GPS or Location Services.	O
FUES.49	The User Equipment shall provide Full Disk Encryption (FDE) or an equivalent capability.	O
FUES.50	The User Equipment operating system shall adhere to [final] PP for MD F FDP_IFC_EXT.1.1 (IFC-1)	T
FUES.51	*Withdrawn*	
FUES.52	The User Equipment shall provide the capability to disable all radios following [draft] MDPP FMT_SMF 1.1 Admin Assignment: list of radios {WiFi, GPS, Cellular, NFC, Bluetooth}	T
FUES.53	The User Equipment shall provide the capability to disable all externally accessible hardware ports following [draft] MDPP FMT_SMF 1.1 Admin Assignment: list of externally accessible hardware ports {USB, SD card, HDMI, Headphone jack}	T
FUES.53	The User Equipment shall provide the capability to disable all audio and visual collection devices following [draft] MDPP FMT_SMF 1.1 Admin Assignment: list of audio or visual collection devices {camera, microphone}	T
FUES.54	The User Equipment shall provide a notification mechanism upon state change of [draft] MDPP FMT_SMF 1.1 Admin Assignment: list of radios {WiFi, GPS, Cellular, NFC, Bluetooth}	T

Requirement Number	Requirement Description	Threshold/ Objective
FUES.55	The User Equipment shall provide a notification mechanism upon state change of [draft] MDPP FMT_SMF 1.1 Admin Assignment: list of externally accessible hardware ports {USB, SD card, HDMI, Headphone jack}	T
FUES.56	The User Equipment shall provide a notification mechanism upon state change of [draft] MDPP FMT_SMF 1.1 Admin Assignment: list of audio or visual collection devices {camera, microphone}	T
FUES.57	The User Equipment shall adhere to [draft] MDPP Requirement MGMT_16 Assignment: {all}	T
FUEA.00	**User Equipment Monitoring Service Requirements**	
FUEA.01	The User Equipment Monitoring Service shall have the ability to categorize unauthorized events into two classes: Major Faults and Minor Faults.	T=O
FUEA.02	The User Equipment Monitoring Service shall have the ability to terminate any encryption utility upon detection of a Major Fault.	T=O
FUEA.03	The User Equipment Monitoring Service shall have the ability to monitor User Equipment activities such as the OS, Input/output (i/o) port activities, files, applications, and processes.	T=O
FUEA.04	The User Equipment Monitoring Service shall have the ability to log unauthorized events in the User Equipment's system log.	T=O
FUEA.05	The User Equipment Monitoring Service shall have the ability to notify the user of an unauthorized event.	T=O
FUEA.06	The User Equipment Monitoring Service shall have the ability to cease operation of the User Equipment and require the user to determine course of action (reboot, shut down, or continue to operate in an un-trusted condition).	T=O
FUEA.07	The User Equipment Monitoring Service shall have the ability to retrieve and modify privileged mode information on the device.	T=O
FUEA.08	The User Equipment Monitoring Service shall have the ability to retrieve and modify privileged mode designated OS level and file directory monitoring information.	T=O
FUEA.09	The User Equipment Monitoring Service shall have the ability to remove all functionalities, files, and applications that are not required for the intended operation of the User Equipment.	T=O
FUEA.10	The User Equipment Monitoring Service shall be able to detect and record fault details to the system log in response to a Minor Fault.	T=O
FUEA.11	The User Equipment Monitoring Service shall be able to detect and record fault details to the system log in response to a Major Fault.	T=O
FUEA.12	The User Equipment Monitoring Service shall have the ability to generate a detailed notification to the user upon detection of a Major Fault.	T=O
FUEA.13	The User Equipment Monitoring Service shall have the ability to vibrate to alert the user upon detection of a Major Fault.	T=O

