



Mobility Capability Package

15 December

2012

The Mobility Capability Package describes the Enterprise Mobility Architecture, a layered security approach for using commercial devices and networks to securely connect mobile users to the Government enterprise. This release focuses on using smartphones and commercial cellular networks to provide a secure voice capability and web-arbitrated services with non-resident data.

Enterprise
Mobility
Version 2.1

Table of Contents

1	Enterprise Mobility	1
1.1	Goals	1
1.2	Enterprise Mobility Overview	2
1.3	Design Summary	4
2	Mobile Applications and Services	5
2.1	Secure Voice over Internet Protocol (SVoIP) Capability	5
2.2	Web-Based Non-Resident Data Capability	7
3	User Equipment	8
3.1	Smartphone	8
4	Access Networks	12
4.1	Cellular Services	12
5	Enterprise Mobility Infrastructure	15
5.1	Objective Enterprise Mobility Infrastructure Architecture	15
5.2	Prototype Enterprise Mobility Infrastructure Architecture	16
6	Mobility Threats, Risks, and Mitigations	20
6.1	Risks	20
6.2	Threats	20
6.3	Risk Mitigations	21
	Acronyms and Terms	23
	Consolidated References	25
Appendix A	Architecture and Configuration - Enterprise Mobility Requirements	A-1
A.1	Overarching Solution Requirements	A-2
A.2	VPN Requirements	A-3
A.3	Secure Voice over Internet Protocol (SVoIP) Requirements	A-5
A.4	Web Based Non-Resident Data Requirements	A-7
A.5	Carrier Service Integration	A-9
A.6	User Equipment Requirements	A-9
A.7	Enterprise Mobility Infrastructure Requirements	A-12
A.8	PKI Requirements	A-17
A.9	Provisioning Requirements	A-18

Appendix B	Test Criteria - Enterprise Mobility	B-1
B.1	Test Criteria for the Overarching Mobility Requirements.....	B-1
B.2	Test Criteria for Overarching VPN Requirements.....	B-5
B.3	Test Criteria for Overarching SVoIP Requirements	B-9
B.4	Test Criteria for Web Based Non-Resident Data Requirements	B-14
B.5	Test Criteria for Carrier Service Integration	B-17
B.6	Test Criteria for User Equipment Requirements.....	B-17
B.7	Test Criteria for Infrastructure Requirements.....	B-25
B.8	Test Criteria for PKI Requirements.....	B-35
B.9	Test Criteria for User Equipment Provisioning Requirements	B-38
Appendix C	Functional Requirements - Enterprise Mobility	C-1
C.1	Overarching Mobility Requirements	C-2
C.2	VPN Requirements	C-2
C.3	Secure Voice over Internet Protocol (SVoIP) Requirements	C-3
C.4	Web Based Non-Resident Data Requirements	C-5
C.5	User Equipment Requirements	C-6
C.6	Enterprise Mobility Infrastructure Requirements.....	C-10
C.7	PKI Requirements	C-10
C.8	Provisioning Requirements	C-11

Figures

Figure 1-1.	Enterprise Mobility	1
Figure 1-2.	Basic Segments of the Enterprise Mobility Architecture.....	2
Figure 2-1.	Two Tunnels of the Enterprise Mobility Solution	5
Figure 5-1.	Objective Enterprise Mobility Infrastructure Architecture.....	15
Figure 5-2.	Prototype Enterprise Mobility Infrastructure Architecture.....	16

Tables

Table A-1.	Requirement Designators	A-1
Table A-2.	Overarching Mobility Requirements	A-2
Table A-3.	VPN Requirements.....	A-3
Table A-4.	SVoIP Requirements	A-5
Table A-5.	Web Based Non-Resident Data Requirements.....	A-7
Table A-6.	Carrier Service Integration Requirements	A-9

Table A-7. User Equipment Requirements.....	A-9
Table A-8. Infrastructure Requirements	A-12
Table A-9. PKI Requirements.....	A-17
Table A-10. Provisioning Requirements.....	A-18
Table B-1. Requirements Designators.....	B-1
Table B-2. Overarching Mobility Test Criteria.....	B-2
Table B-2. VPN Test Criteria	B-5
Table B-3. SVoIP Test Criteria.....	B-9
Table B-4. Web Based Non-Resident Data Test Criteria	B-14
Table B-5. Carrier Service Integration Test Criteria	B-17
Table B-6. User Equipment Test Criteria.....	B-17
Table B-7. Infrastructure Test Criteria	B-25
Table B-8. PKI Test Criteria.....	B-35
Table B-9. Provisioning Test Criteria	B-38
Table C-1. Requirement Designators	C-1
Table C-2. Overarching Mobility Requirements.....	C-2
Table C-3. VPN Requirements	C-2
Table C-4. SVoIP Requirements.....	C-3
Table C-5. Web Based Non-Resident Data Requirements	C-5
Table C-6. User Equipment Requirements.....	C-6
Table C-7. Infrastructure Requirements	C-10
Table C-8. PKI Requirements.....	C-10
Table C-9. Provisioning Requirements	C-11

Mobility Capability Package

The Mobility Capability Package is a product of the National Security Agency's Information Assurance Directorate (NSA/IAD) Mobility Program and the NSA/IAD Commercial Solutions for Classified (CSfC) Program. NSA/IAD is developing new ways to leverage emerging technologies to deliver more timely Information Assurance solutions for rapidly evolving United States Government (USG) customer requirements. To satisfy this new business objective, the CSfC process was established to enable commercial products used in layered solutions to protect classified National Security Systems (NSS) and the data they carry. This satisfies USG customers' urgent requirements to communicate securely with interoperable products based on commercial standards in a solution that can be fielded in months, not years.

This document is the third of a series of releases of the Mobility Capability Package (Mobility CP). The intent of the early release of these documents is to establish a partnership between USG system integrators and NSA/IAD experts to build Secure Mobility capabilities and to establish a dialogue with industry to develop the commercially available products for those capabilities. At this time, guidance in this document may not be applied without consulting NSA/IAD for support prior to presenting a solution to the implementing organization's Delegated Authorizing Official (DAO). USG entities interested in presenting solutions to their DAOs in accordance with this guidance must first submit a request for CP application support to NSA/IAD. In the future, however, customers and their solution providers will be able to use this guidance to implement solutions without such NSA/IAD involvement.

USG entities using this Capability Package to establish their own mobility capabilities need to ensure that in doing so they 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, such as NIST SP 800-53. If there is a conflict between the Mobility Capability Package Requirements and the C&A requirements, the guidance in the Capability Package takes precedence. An analysis has not been performed to identify the conflicts. This is because the National Manager as specified in CNSSD 502 has deemed that where National Security Systems (NSS) and the protection of classified information carried on them are concerned, the particular component layering and implementation guidance in this document is required to adequately secure the composite commercial solution. While this document is intended to allow USG entities as much flexibility as possible in implementing a mobility capability, vendor diversity for the encryption and security critical functions is essential to the security of the overall solution. Consequently, if an agency is deciding between a solution that meets more objective requirements and is composed of products from a single vendor and a solution that meets fewer objective requirements that includes products from multiple vendors, the agency must select the multi-vendor solution, as dictated by this guidance.

The National Manager is authorized to 1) approve, and has approved, this CP as an information assurance technique for securing NSS and the information they carry in the mobile environment and, 2) prescribe this CP 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 Capability Package. In accordance with Section 9.b of CNSSD 502, users of this CP are responsible for obtaining, under their established agency accreditation and approval processes, certification and accreditation of any mobility solution processing classified information that has been developed in accordance with this CP. Failure to properly and

adequately follow the guidance in this Capability Package may reduce the security of the solution and, in the case of NSS, provide insufficient protection for NSS processing classified information, which would constitute a violation of CNSSD 502. If users applying this CP 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. A request for a waiver must include a detailed justification for the deviation from the CP guidance.

DISCLAIMER

This Capability Package 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 United States Government 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 Capabilities Package, even if advised of the possibility of such damage.

The User of this Capability Package agrees to hold harmless and indemnify the United States Government, 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 Capability Package is intended to constitute an endorsement, explicit or implied, by the U.S. Government 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 Program (NIAP), please visit the following web sites: http://www.nsa.gov/ia/business_research/ia_bao/commercial_solutions_for_classified_program.shtml
<http://www.niap-ccevs.org/pp>
<http://www.iad.gov>

Capability Package Change Log

Version	Date	Change Description
1.1	02/29/12	Initial revision for public distribution.
1.2	03/26/12	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 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	11/15/2012	<ul style="list-style-type: none"> • Clarifications, corrections, and edit due to received comments on CP 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 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”.

1 Enterprise Mobility

1.1 Goals

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 Capability Package 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 Mobility Capability Package is incrementally evolving towards a complete enterprise solution:

- **Evolving Capabilities:** Version 1.1 of the Mobility Capability Package 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 Mobile Device Management services.
- **Evolving Guidance:** Initial versions of the Mobility Capability Package 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 later versions, 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 when connecting to existing Government enterprise services. 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.