Requirement Number	Requirement Description	Threshold/ Objective
FUEA.14	The User Equipment Monitoring Service shall have the ability to remove all files containing encrypted or decrypted certificates and key material, without user intervention, upon detection of a Major Fault.	T=O
FUEA.15	The User Equipment Monitoring Service shall have the ability to terminate any VPN client process and connection upon detection of a Major Fault.	T=O
FUEA.16	The User Equipment Monitoring Service shall have the ability to allow standard phone calls upon detection of a Major Fault.	T=O
FUEA.17	The User Equipment Monitoring Service shall have the ability to allow 911 calls.	T=O
FUEA.18	The User Equipment Monitoring Service shall have the ability to enable standard phone calls in response to a Major Fault	T=O
FUEA.19	The User Equipment Monitoring Service shall have the ability to detect the removal and insertion of any removable media.	T=O
FUEA.20	When connected to the Mobility Enterprise, the User Equipment Monitoring Service shall have the ability to block any outgoing phone calls other than to 911 or equivalent services Outside of the Continental United States (OCONUS).	T=O
FUEA.21	The User Equipment Monitoring Service shall have the ability to log incoming or outgoing phone calls if they are blocked.	T=O
FUEA.22	The User Equipment Monitoring Service shall have the ability to monitor the OS file system to monitor different types of specified events that could take place in a directory or to a specific file.	T=O
FUEA.23	The User Equipment Monitoring Service shall have the ability to receive detected events written to the system log, and based on a priority level, initiate corresponding notifications to the user.	T=O
FUEA.24	The User Equipment Monitoring Service shall have the ability to disable the Wi-Fi state if it is enabled.	T=O
FUEA.25	The User Equipment Monitoring Service shall have the ability to detect when non-approved programs are running.	T=O
FUEA.26	The User Equipment Monitoring Service shall have the ability to prevent unauthorized applications and services from accessing the camera and the camera services.	T=O
FUEA.27	The User Equipment Monitoring Service shall have the ability to detect the mounting of a USB connection as mass storage.	T=O
FUEA.28	The User Equipment Monitoring Service shall have the ability to block standard phone calls.	T=O
FUEA.29	The User Equipment Monitoring Service shall have the ability to notify the user upon detection of a Major or Minor Fault.	T=O

C.6 Enterprise Mobility Infrastructure Requirements

Table 29: Infrastructure Requirements

Requirement Number	Requirement Description	Threshold/ Objective
FIFS.00	**Enterprise Mobility Infrastructure Security Services Requirements**	
FIFS.01	The Enterprise Mobility Infrastructure Security Services shall allow configuration of an audit policy that encompasses deletion and/or overwriting of audit records.	T=O
FIFS.02	The Enterprise Mobility Infrastructure Security Services shall provide the ability to backup audit records to tape or other long-term storage media.	T=O
FIFA.00	**Enterprise Mobility Infrastructure Architecture Requirements**	
FIFA.01	The Certificate Validation Service shall have the capability to support the Online Certificate Status Protocol (OCSP).	O

C.7 PKI Requirements

Table 30: PKI Requirements

Requirement Number	Requirement Description	Threshold/ Objective
FECA.00	**Certificate, Key, and Trust Management**	
FECA.01	*Withdrawn into PROSE 5.2.3, version 2.2*	T=O
FECA.02	*Withdrawn into PROSE 5.2.3, version 2.2*	T=O
FECA.03	*Withdrawn into PROSE 5.2.3, version 2.2*	T=O
FECA.04	*Withdrawn into PROSE 5.2.3, version 2.2*	T=O

C.8 Provisioning Requirements

To implement a platform directly corresponding to the Mobility Prototype Architecture, any using agency must closely observe the following provisioning requirements. However, these requirements constrain the solution space to that of the Mobility Prototype Architecture. The two meta-requirements that must be met by all implementations of this Mobility Security Guide are:

1. There must be a DAA/AO approved procedure for provisioning the User Equipment
2. This procedure must ensure the User Equipment has a known trusted state prior to provisioning

Given the using agency observes these two design principles for implementations not directly corresponding to the Mobility Prototype Architecture, the implementer will provision User Equipment in a known secure state, subsequently remaining in a fully understood state after provisioning.

Table 31: Provisioning Requirements

Requirement Number	Requirement Description	Threshold/ Objective
FEWS.00	**Enrollment Work Station Requirements**	
FEWS.01	The Enrollment Workstation shall be able to load a certificate on to removable media.	T=O
FEWS.02	The Enrollment Workstation shall be able to interface to a removable security module.	O

Requirement Number	Requirement Description	Threshold/ Objective
FEWS.03	The Enrollment Workstation shall be able to accept entry of requests for device certificates.	T=O
FUEP.00	**User Equipment Provisioning Requirements**	
FUEP.01	The Device Provisioning Workstation shall maintain a registration data store including each device it provisions.	O
FUEP.02	The Device Provisioning Workstation shall be able to define, manage, set, and monitor policies to allow or preclude the use of Bluetooth.	T=O
FUEP.03	The Device Provisioning Workstation shall be able to define, manage, set, and monitor policies to allow or preclude the use of Wi-Fi.	T=O
FUEP.04	The Device Provisioning Workstation shall be able to define, manage, set, and monitor policies to allow or preclude the use of the camera.	T=O
FUEP.05	The Device Provisioning Workstation shall be able to define, manage, set, and monitor policies to allow or preclude the use of Near Field Communications (NFC).	T=O
FUEP.06	The Device Provisioning Workstation shall be able to define, manage, set, and monitor policies to allow or preclude the use of USB for mass storage.	T=O
FUEP.07	The Device Provisioning Workstation shall be able to accept signed applications provided on removable media.	T=O
FUEP.08	The Device Provisioning Workstation shall be able to verify the integrity of signed applications provided on removable media.	O
FUEP.09	The Device Provisioning Workstation shall maintain a data store of accepted signed applications.	T=O
FUEP.10	The Device Provisioning Workstation shall be able to digitally sign material to be placed on a removable media.	O
FUEP.11	The Device Provisioning Workstation shall allow a user to define device policy settings.	T=O
FUEP.12	The Device Provisioning Workstation shall maintain white lists, black lists, and mandatory lists of applications applicable to each device type.	T=O
FUEP.13	The Device Provisioning Workstation shall be able to interface to a non-secure removable media card.	O
FUEP.14	The Device Provisioning Workstation shall be able to interface to a removable security module.	O
FUEP.15	The Device Provisioning Workstation shall be able to interface to the device via its USB port.	T=O
FUEP.16	The Device Provisioning Workstation shall accept inputs from removable media and devices as input to the registration data store.	O
FUEP.17	The Device Provisioning Workstation shall accept requests for device registration information.	T=O
FUEP.18	The Device Provisioning Workstation shall have the ability to load approved software and scripts, including monitoring and trusted provisioning applications, onto the device.	T=O
FUEP.19	The Device Provisioning Workstation shall have the ability to load device configuration and policy information onto the device.	T=O

Appendix D Terminology

This appendix contains background information such as terms, definitions, and acronyms. It is included to provide facts related to the composition of the Mobility Security Guide, associated Protection Profiles, and NIST SP 800-164 for those who may be unfamiliar with specific terminology used by USG and the authors of the Mobility Security Guide.

D.1 Acronyms

Table 32: Acronyms

Acronym	Description
3G	Third Generation wireless telephone technology
4G	Fourth Generation standard for mobile telecommunications
AAA	Authentication, Authorization, and Accounting
AES	Advanced Encryption Standard
AH	Authentication Header
API	Application Programming Interfaces
APN	Access Point Name
APT	Advanced Persistent Threat
CA	Certificate Authority
CBC	Cyber Block Chaining
CCM	Counter Mode
C&A	Certification & Accreditation
CDMA	Code Division Multiple Access, a 3G mobile communications standard
CP	Capability Package
CPS	Certification Practice Statement
CRL	Certificate Revocation Lists
CSfC	Commercial Solutions for Classified
CSP	Critical Security Parameter (see Critical Security Parameter)
CSR	Certificate Signing Request
CTR	Counter
DAO	Designated Authorizing Official
DAR	Data At Rest
DEK	Data Encryption Key (see Data Encryption Key)
DES	Data Encryption System
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DN	Distinguished Name
DNS	Domain Name Service