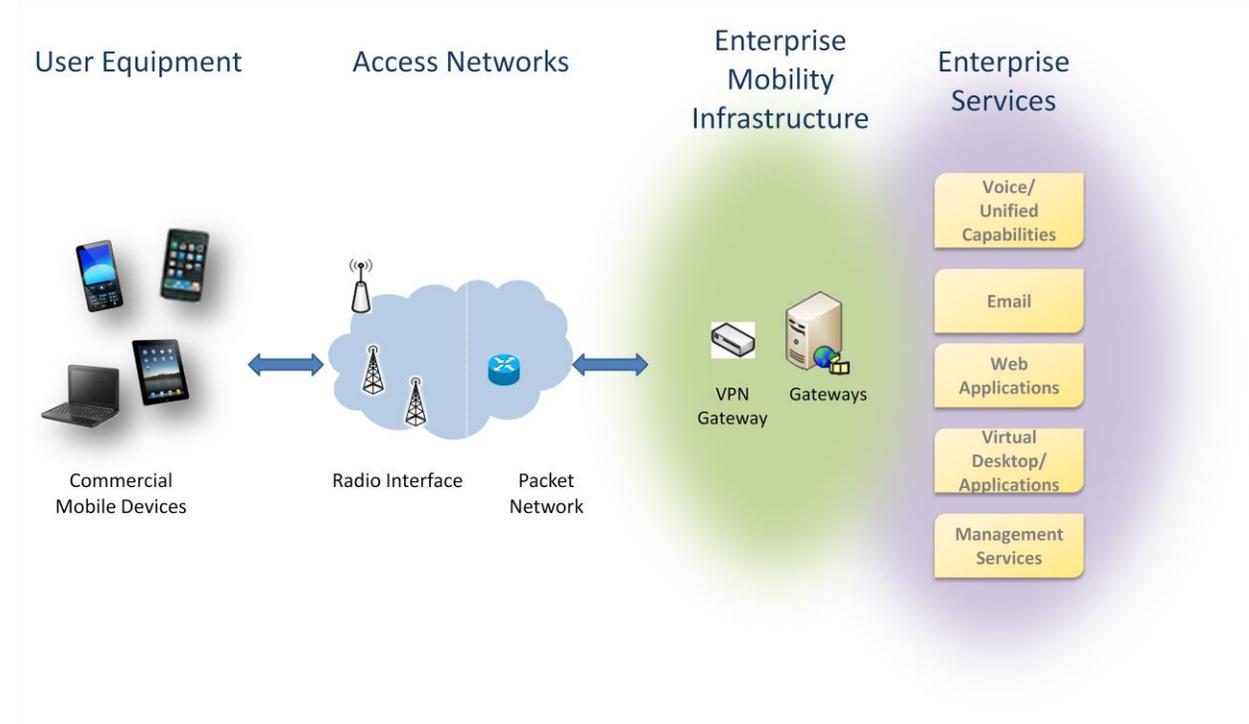


Figure 1-2. Basic Segments of the Enterprise Mobility Architecture

Enterprise Services are the existing and evolving services provided for all enterprise users, including mobile users. Government enterprise services include communication applications such as data (email, chat, presence) and voice (telephone/teleconferencing). 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.
- Section 2 contains more information on specific mobile applications and services.

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.

- 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 need to be hardened to protect integrity and reduce risks.
- Section 3 contains additional information on User Equipment.

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 also 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 the 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 mobile devices to Government facilities.
- The only commercial network service that is allowed for use by the mobile device user is the data connection 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, carrier-provided voice, SMS, and other value-added services will not be available to the user via the mobile client. 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. It includes call control to establish data connections with authorized User Equipment. Applications may 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 mobile devices 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 updates to ensure proper

configuration. Enterprise security management services need to ensure that there is 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, possible 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 the mobile device to the Government enterprise.
- Ensure that all service requests and user traffic from a mobile device 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.
- 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.
- 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 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 access network and applications being used and is specified elsewhere in this Mobility Capability Package.
- 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 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 NIST publications listed in the Consolidated Reference section, page 25.

2 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.

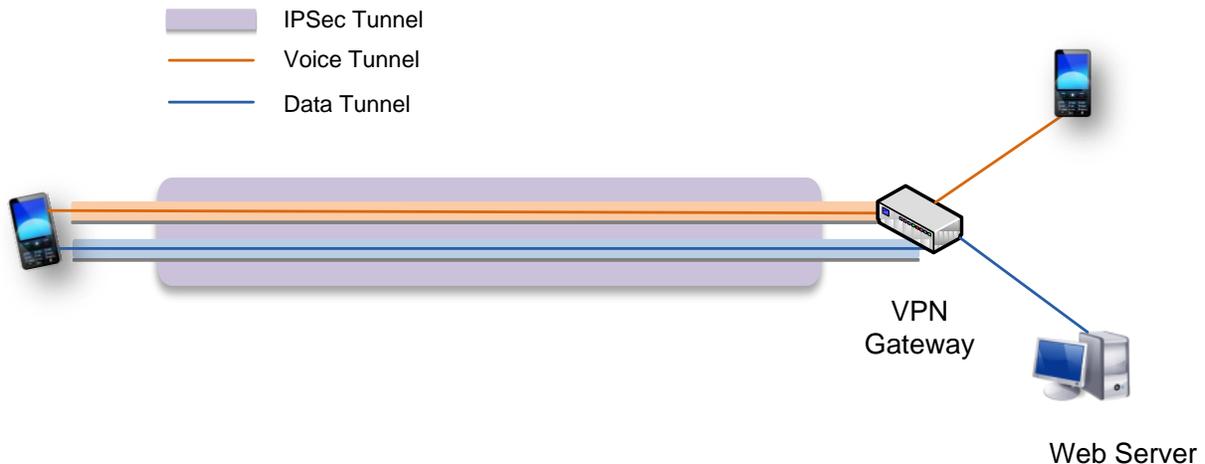


Figure 2-1. Two Tunnels of the Enterprise Mobility Solution

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

- All data between User Equipment and the Enterprise Mobility Infrastructure is protected in an IPsec Virtual Private Network (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 Internet Key Exchange (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.

2.1 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 Secure Voice over IP (SVoIP) Capability found in Appendix A.3 and functional requirements in Appendix C.3 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 Secure Voice over IP (SVoIP) Capability requirements are found in Appendix B.3.

2.1.1 Security-Relevant Components

User Equipment uses an SVoIP client application that is configured to use the existing VPN tunnel for the outer layer of encryption. An inner Transport Layer Security (TLS) tunnel to a Session Initiation Protocol (SIP) Server residing in the Enterprise Mobility Infrastructure protects call control traffic, and an inner Secure Real-time Transport Protocol (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:** Session Initiation Protocol (SIP) is used for registration of User Equipment, call setup, and call termination. TLS with Suite B compliant cryptosuites 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 user ID and password supplied in the TLS-protected session.
- **SVoIP Media Streams:** SRTP is used to protect media streams between User Equipment. 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. All SIP traffic with User Equipment is protected using TLS with Suite B compliant cryptosuites. 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 user ID and password supplied in the TLS-protected session. The SIP Server may consult a 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. Secure voice gateways to non-IP systems and interoperability between secure systems will be more fully discussed in future versions of this Capability Package.

2.1.2 Gap Analysis

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.

2.2 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.4 and functional requirements in Appendix C.4 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 Web-Based Non-Resident Data Capability are found in Appendix B.4.

2.2.1 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 cryptosuites. 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 user ID 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 whitelisting). Finally, the client (Web Browser) and the server (Web Servers) 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 a 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.

3 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 Capability Package describes the smartphone cellular capability only; future releases of this and other Capability Packages will include other mobile device capabilities, such as laptops and tablets, over other transport mechanisms.

3.1 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.

The User Equipment is a commercial smartphone that is configured to provide secure data connections to the Enterprise Mobility Infrastructure and secure voice communications 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 2.1 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 2.2 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:

- Device protection capabilities, including system configuration, device monitoring, authentication, and updates
- VPN client
- Local key and certificate management for the VPN client and other applications

3.1.1 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 mobile device 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. It 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. Except at initial provisioning, User Equipment should be configured to disallow software installation because of limitations in current device management technologies. (See also Updates, page 9).

- **Device Monitoring:** A monitoring service must be available on the User Equipment in order to ensure that it operates under known, authorized conditions. It must start 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 new software has been installed and that all configuration settings are correct, monitoring the operating system, processes, applications, files, and interface port activities. The monitoring service must alert the user when issues are found and log the information locally to the User Equipment; initial deployments may have no provision for remote logging. 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 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 zeroes the device, rendering it inoperable for secure use. At the present time, the monitoring service rides on top of the operating system which itself rides on the hardware platform. It is recommended that monitoring service vendors work to incorporate monitoring functionality into system firmware. If the hardware and operating system is 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 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 is required to protect secure credential storage (such as VPN certificates and private keys). The corresponding authentication information (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:** Operating system updates are usually delivered to commercial smartphones using the carrier Over the Air (OTA) update process or via direct data connection to the operating system vendor. Since Enterprise Mobility currently limits these connections, initial deployments will not have remote software update capabilities for applications or the operating system, and these

updates can only be done by re-provisioning the User Equipment. For ongoing management, the carrier provides OTA updates to the radio interface software on the User Equipment. All non-essential updates must be blocked by the User Equipment.

3.1.2 VPN Client

Two layers of encryption will be used to protect all data carried over the carrier network. All data between User Equipment and the Enterprise Mobility Infrastructure is protected in a Virtual Private Network (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 AES for data encryption. FIPS 140-2 certification is required. Within IPsec/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 capability within the operating system exists, it must be configured to only allow IPsec/IKE VPN communications.

3.1.3 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, which the user must decrypt using a separate authentication (password or passphrase). The decrypted private keys must not be stored on non-volatile memory.

3.1.4 Gap Analysis

The configuration of the User Equipment may be the only area where the using organization can make changes from a standard commercial device. In order to provide additional protection to the User Equipment, some applications and services must be allowed to be removed, a monitoring service must be able to run, and physical/logical tamper detection measures must be added. Certain applications and parts of the operating system can be security hardened.

This security hardening must be achieved before the User Equipment is provided to a user. In initial deployments, any configuration changes to the device can only be accomplished by re-provisioning the device. By design, in this version of the Capability Package there is no mechanism to make changes to any components that are monitored or hardened.

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.

Operating system updates are usually delivered to commercial smartphones using the carrier OTA update process or via direct data connection to the operating system vendor. Since Enterprise Mobility does not allow these connections, initial deployments will not have remote software update capabilities for applications or the operating system, and these updates can only be done by re-provisioning the User Equipment. Device Management Services that can securely deploy signed updates to the User

Equipment within the VPN tunnel from the Enterprise Mobility Infrastructure will be needed to securely and remotely update software.