Acronym	Description
DNSSEC	Domain Name System Security Extension
DO	Device Owner (see Device Owner)
DoD	Department of Defense
DoDEDIPI	Department of Defense Electronic Data Interchange Personnel Identifier
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
E911	Enhanced 9-1-1
EBC	Edge Border Control
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ESF	Enduring Security Framework
ESP	Encapsulating Security Payload
ESP	Encapsulating Security Protocol
FEK	File Encryption Key
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HA	Header Authentication
HMAC	Hash-Based Message Authentication Code
HTTP	Hyper Text Transfer Protocol
HSPA	High Speed Packet Access
IAD	Information Assurance Directorate
ID	Identification
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMEI	International Mobile Equipment Identity
i/o	Input/output
IO	Information Owner (see information owner)
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
KEK	Key Encryption Key (see Key Encryption Key)
KTS-OAEP	Key Transport System – Optimal Asymmetrical Encryption Padding
LTE	Long Term Evolution
MDE	Mobile Device Endpoint
MDI	Mobile Device Interface
MDM	Mobile Device Management

Acronym	Description
MSG	Mobility Security Guide
NAT	Network Address Translation
NFC	Near Field Communication
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSA/IAD	National Security Agency/Information Assurance Directorate
NSS	National Security System
NTP	Network Time Protocol
OCSP	Online Certification Status Protocol
OEM	Original Equipment Manufacturer
OS	Operating System
OTA	Over The Air
PAT	Port Address Translation
PBKDFV2	Password Based Key Derivation Function Version 2
PDM	Policy Delivery Mechanism (see Policy Delivery Mechanism)
PEM	Policy Enforcement Mechanism (see Policy Enforcement Mechanism)
PEnE	Policy Enforcement Engine (see Policy Enforcement Engine)
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PMM	Policy Management Mechanism (see Policy Management Mechanism)
PP	Protection Profile
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
RAN(s)	Radio Access Network(s)
RBG	Random Bit Generator
rDSA	RSA Digital Signature Algorithm
RFC	Request for Comment
RoT	Root of Trust (see Root of Trust)
RTI	Root of Trust for Integrity (see Root of Trust for Integrity)
RTM	Root of Trust for Measurement (see Root of Trust for Measurement)
RTP	Real-time Protocol
RTR	Root of Trust for Reporting (see Root of Trust for Reporting)
RTS	Root of Trust for Storage (see Root of Trust for Storage)
RTU	Root of Trust for Update (see Root of Trust for Update)
RTV	Root of Trust for Verification (see Root of Trust for Verification)
S/MIME	Secure/Multipurpose Internet Mail Extensions

Acronym	Description
SBC	Session Border Controller
SCRM	Supply Chain Risk Management
SDES	Security Descriptions
SDP	Session Description Protocol
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMS	Short Message Service
SP	Service Pack
SRTCP	Secure Real Time Control Protocol
SRTP	Secure Real Time Protocol
SSL	Secure Sockets Layer
SVoIP	Secure Voice Over Internet Protocol
TLS	Transport Layer Security
UE	User Equipment
UMTS	Universal Mobile Telephone Service
USB	Universal Serial Bus
USG	United States Government
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity

D.2 DEFINITIONS

Table 33: Definitions

Term	Definition
Application	A software program hosted by an information system; can refer to a software program hosted on a mobile device. (Source: NIST SP 800-137)
Critical Security Parameter	Security related information (e.g. secret and private cryptographic keys, and authentication data such as passwords and Personal Identification Numbers [PIN]s) whose disclosure or modification can compromise the security of a cryptographic module.
Data Encryption Key	Key that encrypts data; usually refers to symmetric encryption keys such as those used for AES or DES symmetric encryption algorithms.
Device	Hardware, firmware, and software, including applications that constitute a mobile communication device with wireless access to both communications networks and the Internet.
Device Owner	Entity that purchases and maintains ownership of a mobile device; can refer to an employee of a company that uses a personally-owned device to access company information.
Fixed Devices	Non-mobile devices that include servers, network appliances, and other infrastructure components that are not mobile as well as any other fixed voice and data equipment (such as wired desktops)
Identity	A characteristic or group of characteristics by which an entity is recognizable; can refer to an asymmetric key associated with a person, device, or application.
Information Owner	Entity whose information is stored and/or processed on a device; can be an application-specific provider, a digital provider, or an enterprise that allows access to resources from mobile devices.
Key Encryption Key	Key that encrypts other keys; usually refers to asymmetric keys such as RSA or Elliptic Curve Cryptography keys, but could also be symmetric encryption keys, which is rare.
Minimum policy requirements	The set of requirements which constitutes the least onerous policy for an entity.
Platform	(See Device).
Policy Delivery Mechanism	A component of the Policy Enforcement Engine that allows the device to receive policies.
Policy Enforcement Engine	A component of a device that allows it to receive, manage, and enforce policies.
Policy Enforcement Mechanism	A component of the PEnE that allows a device to enforce policies.
Root of Trust	An unconditionally trusted component of a device consisting of a computing engine and software that performs fundamental security service such as measurement, storage, integrity, verification, reporting, or updating.
Root of Trust for Integrity	A root of trust that provides services to protect the integrity of measurements and assertions.
Root of Trust for Measurement	A root of trust that provides measurement services; usually refers to a component capable of hashing data including executables and configuration data.
Root of Trust for Reporting	A root of trust that provides a service which signs information using unambiguous identities and providing integrity, non-repudiation, anti-replay, and freshness properties.
Root of Trust for Storage	A root of trust that provides a storage service for critical security parameters (CSPs).
Root of Trust for Update	A root of trust that provides a trusted update capability; usually applied to other roots of trust.
Root of Trust for Verification	A root of trust that provides a trusted verification capability.
Roots of Trust	Two or more roots of trust from the set of fundamental roots of trust, namely RTM, RTS, RTI, RTV, RTR, and RTU.
Supply Chain Risk Management (SCRM)	A program to establish processes and procedures to minimize acquisition-related risks to critical acquisitions including, hardware components and software solutions from supply chain threats due to reliance on global sources of supply.

D.3 Specialized Requirements Terms and Definitions

These terms apply to each of the requirements appendices (Appendix A and C) and reflect language that is specific to the construction of the requirements. Because the requirements were written over large periods of time by different teams, this Mobility Security Guide provides the table below to clarify the intent of each of the original authoring teams. It is anticipated that by providing this table we can reduce any confusion related to the use of requirements specific terms.

Important Note: These specialized terms and definitions do not exclusively map to terminology adopted by standards bodies (in RFCs, for example). The reviewer should carefully apply the definitions outlined in this table to the requirements of this Mobility Security Guide.

Table 34: Specialized Requirements Terms and Definitions

Term	Description
MAY	This word is used to call out architecturally-specific methods for implementing “MUST” and/or “SHOULD” statements
MUST	As well as “REQUIRED” or “SHALL”, MUST means that the definition is a baseline requirement of the specification having the additional intent that the functionality be feasible to implement on a commercial scale within the near term (0 to 6 months)
MUST NOT	This phrase means the definition is a prohibition of the specification
Objective	An objective (O) requirement specifies a feature or function that the Government desires and expects.
REQUIRED	As well as "SHALL" or “MUST”, required means that the definition is a requirement of the specification
SHALL	This word is a requirement of the specification
SHALL NOT	This phrase means that the definition is a prohibition of the specification
SHOULD	Implies a reasonable baseline requirement given the growth in mobile threat vectors but may only be commercially feasible to implement in the next 6 to 12 months
T=O	The threshold requirement also serves as the objective requirement
Threshold	A threshold (T) requirement specifies a minimum acceptable feature or function that, in the Government’s judgment, still provides the needed capabilities if the corresponding objective requirement cannot reasonably be met (e.g., due to lack of technology maturity, cost or time constraints)