Commercial smartphones do not yet provide all of the security mechanisms and levels of assurance that are desired. Additional capabilities, such as mobile device integrity checks and hardware roots of trust, would provide greater assurance.

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.5 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 Carrier Service Integration are found in Appendix B.5.

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 CDMA-2000, UMTS or 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:

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

4.1.1 Cellular to Enterprise Connection

When implementing the Mobility Enterprise architecture, the integrator will need to decide how to connect the Enterprise Mobility Infrastructure to the cellular data network. Within cellular networks, mobile devices are provisioned and authorized by the carrier to connect to certain data networks. In GSM or LTE networks, these specific networks are often designated by a label called an Access Point Name (APN). CDMA data networks have a similar type of connection to a "Gateway". While the APN or Gateway identifies the data network that a handset should connect to for a given session, the important aspect to understand is the nature of the destination data network. This destination network could be a corporate network, a public network (e.g., the Internet) or a separate transport network (a carrier's private internal network). There are advantages and disadvantages with each of these choices.

- To provide some guaranteed QoS on the link, the Enterprise Mobility prototype used a private transport network to connect the carrier data network to the enterprise. Only one transport mechanism per user equipment should be available for any session. This also added a layer of security, as the IP address for the interface to the Enterprise Mobility Infrastructure is internal to the private transport network and not globally routable. The disadvantage of this choice is that the solution does not scale to support roaming beyond the home network.
- An alternate solution would be to connect from the carrier data network to the Enterprise Mobility Infrastructure via public transport (e.g., the Internet). This would provide an advantage to the integrator of allowing a wider service area, but would have the disadvantage of exposing the outer tunnel of encryption to the Internet under normal operation. It is also noted that QoS

on the transport link is unspecified and could create service issues. This solution is currently under study and may require additional mitigations.

- A hybrid approach could also be used, with non-roaming connections utilizing a private transport network, and roaming connections relying on public transport. This approach is still under study and may require security enhancements in the Government enterprise to ensure availability of the solution.

Options are being explored regarding implementing a Government cellular infrastructure to connect mobile devices to Government enterprises, in order to further protect the integrity of the User Equipment, protect subscriber account and usage information, and limit exposure to roaming partners.

4.1.2 Service-Level Expectations

The technology used in cellular radio and data networks has some ability to prioritize traffic based on need and bandwidth constraints. This Quality of Service (QoS) functionality was initially specified and developed for 3G networks to properly handle and enforce data usage, but it was never widely deployed. In a 3G-based network, there should be no expectation of a guaranteed level of service from the carriers.

With the introduction of 4G systems, there are mechanisms specified to have per-service based bearers established in the packet core and enforced. There are many advantages to implementing QoS, including optimizing the use of limited radio resources and network bandwidth. Carriers seek to use this efficiency in providing differentiated services and to increase revenues.

While 4G networks hold promise for improved QoS for data applications, the use of an IPsec VPN may preclude 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 Mobile Device Dependencies on Carrier and Manufacturer

The User Equipment contains the baseband processor, which is the signal processor to connect to the Radio Access Network (RAN). 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.

While most of the features discussed in the Mobility Capability Package reside in the mobile device's applications processor and its operating system, it is important for the integrator to understand the role of the baseband processor in providing the interface to the cellular network, and in some cases, managing connections from the applications processor to device peripherals (such as the microphone). Given its importance to the ecosystem, it is important for an integrator to understand the functions controlled by the baseband processor, and the hardware architecture of the mobile device.

The carrier, often in partnership with the manufacturer of the mobile device, has deployed architecture to configure and manage the software for the 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 mobile device verifies the signature on installation and/or boot.

4.1.4 Disabling Voice and SMS Services

The Enterprise Mobility architecture requires that the only commercial network service allowed for use by the mobile device 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 voice service or SMS while configured for secure use.

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 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.

5.1 Objective Enterprise Mobility Infrastructure Architecture

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

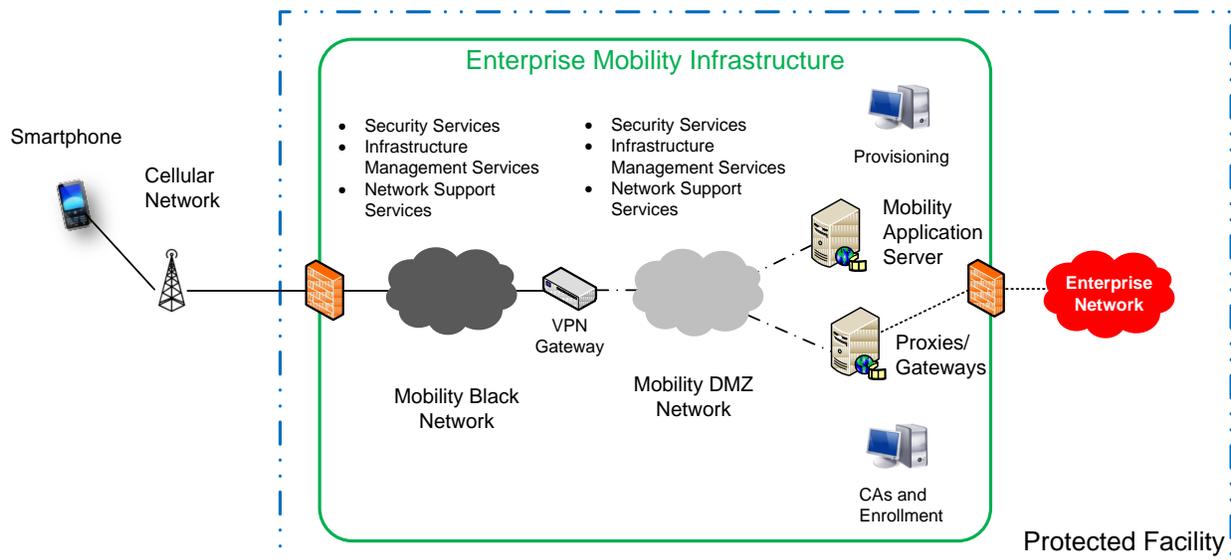


Figure 5-1. Objective Enterprise Mobility Infrastructure Architecture

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 Secure VoIP and Web-based Non-Resident Data services over a cellular Access Network.

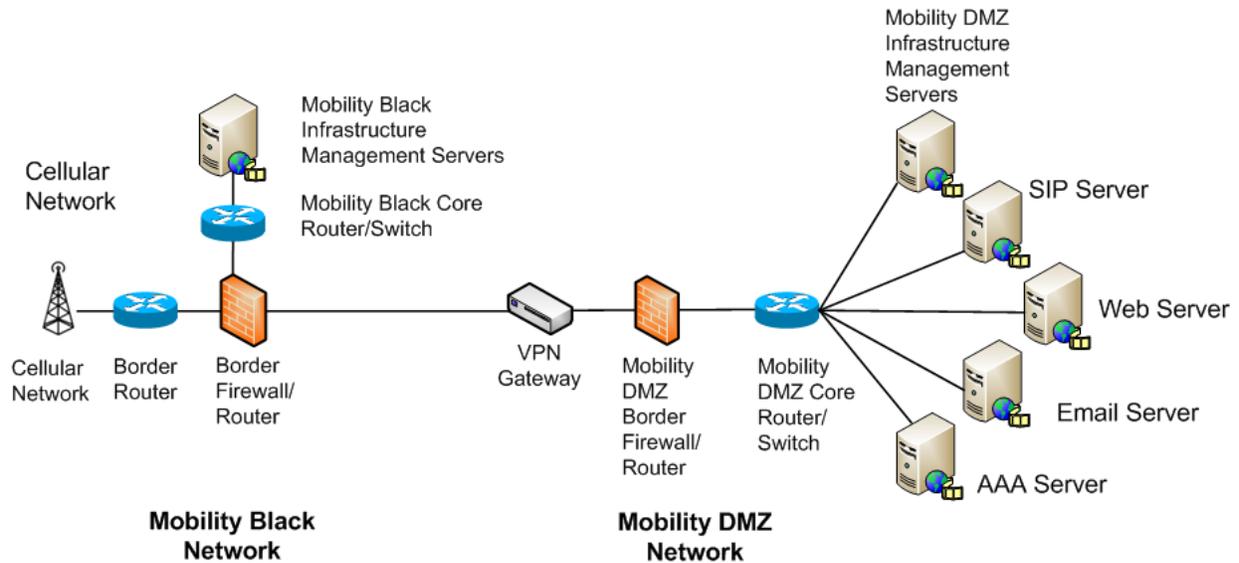


Figure 5-2. Prototype Enterprise Mobility Infrastructure Architecture

A brief description of the components follows, with more detailed architecture and configuration requirements provided in Appendix A and functional requirements in Appendix C. 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:

- **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 National Security System. To assist the using agency's accrediting officials, test criteria for the Infrastructure are found in Appendix B.7.
- **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 National Security System. To assist the using agency's accrediting officials, test criteria for the Infrastructure are found in Appendix B.7.

- **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 DMZ Network Components

The following components may be deployed as part of the Mobility DMZ 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 Internet Key Exchange (IKE) with mutual public key certificate authentication with Suite B compliant cryptosuites. 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.2 and functional requirements in Appendix C.2 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 VPN Capability are found in Appendix B.2.
- **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 cryptosuites. 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 user ID and password supplied in the TLS-protected session. The SIP Server may consult a AAA Server on the Enterprise Mobility Infrastructure for this user authentication/authorization. More information on SVOIP capabilities may be found in Section 2.1. Threshold requirements in Appendix A.3 and functional requirements in Appendix C.3 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, test criteria for the SVOIP capability are found in Appendix B.3.
- **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 2.2. Threshold requirements in Appendix A.4 and functional requirements in Appendix C.4 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 Web capability are found in Appendix B.4.
- **Email Server:** The Email Server indirectly provides web-based email services to User Equipment via the Web Server. See Section 2.2 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 National Security System. To assist the using agency’s accrediting officials, test criteria for the Infrastructure are found in Appendix B.7.

- **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 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 B.7.
- **Mobility DMZ Core Switch/Router:** The Mobility DMZ Core Switch/Router provides access to Mobility DMZ Network applications and support services, which as described in Section 5.2.3.

Although use of Mobile Device Management (MDM) services is a goal, the prototype Enterprise Mobility Infrastructure does not make use of MDM, and relies on return of the mobile device for re-provisioning.

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 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. 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 B.7.
- **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 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 B.7.
- **Backup Service:** This service is used to back up infrastructure components, but not User Equipment.

Additional network support services (such as DNS Servers, NTP Servers, and 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 Stand-alone Provisioning Components

Note: these components are not pictured in Figure 5-2, since they are not connected to the prototype Enterprise Mobility Infrastructure network.

Components that primarily provide provisioning functions include certificate and trust management systems, and workstations used to configure and initialize User Equipment for secure operations. The following stand-alone provisioning components are deployed in the prototype Enterprise Mobility Infrastructure:

- **Outer (VPN) Certificate Authority and Enrollment Workstation:** The goal is to use Government Enterprise Public Key Infrastructures (PKIs), but initial Certificate Authorities may be stand-alone commercial products. The prototype Enterprise Mobility Infrastructure includes a stand-alone Certificate Authority with an associated Enrollment Workstation 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 A.8 and functional requirements in Appendix C.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 PKI components are found in Appendix B.8.
- **Inner (User) Certificate Authority and Enrollment Workstation:** The goal is to use Government PKIs, but initial Certificate Authorities may be stand-alone commercial products. The prototype Enterprise Mobility PKI Components includes a stand-alone Certificate Authority with an associated Enrollment Workstation 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 A.8 and functional requirements in Appendix C.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 PKI components are found in Appendix B.8.
- **Provisioning Workstation:** Provisioning of User Equipment is performed using a dedicated terminal that is not connected to any network. This terminal 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 Workstation found in Appendix A.9 and functional requirements in Appendix C.8 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 provisioning components are found in Appendix B.9.

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 mobile device or within Enterprise Mobility Infrastructure, or other unauthorized modifications of mobile devices or infrastructure components
- Sensitive data being stored unprotected on mobile devices
- Loss of authentication credentials such as passwords or private keys for certificates
- Disruption of services
- Software flaws, out-of-date OSes, and 3rd party firmware to gain access to device features that are locked by default.
- Near field communications (magnetic field induction – inductive coupling), threat from eavesdropping.
- Exposure of mobile phone number to prevent Vishing and Phishing.
- Improper disposal of old cell phones with sensitive configurations and/or data.
- Improper use of social media applications.

6.2 Threats

Some principal threat areas to address are:

- Attacks on mobile devices 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 mobile devices 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 mobile device 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:

- 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 Risk Mitigations

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 mobile devices 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 mobile device – 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.
- 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 mobile device 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.

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 access point threat could be mitigated through use of mutual authentication in the cellular radio network.

Acronyms and Terms

Acronym	Description
3G	Third Generation wireless telephone technology
4G	Fourth Generation standard for mobile telecommunications
AAA	Authentication, Authorization, and Accounting
AES	Advanced Encryption Standard
APN	Access Point Name
B2BUA	Back-to-Back User Agent
CA	Certificate Authority
CDMA	Code Division Multiple Access, a 3G mobile communications standard
CRL	Certificate Revocation Lists
CSfC	Commercial Solutions for Classified
DAO	Delegated Authorizing Official
DHS	Department of Homeland Security
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DoD	Department of Defense
E911	Enhanced 9-1-1
EBC	Edge Border Control
FIPS	Federal Information Processing Standards
GSM	Global System for Mobile Communications
IAD	Information Assurance Directorate
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
LTE	Long Term Evolution
MDM	Mobile Device Management
NAT	Network Address Translation
NIAP	National Information Assurance Partnership
NTP	Network Time Protocol
OCSP	Online Certification Status Protocol
OS	Operating System
OTA	Over The Air
PAT	Port Address Translation
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standards
QoS	Quality of Service
RFC	Request for Comment
RTP	Real-time Protocol

Acronym	Description
S/MIME	Secure/Multipurpose Internet Mail Extensions
SBC	Session Border Controller
SDES	Security Descriptions
SDP	Session Description Protocol
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SRTCP	Secure Real Time Control Protocol
SRTP	Secure Real Time Protocol
SVoIP	Secure Voice Over Internet Protocol
TLS	Transport Layer Security
UE	User Equipment
UMTS	Universal Mobile Telephone Service
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity

Specialized Terms

Term	Description
Fixed Devices	Non-mobile devices that include servers, network appliances, and other infrastructure components that are not mobile.
Objective	An objective (O) requirement specifies a feature or function that the Government desires and expects.
REQUIRED	This word or "SHALL" mean 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
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).

Consolidated References

National Policies:

- NSTISSP-11 Fact Sheet for National Information Assurance Acquisition Policy
- CNSSP-15 National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information
- CNSSD-502 National Policy on the Security of National Security Systems

Protection Profiles (available from NIAP):

- Security Requirements for Network Devices
- Network Device Protection Profile Extended Package: Stateful Traffic Filter Firewall
- Network Device Protection Profile Extended Package: IPsec VPN Gateway
- Security Requirements for Voice over IP Application
- Security Requirements for Mobility SIP Server
- Security Requirements for Mobile Operating Systems

Suite B references:

- IETF RFC 6379 "Suite B Cryptographic Suites for 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 "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 5346 "The Transport Layer Security (TLS) Protocol"

- 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”

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 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.

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.

Table A-1. Requirement Designators

Designator	Requirements Addressed
MOB	Overarching MOB ility requirements that solutions fielded using this CP should implement
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 E rastructure host A rchitecture
IFB	Requirements for I n E rastructure host B oundary protection
IFH	Requirements for I n E rastructure h ost systems
IFM	Requirements for I n E rastructure host M anagement
IFN	Requirements for I n E rastructure host N etworking
IFS	Requirements for I n E rastructure host S ecurity services
SVC	Requirements for the S VoIP c lient running on the User Equipment
SVP	Requirements for the overall S VoIP infrastructure
SVS	Requirements for the S VoIP 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, S martPhone
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 A-2. Overarching Mobility Requirements

REQUIREMENT NUMBER	REQUIREMENT DESCRIPTION	THRESHOLD/OBJECTIVE	Architecture/Configuration/Guidance (A/C/G)
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
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
MOB.03	Products for each layer of network encryption shall be from different vendors.	T=O	A
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
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
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.	T=O	A
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
MOB.08	Every device/component shall be issued unique certificates and corresponding private keys for authentication.	T=O	A
MOB.09	The authentication certificates for each layer of network encryption shall be issued by different Certificate Authorities.	T=O	A
MOB.10	All components of the system shall have been approved via NIAP and NSA's Commercial Solutions for Classified	T=O	A
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

REQUIREMENT NUMBER	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE	Architecture/ Configuration/ Guidance (A/C/G)
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
MOB.13	All cryptographic algorithms shall conform to the full Suite B standard as documented in CNSSP-15.	O	A
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
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
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

A.2 VPN Requirements

Table A-3. VPN Requirements

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE	Architecture/ Configuration/ Guidance (A/C/G)
VPN.00	Overarching VPN Requirements		
VPN.01	The VPN shall be a non-proprietary, standards based IPsec solution.	T=O	A
VPN.02	The VPN Gateway and client shall use IPsec in tunnel-mode.	T=O	A
VPN.03	The VPN Gateway and client shall use IKEv1.	T	A
VPN.04	The VPN Gateway and client shall use IKEv2.	O	A
VPN.05	The VPN Gateway and client shall be configured to use the cipher suites specified in IETF RFC 6379 "Suite B Cryptographic Suites for IPsec"	T=O	C
VPN.06	The VPN Gateway and client shall be configured to prohibit split-tunneling.	T=O	C
VPN.07	The VPN Gateway and client shall be configured to maintain the tunnel even if applications are not transmitting data.	O	C
VPN.08	The VPN client shall be able to automatically reconnect the VPN.	O	A

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE	Architecture/ Configuration/ Guidance (A/C/G)
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
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
VPG.03	The VPN Gateway shall audit and report all integrity check failures.	T=O	C
VPG.04	The VPN Gateway shall be configured in accordance with applicable DoD or using organization guidance.	T=O	C
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
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
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
VPG.08	The VPN Gateway shall perform certificate path validation.	T=O	C
VPG.09	The VPN Gateway shall check for revoked certificates.	T=O	C
VPG.10	The VPN Gateway shall check for invalid certificates.	T=O	C
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
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

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

Table A-4. SVoIP Requirements

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE	Architecture/ Configuration/ Guidance (A/C/G)
SVP.00	Overarching SVoIP Requirements		
SVP.01	The Enterprise Mobility Solutions shall use the Suite B cryptosuite.	T=O	A
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
SVP.03	The User Equipment SVoIP Client shall use the SDES-SRTP Protocol.	T=O	A
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
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
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
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
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
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
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

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE	Architecture/ Configuration/ Guidance (A/C/G)
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
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
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.	T=O	C
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
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
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.	T=O	C
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
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 mobile device, in order to establish the TLS channel for SIP messages.	T=O	C

A.4 Web Based Non-Resident Data Requirements

Table A-5. Web Based Non-Resident Data Requirements

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE	Architecture/ Configuration/ Guidance (A/C/G)
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
WND.02	The web browser shall be included in any permitted applications white list.	T=O	A
WND.03	The web browser shall be able to pass user identity certificates as application credentials.	O	C
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
WNC.02	The web browser shall be configured to connect to only authorized web servers.	T=O	C
WNC.03	The web browser shall be configured to use the existing outer VPN tunnel for network access.	T=O	C
WNC.04	The web browser shall be configured to disable any encryption protocol that is not Suite B compliant.	T=O	C
WNC.05	Web browser history shall only be maintained in volatile memory on the User Equipment.	T=O	C
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
WNC.07	The web browser shall use a Suite B compliant Transport Layer Security (TLS) protocol 1.2 or later.	T=O	C
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
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
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
WNS.02	The web server shall be configured to reject SSL encryption handshakes	T=O	C
WNS.03	The web server shall be able to re-authenticate user equipment.	O	C
WNS.04	The web server shall be able to be configured to use user identity certificates to authenticate users.	O	C

A.5 Carrier Service Integration

Table A-6. Carrier Service Integration Requirements

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE	Architecture/ Configuration/ Guidance (A/C/G)
CSI.00	Carrier Service Integration		
CSI.01	The Enterprise Mobility Infrastructure Integrator shall negotiate with the carrier QoS of IPsec VPN traffic from/to mobile devices that provides 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
CSI.03	The using agency shall be cognizant of rogue carrier threats and build contingency plans in response	T=O	A
CSI.04	The Enterprise Mobility Infrastructure Integrator shall use Suite B compliant cryptosuites	T=O	C
CSI.05	The Enterprise Mobility Infrastructure shall have a documented plan to detect and mitigate rogue base stations	T=O	C

A.6 User Equipment Requirements

Table A-7. User Equipment Requirements

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE	Architecture/ Configuration/ Guidance (A/C/G)
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
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
UES.03	The User Equipment screen lock shall be configured to lock in accordance with applicable DoD or using agency guidance of automatic lock after a configurable amount of time	T=O	C
UES.04	The User Equipment shall be configured to allow the USB cable to be used only to charge the device.	T=O	C
UES.05	The User Equipment shall be configured to disable processing of incoming cellular messaging services.	T=O	C

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE	Architecture/ Configuration/ Guidance (A/C/G)
UES.06	The User Equipment shall be configured to disable outgoing cellular messaging services.	T=O	C
UES.07	The User Equipment shall be configured to disable incoming cellular voice calls.	T=O	C
UES.08	The User Equipment shall be configured to disable outgoing cellular voice calls.	T=O	C
UES.09	The User Equipment shall be configured to disable dial-up modem or tethering capabilities.	T=O	C
UES.10	The User Equipment shall be configured to disable Bluetooth.	T=O	C
UES.11	The User Equipment shall be configured to disable Wi-Fi.	T=O	C
UES.12	The User Equipment shall be configured to disable Auto Answer.	T=O	C
UES.13	The User Equipment shall be configured to disable Voice Mail.	T=O	C
UES.14	The User Equipment shall be configured to disable Automatic Redial.	T=O	C
UES.15	The User Equipment shall be configured to disable all transmitted GPS and location services except E911 or those authorized by the DAO.	T=O	C
UES.16	The system shall be configured to disable any feature that will be capable of "Phoning home" or reporting back to a centralized vendor-managed server.	T=O	C
UES.17	The User Equipment shall be configured with Over the Air (OTA) updates from the carrier disabled that are not absolutely required for the phone to access the network.	T=O	C
UES.18	The User Equipment operating system firewall shall be configured according to DoD and local system policy.	O	C
UES.19	The User Equipment operating system firewall shall be configured to only allow IKE and IPsec traffic.	O	C
UES.20	The Certificate storage password shall be configured for length and complexity in according with DoD or using agency policy on mobile security.	T=O	C
UES.21	The User Equipment shall be configured to receive configuration policies and software updates from authorized remote systems.	O	C

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE	Architecture/ Configuration/ Guidance (A/C/G)
UES.22	The User Equipment screen lock shall be configured to lock in accordance with applicable DoD or using agency guidance of automatic lock after a configurable number of incorrect authentication attempts	T=O	C
UES.23	The User Equipment shall employ visually inspectable tamper indicating technology	T	G
UES-24	The User Equipment shall employ active electronic/logical tamper indicating technology	O	G
UEA.00	User Equipment Monitoring Service Requirements		
UEA.01	The User Equipment Monitoring Service shall classify the insertion or removal of removable media as a Minor Fault.	T=O	C
UEA.02	The transition of the Wi-Fi service from "Disabled" to "Enabled" shall be considered a Major Fault.	T=O	C
UEA.03	The transition of the Bluetooth service from "Disabled" to "Enabled" shall be considered a Major Fault.	T=O	C
UEA.04	The detection of a USB data connection shall be considered a Major Fault.	T=O	C
UEA.05	The dialing of '911' shall be considered a Major Fault.	T=O	C
UEA.06	The User Equipment Monitoring Service shall classify detection of the starting or discovery of unauthorized process detections as a Minor Fault unless explicitly defined as a Major Fault	T=O	C
UEA.07	The User Equipment Monitoring Service shall classify unauthorized file system changes as a Minor Fault.	T=O	C
UEA.08	The User Equipment Monitoring Service shall be configured to visually, audibly, and haptically notify the user upon detection of a Major or Minor Fault.	T=O	C
UEA.09	The User Equipment Monitoring Service shall be configured to vibrate to alert the user upon detection of a Major Fault.	T=O	C
UEA.10	The User Equipment Monitoring Service shall remove any files containing encrypted or decrypted certificates or key material upon detection of a Major Fault. (Zeroize/Tamper the device)	T=O	C
UEA.11	The User Equipment Monitoring Service shall terminate any encryption utility upon detection of a Major Fault.	T=O	C
UEA.12	The User Equipment Monitoring Service shall terminate any VPN client process upon detection of a Major Fault.	T=O	C

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE	Architecture/ Configuration/ Guidance (A/C/G)
UEA.13	The User Equipment Monitoring Service shall allow standard phone calls upon detection of a Major Fault.	T=O	C
UEA.14	The User Equipment Monitoring Service shall be configured to notify the user of Major and Minor Faults.	T=O	C
UEA.15	The User Equipment Monitoring Service shall be configured to log all Faults.	T=O	C
UEA.16	The User Equipment Monitoring Service shall block standard phone calls.	T=O	C

A.7 Enterprise Mobility Infrastructure Requirements

Table A-8. Infrastructure Requirements

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE	Architecture/ Configuration/ Guidance (A/C/G)
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
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
IFB.03	The Enterprise Mobility Infrastructure shall implement Network Firewalls in accordance with applicable DoD or using agency policy and guidance.	T=O	A
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
IFH.02	An Infrastructure Host System shall authenticate users in accordance with applicable DoD or using agency policy and guidance.	T=O	C
IFH.03	An Infrastructure Host System shall prohibit unauthorized users from accessing resources.	T=O	C
IFH.04	An Infrastructure Host System shall maintain separation of user roles.	T=O	C

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/OBJECTIVE	Architecture/Configuration/Guidance (A/C/G)
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
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
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
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
IFH.09	An Infrastructure Host System shall verify the integrity of its software environment.	T	C
IFH.10	An Infrastructure Host System shall implement hardware roots of trust for performing integrity verification and reporting (attestation).	O	C
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
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
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

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE	Architecture/ Configuration/ Guidance (A/C/G)
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
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
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
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
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
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
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
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
IFS.02	The Enterprise Mobility Infrastructure Security Services shall provide integrity protection of audit records in transit from infrastructure components.	T=O	A

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE	Architecture/ Configuration/ Guidance (A/C/G)
IFS.03	The Enterprise Mobility Infrastructure Security Services shall provide integrity protection of audit records at rest.	T=O	A
IFS.04	The Enterprise Mobility Infrastructure Security Services shall support Windows Domain authentication if the infrastructure includes components running Microsoft Windows.	T=O	A
IFS.05	The Enterprise Mobility Infrastructure Security Services shall support Kerberos authentication if the infrastructure includes components running Linux.	T=O	A
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
IFS.07	The Enterprise Mobility Infrastructure Security Services shall require the authentication of users based on userid and password.	T=O	C
IFS.08	The Enterprise Mobility Infrastructure Security Services shall authorize access using role-based access control	T=O	C
IFS.09	The Enterprise Mobility Infrastructure Security Services shall audit all authentication and authorization failures.	T=O	C
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
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
IFA.00	Enterprise Mobility Infrastructure Architecture Requirements		
IFA.01	The Enterprise Mobility Infrastructure shall implement Directory Services.	T=O	A
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
IFA.03	The Enterprise Mobility Infrastructure shall provide DNSSEC Servers within the infrastructure networks.	O	A
IFA.04	The Certificate Validation Service shall validate X.509 certificates.	T=O	C

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE	Architecture/ Configuration/ Guidance (A/C/G)
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
IFA.06	The Enterprise Mobility Infrastructure Security Services shall be configured to enable posting of full CRLs to the Directory Service.	O	C
IFA.07	The Enterprise Mobility Infrastructure Security Services shall be configured to enable posting of delta CRLs to the Directory Service.	O	C
IFA.08	The Enterprise Mobility Infrastructure Security Services shall include a Certificate Validation Service.	O	C
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
IFN.02	If implemented, the Enterprise Mobility Infrastructure shall provide Network Time Servers that provide time synchronization within the infrastructure networks.	T=O	A
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
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
IFN.05	The Enterprise Mobility Infrastructure Directory Services shall be configured to allow storage of X.509 certificates.	T=O	C
IFN.06	The Enterprise Mobility Infrastructure Directory Services shall be configured to allow storage of X.509 CRLs.	T=O	C
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

A.8 PKI Requirements

Table A-9. PKI Requirements

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE	Architecture/ Configuration/ Guidance (A/C/G)
ECA.00	Certificate, Key, and Trust Management		
ECA.01	The Certificate Authority cryptomodule shall be FIPS 140-2 compliant.	T=O	C
ECA.02	A Certificate Authority service shall be configured to generate user certificates.	T=O	C
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 for user certificates.	T=O	C
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
ECA.05	The Certificate Authority service shall maintain a Certificate Revocation List (CRL).	T=O	C
ECA.06	The Certificate Authority service shall process certificate revocation requests.	T=O	C
ECA.07	The Certificate Authority service shall be configured to process PKCS #7 and #10 messages.	T=O	C
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
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
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
EWS.03	The Enrollment Workstation shall be able to accept entry of requests for user certificates.	T=O	C
EWS.04	The Enrollment Workstation shall be able to interface to non-secure removable media.	T=O	C
EWS.05	The Enrollment Workstation shall generate certificates for the digital signature algorithms defined in CNSSP-15, Annex C.	T	C
EWS.06	The Enrollment Workstation shall generate certificates for the digital signature algorithms defined in CNSSP-15, Annex B.	O	C

A.9 Provisioning Requirements

Table A-10. Provisioning Requirements

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE	Architecture/ Configuration/ Guidance (A/C/G)
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
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
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
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

Appendix B Test Criteria - Enterprise Mobility

B.1 Test Criteria for the Overarching Mobility Requirements

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 that results 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 capability package.

Table B-1. Requirements Designators

Designator	Requirements Addressed
MOB	Overarching MOB ility requirements that a solution fielded using this CP should implement
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
SVC	Requirements for the S V oIP c lient running on the User Equipment
SVP	Requirements for the overall S V oIP infrastructure
SVS	Requirements for the S V 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, S martPhone
VPG	Requirements applicable to the V PN G ateway
VPN	Requirements for designing and implementing the V PN 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

Table B-2. Overarching Mobility Test Criteria

Requirement Number	Test Criteria
	Overarching Mobility Requirements
MOB.01	<p>All network traffic across an untrusted transport medium shall be protected by a minimum of two layers of encryption.</p> <ol style="list-style-type: none"> 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? <ol style="list-style-type: none"> a. How is the original data first encrypted? b. How is the once encrypted data encrypted a second time?
MOB.02	<p>The Mobility components providing the outer layer of encryption and inner layer of encryption shall use non-proprietary standards based protocols.</p> <ol style="list-style-type: none"> 1. Identify which encryption standards are used to protect the inner and outer layers of encryption 2. Are the encryption algorithms non-proprietary and standards-based? <ol style="list-style-type: none"> a. Is the encryption CNSSP-15 (Suite B) compliant? b. Has the encryption software been approved by NIST and compliant with FIPS 140-2 3. Verify that the encryption algorithms are based on non-proprietary standards based protocols
MOB.03	<p>Products for each layer of network encryption shall be from different vendors.</p> <ol style="list-style-type: none"> 1. Determine which vendors provide the products used for the inner and outer layers of encryption 2. Verify that the vendor product used to encrypt the inner layer of encryption is not the same as the product used to encrypt the outer layer of encryption
MOB.04	<p>The software for each layer of network encryption shall not use the same software cryptographic libraries or depend on the same services.</p> <ol style="list-style-type: none"> 1. Enumerate 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	<p>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.</p> <ol style="list-style-type: none"> 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	<p>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.</p>

Requirement Number	Test Criteria
	<ol style="list-style-type: none"> 1. Identify all Mobility components providing encryption for inner and outer layers 2. Identify base OS used in each Mobility component 3. Verify that each Mobility component does not use the same base OS
MOB.07	<p>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.</p> <ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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	<p>Every device/component shall be issued unique certificates and corresponding private keys for authentication.</p> <ol style="list-style-type: none"> 1. Identify all the devices/components that use a digital certificate 2. Compare all the digital certificates 3. Verify that each certificate is unique <ol style="list-style-type: none"> a. Ensure no two certificates share the same issuer/serial number field b. Ensure each certificate has a corresponding private key
MOB.09	<p>The authentication certificates for each layer of network encryption shall be issued by different Certificate Authorities.</p> <ol style="list-style-type: none"> 1. Identify the authentication certificates for each layer of network encryption 2. Compare the digital certificates 3. Verify that no two certificates share the same Certificate Authority
MOB.10	<p>All components of the system shall have been approved via NIAP and NSA's Commercial Solutions for Classified</p> <ol style="list-style-type: none"> 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	<p>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).</p> <ol style="list-style-type: none"> 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 user authentication steps <ol style="list-style-type: none"> a. The user must enter a password, passphrase or PIN on two separate occasions that are different.

Requirement Number	Test Criteria
MOB.12	<p>All cryptographic algorithms will conform to the Suite B standard or the Suite B transitional standard as documented in CNSSP-15.</p> <ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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	<p>All cryptographic algorithms will conform to the full Suite B standard as documented in CNSSP-15.</p> <ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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	<p>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.</p> <ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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	<p>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.</p> <ol style="list-style-type: none"> 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	<p>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.</p>

Requirement Number	Test Criteria
	<ol style="list-style-type: none"> 1. Identify the Certification Practice Statement (CPS) for the network system 2. Verify the CPS includes applicable DoD or using agency guidance

B.2 Test Criteria for Overarching VPN Requirements

Table B-3. VPN Test Criteria

Requirement Number	Test Criteria
	Overarching VPN Requirements
VPN.01	<p>The VPN shall be a non-proprietary, standards based IPsec solution.</p> <ol style="list-style-type: none"> 1. Identify the IPsec standards used by the VPN 2. Verify the IPsec standards are non-proprietary and standards-based? <ol style="list-style-type: none"> 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	<p>The VPN Gateway and client shall use IPsec in tunnel-mode.</p> <ol style="list-style-type: none"> 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	<p>The VPN Gateway and client shall use IKEv1.</p> <ol style="list-style-type: none"> 1. Identify the VPN Gateway and client platforms 2. Configure the VPN Gateway's IPsec protocol to use IKEv1 3. Configure the VPN client's IPsec protocol to use IKEv1 4. Verify both the VPN Gateway and client settings are configured for IKEv1
VPN.04	<p>The VPN Gateway and client shall use IKEv2.</p> <ol style="list-style-type: none"> 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	<p>The VPN Gateway and client shall be configured to use the cipher suites specified in IETF RFC 6379 "Suite B Cryptographic Suites for IPsec".</p> <ol style="list-style-type: none"> 1. Identify the VPN Gateway and client platforms 2. Review the encryption configuration of each platform <ol style="list-style-type: none"> 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 6379 under "Suite B Cryptographic Suites for IPsec"
VPN.06	<p>The VPN Gateway and client shall be configured to prohibit split-tunneling.</p> <ol style="list-style-type: none"> 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

Requirement Number	Test Criteria
VPN.07	<p>The VPN Gateway and client shall be configured to maintain the tunnel even if applications are not transmitting data.</p> <ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> a. Launch an app that requires access to the network through the VPN tunnel to test connectivity
VPN Gateway Requirements	
VPG.01	<p>The VPN Gateway shall audit and report all unsuccessful attempts to establish a security association.</p>
	<ol style="list-style-type: none"> 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 the VPN Gateway and deliberately fail <ol style="list-style-type: none"> a. Use a device with an invalid digital certificate 5. Verify the VPN Gateway audited and reported the failed connection attempt <ol style="list-style-type: none"> a. Ensure the auditing and reporting is in accordance with applicable guidance
VPG.02	<p>The VPN Gateway shall audit and report successful attempts to establish a security association in accordance with applicable DoD or using agency guidance.</p>
	<ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> a. Ensure the auditing and reporting is in accordance with applicable guidance
VPG.03	<p>The VPN Gateway shall audit and report all integrity check failures.</p>

Requirement Number	Test Criteria
	<ol style="list-style-type: none"> 1. Identify the VPN Gateway and bring up the audit and report settings 2. Configure the VPN Gateway to log all integrity check failures <ol style="list-style-type: none"> a. Ensure IPsec/ESP (Encapsulating Security Protocol) is enabled b. Ensure IPsec/HA (Header Authentication) 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.
	<ol style="list-style-type: none"> 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.
	<ol style="list-style-type: none"> 1. Identify the VPN Gateway DHCP configuration settings 2. Configure the VPN Gateway for DHCP address assignment <ol style="list-style-type: none"> 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.
	<ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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.

Requirement Number	Test Criteria
	<ol style="list-style-type: none"> 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.
	<ol style="list-style-type: none"> 1. Identify the VPN Gateway configuration settings for certificate acceptance and path validation 2. Enable settings for accepting CA subordinate certificates
VPG.09	The VPN Gateway shall check for revoked certificates.
	<ol style="list-style-type: none"> 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 No Test Cases Written Yet
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.
	<ol style="list-style-type: none"> 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 3. Configure a device using a digital certificate 4. Revoke the device's digital certificate <ol style="list-style-type: none"> a. Add it to the blacklist b. Remove it from the white list 5. Attempt to connect the device with revoked certificate to the network through the VPN Gateway 6. Verify the device's connection was rejected due to the certificate being on the blacklist 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 No Test Cases Written Yet

B.3 Test Criteria for Overarching SVoIP Requirements

Table B-4. SVoIP Test Criteria

Requirement Number	Test Criteria
	Overarching SVoIP Requirements
SVP.01	<p>The Enterprise Mobility Solutions shall use the Suite B cryptosuite.</p> <ol style="list-style-type: none"> 4. Identify all encryption algorithms used to protect data at every layer for transmission across an untrusted communications link 5. Identify the classification of the data being transmitted 6. Verify all algorithms meet the required strength for the classification in accordance with Suite B and Suite B Transitional as stated in CNSSP-15 <ol style="list-style-type: none"> a. 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	<p>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.</p> <ol style="list-style-type: none"> 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	<p>The User Equipment SVoIP Client shall use the SDES-SRTP Protocol.</p> <ol style="list-style-type: none"> 1. On the client device, review the 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	<p>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.</p> <ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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	<p>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.</p>

Requirement Number	Test Criteria
	<ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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	<p>The Enterprise Mobility System shall provide the capability for User Equipment to communicate with fixed enterprise VoIP devices operating at the same classification level.</p> <ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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	<p>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.</p> <ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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	<p>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.</p>

Requirement Number	Test Criteria
	<ol style="list-style-type: none"> 1. Install an authorized digital certificate on the User Equipment that was created by a designated SVoIP Certificate Authority 2. Verify the User Equipment connects to the Enterprise Mobility System 3. Install an unauthorized digital certificate on the User Equipment 4. Verify the Enterprise Mobility System rejects the User Equipment's connection
SVP.09	<p>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.</p> <ol style="list-style-type: none"> 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	<p>The Enterprise Mobility System and User Equipment client shall be configured to use a password for client authentication for SIP REGISTER function requests.</p> <ol style="list-style-type: none"> 1. Attempt to register the User Equipment with the Enterprise Mobility System SIP Server 2. Ensure that a password is requested to register <ol style="list-style-type: none"> 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
SVP.11	<p>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.</p> <p>No test available for this objective requirement at this time</p>
SVoIP Server Requirements	
SVS.01	<p>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.)</p> <ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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

Requirement Number	Test Criteria
SVS.02	<p>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.</p> <ol style="list-style-type: none"> 1. On the SVoIP Mobility System, configure the SIP Server to connect VoIP traffic directly between UEs via the Grey Network VPN tunnels after the SIP Server has established the VoIP connection <ol style="list-style-type: none"> 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 on the Grey Network using SRTP <ol style="list-style-type: none"> 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	<p>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.</p> <ol style="list-style-type: none"> 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 and establish a SVoIP connection 3. Verify the Caller-ID messages on each phone are correct <ol style="list-style-type: none"> a. The “home” User Equipment displays the Caller-ID of the “far-end” phone on its display b. The “far-end” User Equipment displays the Caller-ID of the “home” phone on its display
SVS.04	<p>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.</p>

Requirement Number	Test Criteria
	<ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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	<p>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.</p> <ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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	<p>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.</p>

Requirement Number	Test Criteria
	<ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> a. Review the SIP Server logs to determine the Caller-ID
SVS.07	<p>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 mobile device, in order to establish the TLS channel for SIP messages.</p> <ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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.4 Test Criteria for Web Based Non-Resident Data Requirements

Table B-5. Web Based Non-Resident Data Test Criteria

Requirement Number	REQUIREMENT DESCRIPTION
	Overarching Web Browser Non-Resident Data Requirements
	The inner TLS tunnel shall be used to transit all traffic between the web browser and the web server.
WND.01	<ol style="list-style-type: none"> 1. Connect User Equipment to the Enterprise Mobility Infrastructure <ol style="list-style-type: none"> a. Ensure the outer tunnel is established 2. Connect to the thin client using the device's browser 3. Review the browser connection details for the encryption used 4. Verify the connection is protected using TLS
	The web browser shall be included in any permitted applications white list.
WND.02	<ol style="list-style-type: none"> 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.
	<ol style="list-style-type: none"> 1. On the User Equipment, review settings for: <ol style="list-style-type: none"> a. Offline storage b. Caching c. Downloads d. History 2. Verify that storage settings do not use non-volatile memory <ol style="list-style-type: none"> 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.
	<ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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.
	<ol style="list-style-type: none"> 1. Connect User Equipment to the Enterprise Mobility Infrastructure <ol style="list-style-type: none"> a. Ensure the outer tunnel is established 2. Connect to the thin client through the web browser 3. Verify the web browser connection is tunneled through the outer VPN tunnel
WNC.04	The web browser shall be configured to disable any encryption protocol that is not Suite B compliant.
	<ol style="list-style-type: none"> 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 User Equipment to the thin client 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.
	<ol style="list-style-type: none"> 1. On the User Equipment, review the browser history settings 2. Verify the history settings do not use non-volatile memory
WNC.06	The web browser shall be configured to disable the use of all versions of the Secure Sockets Layer (SSL) protocol.

	<ol style="list-style-type: none"> 1. Review the connection settings for the User Equipment’s browser connection 2. Disable all SSL settings 3. Connect User Equipment to the thin client 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.
	<ol style="list-style-type: none"> 1. Review the connection settings for the User Equipment’s browser connection 2. Enable TLS 1.1 or later or another approved cryptographic protocol 3. Connect User Equipment to the thin client 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.
	<ol style="list-style-type: none"> 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
	<ol style="list-style-type: none"> 1. Review the connection settings for the web server connection 2. Enable the following encryption capabilities <ol style="list-style-type: none"> a. TLS is enabled b. The only allowable encryption includes those algorithms defined as part of Suite B c. SSL and non-Suite B algorithms have been disabled 3. Connect User Equipment to the 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 and a Suite B algorithm
WNS.02	The web server shall be configured to reject SSL encryption handshakes
	<ol style="list-style-type: none"> 1. Review the connection settings for the web server connection 2. Disable all SSL settings 3. Attempt User Equipment connection to the thin client using SSL protocol <ol style="list-style-type: none"> a. Disable all connection protocols except SSL 4. Verify the connection was rejected because the web server prohibits SSL connections
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.
	<ol style="list-style-type: none"> 1. Review the connection settings of the web browser for connection re-authentication 2. Set the connection to require re-authentication at least every 24 hours 3. On the User Equipment, connect the web browser to the thin client 4. Ensure the user is authenticated to the web server 5. Remain connected to the server for more than 24 hours 6. Verify the connection requires re-authentication after being connected for 24 hours

B.5 Test Criteria for Carrier Service Integration

Table B-6. 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 mobile devices that provides users with the lowest amount of network latency that is cost effective
	<ol style="list-style-type: none"> 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
	<ol style="list-style-type: none"> 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
	<ol style="list-style-type: none"> 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
	<ol style="list-style-type: none"> 1. Identify all the cryptographic signatures used in the Enterprise Mobility Infrastructure 2. Verify the cryptographic signatures use Suite B compliant cryptosuite
CSI.05	The Enterprise Mobility Infrastructure shall have a documented plan to detect and mitigate rogue base stations
	<ol style="list-style-type: none"> 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.6 Test Criteria for User Equipment Requirements

Table B-7. 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.
	There is no test criterion for this requirement at this time.
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.

Requirement Number	Test Criteria
	<ol style="list-style-type: none"> 1. Configure the User Equipment screen lock password complexity and length to meet applicable security documentation requirements 2. 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	<p>The User Equipment screen lock shall be configured to lock in accordance with applicable DoD or using agency guidance of automatic lock after a configurable amount of time and a configurable number of incorrect attempts.</p> <ol style="list-style-type: none"> 1. Configure the User Equipment to lock the screen after a set amount of time that meets applicable security documentation requirements 2. Configure the User Equipment to lock the device after a set number of incorrect password entries that meets applicable security documentation requirements 3. Break the User Equipment's screen lock and then allow the screen to lock after a period of inactivity 4. Attempt to break the screen lock with an incorrect password 5. Repeatedly attempt to break the screen lock with an incorrect password until the device locks the user out due to repeated incorrect password entries 6. Verify automatic screen lock occurs after the configured amount of device inactivity and device lock out occurs after the configured number of password entry failures
UES.04	<p>The User Equipment shall be configured to allow the USB cable to be used only to charge the device.</p> <ol style="list-style-type: none"> 1. Find device's USB driver/service settings 2. Disable USB data connection capability <ol style="list-style-type: none"> 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 connect 5. Connect device to a power source through the USB 6. Verify the device's battery charges
UES.05	<p>The User Equipment shall be configured to disable processing of incoming cellular messaging services.</p> <ol style="list-style-type: none"> 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	<p>The User Equipment shall be configured to disable outgoing cellular messaging services.</p> <ol style="list-style-type: none"> 1. Configure the firmware, operating system or app settings to prevent the User Equipment from processing outgoing cellular messages 2. From the User Equipment attempt to send a text message to another device 3. Verify the device prohibits transmission of the text message

Requirement Number	Test Criteria
UES.07	<p>The User Equipment shall be configured to disable incoming cellular voice calls.</p> <ol style="list-style-type: none"> 1. Configure the firmware, operating system or app settings to prevent the User Equipment from accepting incoming cellular voice calls 2. From a commercial cellular phone, dial the User Equipment phone 3. Verify the device does not accept, process or acknowledge the incoming voice call
UES.08	<p>The User Equipment shall be configured to disable outgoing cellular voice calls.</p> <ol style="list-style-type: none"> 1. Configure the firmware, operating system or app settings to prohibit User Equipment outgoing cellular voice calls 2. Attempt to dial an outgoing cellular voice call to a commercial phone 3. Verify the User Equipment prohibits outgoing cellular voice calls
UES.09	<p>The User Equipment shall be configured to disable dial-up modem or tethering capabilities.</p> <ol style="list-style-type: none"> 1. Configure the firmware, operating system or app settings to disable any modem or other tethering functionality on the User Equipment <ol style="list-style-type: none"> a. Remove dial-up modem drivers and software b. Remove communication device drivers not related to the Enterprise Mobility System connection such as NFC, Bluetooth etc... c. Disable settings 2. Attempt to tether the User Equipment to another device <ol style="list-style-type: none"> a. Using a dial-up modem b. Using a cable c. Using Near-Field Communication (NFC) d. Using Bluetooth e. 802.11 Wi-Fi 3. Verify attempted tethering fails to establish a connection
UES.10	<p>The User Equipment shall be configured to disable Bluetooth.</p> <ol style="list-style-type: none"> 1. Configure the firmware, operating system or app settings to disable the User Equipment's Bluetooth communication capability <ol style="list-style-type: none"> 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	<p>The User Equipment shall be configured to disable Wi-Fi.</p> <ol style="list-style-type: none"> 1. Configure the firmware, operating system or app settings to disable the User Equipment's Wi-Fi communication capability <ol style="list-style-type: none"> 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	<p>The User Equipment shall be configured to disable Auto Answer.</p> <ol style="list-style-type: none"> 1. Configure the firmware, operating system or app settings to disable the User Equipment's auto answer feature 2. Call the User Equipment using another User Equipment 3. Verify the User Equipment does not auto answer the incoming call

Requirement Number	Test Criteria
UES.13	The User Equipment shall be configured to disable Voice Mail.
	<ol style="list-style-type: none"> 1. Configure the firmware, operating system or app settings to disable the User Equipment's voice mail feature <ol style="list-style-type: none"> a. If necessary, call the wireless provider to disable the centralized voice mail feature 2. Call the User Equipment using another User Equipment 3. Verify the User Equipment does not redirect to a voice mail account
UES.14	The User Equipment shall be configured to disable Automatic Redial.
	<ol style="list-style-type: none"> 1. Configure the firmware, operating system or app settings to disable the User Equipment's automatic redial feature 2. Make a call to another User Equipment that is turned off 3. Verify the User Equipment does not attempt to redial the number or prompt for automatic redial
UES.15	The User Equipment shall be configured to disable all GPS and location services except E911.
	<ol style="list-style-type: none"> 1. 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
UES.16	The system shall be configured to disable any feature that will be capable of "Phoning home" or reporting back to a centralized vendor-managed server.
	<ol style="list-style-type: none"> 1. Ensure there are no apps that report back to a centralized vendor-managed server 2. Configure the firmware, operating system or app settings to disable any User Equipment capability for reporting back to a vendor-managed server 3. Verify the User Equipment has no apps or functions for reporting back to a centralized vendor-managed server
UES.17	The User Equipment shall be configured with Over the Air (OTA) updates from the carrier disabled that are not absolutely required for the phone to access the network.
	<ol style="list-style-type: none"> 1. Configure the User Equipment to disable OTA updates not required by the carrier for network access <ol style="list-style-type: none"> a. Disable OTA settings in firmware b. Remove OTA certificates c. Disable/remove the operating system OTA update service 2. Verify OTA update capability not required for carrier network access has been disabled
UES.18	The User Equipment operating system firewall shall be configured according to DoD and local system policy.
	<ol style="list-style-type: none"> 1. Identify DoD and local policies applicable to the system 2. Configure the User Equipment firewall in accordance with the identified policies 3. Verify the firewall is operating as required by identified policies <ol style="list-style-type: none"> a. Firewall is rejecting unnecessary traffic b. Firewall is accepting necessary traffic
UES.19	The User Equipment operating system firewall shall be configured to only allow IPsec traffic.

Requirement Number	Test Criteria
	<ol style="list-style-type: none"> 1. Configure the User Equipment firewall to only allow IPsec traffic <ol style="list-style-type: none"> a. Authentication Header (AH) b. Encapsulating Security Payload (ESP) c. Internet Key Exchange (IKE) 2. Verify the firewall passes IPsec traffic and rejects non-IPsec traffic
UES.20	<p>The Certificate storage password shall be configured for length and complexity in according with DoD or using agency policy on mobile security.</p> <ol style="list-style-type: none"> 1. Configure the User Equipment certificate storage password complexity and length to meet applicable security documentation requirements 2. Set the certificate storage 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.21	<p>The User Equipment shall be configured to receive configuration policies and software updates from authorized remote systems.</p> <ol style="list-style-type: none"> 1. Configure the firmware, operating system or app settings to update the User Equipment with policies and software from authorized sources 2. Ensure the User Equipment contains digital certificates from the authorized sources 3. Create a software update and push to the User Equipment from an unverifiable source <ol style="list-style-type: none"> a. Remove an approved source's digital certificate from the User Equipment b. Create an unapproved source 4. Verify the User Equipment does not accept the update from the unverifiable source 5. Create a software update and push to the User Equipment from an approved source 6. Verify the User Equipment accepts the update
UES.22	<p>The User Equipment screen lock shall be configured to lock in accordance with applicable DoD or using agency guidance of automatic lock after a configurable number of incorrect authentication attempts</p>
	<ol style="list-style-type: none"> 1. Incorrectly authenticate to the User Equipment in excess of the DoD or using agency guidance for automatic lock after incorrect authentication attempts 2. Verify that the User Equipment prevents further attempts for a configurable period of time

User Equipment Monitoring Service Requirements	
UEA.01	The User Equipment Monitoring Service shall classify the insertion or removal of removable media as a Minor Fault.
	<ol style="list-style-type: none"> 1. Identify the media slots on the User Equipment 2. Configure the User Equipment monitoring service to generate a minor fault when media is inserted into any of the media slots 3. Insert media into one of the User Equipment slots 4. Verify a minor fault was generated when the media was inserted into the User Equipment
UEA.02	The transition of the Wi-Fi service from "Disabled" to "Enabled" shall be considered a Major Fault.
	<ol style="list-style-type: none"> 1. Ensure the Wi-Fi service is disabled 2. Configure the User Equipment monitoring service to generate a major fault if the Wi-Fi service is enabled 3. Enable the Wi-Fi service <ol style="list-style-type: none"> a. Log on as administrator as necessary 4. Verify a major fault was generated when the Wi-Fi service was enabled
UEA.03	The transition of the Bluetooth service from "Disabled" to "Enabled" shall be considered a Major Fault.
	<ol style="list-style-type: none"> 1. Ensure the Bluetooth service is disabled 2. Configure the User Equipment monitoring service to generate a major fault if the Bluetooth service is enabled 3. Enable the Bluetooth service <ol style="list-style-type: none"> a. Log on as administrator as necessary 4. Verify a major fault was generated when the Bluetooth service was enabled
UEA.04	The detection of a USB data connection shall be considered a Major Fault.
	<ol style="list-style-type: none"> 1. Determine the User Equipment's USB data capabilities <ol style="list-style-type: none"> a. Disabled b. Configured for data transfer c. Configured for User Equipment charging d. Drivers present 2. Configure the User Equipment monitoring service to generate a major fault if a USB data connection is established 3. Enable USB data transfer <ol style="list-style-type: none"> a. Install necessary drivers b. Enable USB data service c. Attach a USB cable to the User Equipment and another computer 4. Verify a major fault was generated when the USB data connection was established
UEA.05	The dialing of '911' shall be considered a Major Fault.

	<ol style="list-style-type: none"> 1. Configure the User Equipment monitoring service to generate a major fault if '911' is dialed 2. Calling '911' is not appropriate for testing purposes without contacting the non-emergency number first and informing them of the date/time of a communication equipment check. <ol style="list-style-type: none"> a. Call non-emergency number for local police, fire, rescue b. Inform them of a pending communication equipment check c. Configure the User Equipment monitoring service to generate a major fault if '911' is dialed d. Dial '911' e. Verify a major fault was generated when '911' was dialed
UEA.06	The User Equipment Monitoring Service shall classify detection of the starting or discovery of unauthorized process detections as a Minor Fault unless explicitly defined as a Major Fault
	<ol style="list-style-type: none"> 1. Load an unapproved app onto the User Equipment 2. Configure the User Equipment monitoring service to generate a minor fault (major fault if so defined) if an unauthorized process is executed 3. Launch the unapproved app 4. Verify the appropriate fault was generated when the unapproved app was executed
UEA.07	The User Equipment Monitoring Service shall classify unauthorized file system changes as a Minor Fault.
	<ol style="list-style-type: none"> 1. Configure the User Equipment monitoring service to generate a minor fault if an unauthorized change occurs to the file system 2. Alter a system file <ol style="list-style-type: none"> a. Delete a system file b. Add a file to a system directory c. Alter a system file 3. Verify a minor fault was generated when an unauthorized file system change occurs
UEA.08	The User Equipment Monitoring Service shall be configured to visually notify the user upon detection of a Major or Minor Fault.
	<ol style="list-style-type: none"> 1. Configure the User Equipment monitoring service to display a notification on the User Equipment screen when a major or a minor fault occurs 2. Cause a major or minor fault on the User Equipment 3. Verify a visual notification was displayed on the EU's display stating a fault has occurred
UEA.09	The User Equipment Monitoring Service shall be configured to vibrate to alert the user upon detection of a Major Fault.
	<ol style="list-style-type: none"> 1. Configure the User Equipment monitoring service to produce a vibratory alert 2. Cause a major fault on the User Equipment 3. Verify the User Equipment vibrated as an alert that a major fault occurred
UEA.10	The User Equipment Monitoring Service shall remove any files containing encrypted or decrypted certificates or key material upon detection of a Major Fault.

	<ol style="list-style-type: none"> 1. Identify on the User Equipment the storage locations of certificate and key material <ol style="list-style-type: none"> a. Unencrypted or encrypted 2. Configure the User Equipment to erase all certificates and keys when a major fault occurs 3. Cause a major fault on the User Equipment 4. Verify the certificates and keys were wiped when the major fault occurred
UEA.11	The User Equipment Monitoring Service shall terminate any encryption utility upon detection of a Major Fault.
	<ol style="list-style-type: none"> 1. Identify encryption utilities on the User Equipment 2. Configure the User Equipment to terminate any encryption utility when a major fault occurs 3. Launch an encryption utility on the User Equipment 4. Cause a major fault on the User Equipment 5. Verify the encryption utility was terminated when the major fault occurred
UEA.12	The User Equipment Monitoring Service shall terminate any VPN client process upon detection of a Major Fault.
	<ol style="list-style-type: none"> 1. Configure the User Equipment to terminate any VPN connections when a major fault occurs 2. Connect the User Equipment to the Enterprise Mobility System SIP Server through a VPN tunnel 3. Cause a major fault on the User Equipment 4. Verify that VPN tunnel was disconnected when the major fault occurred
UEA.13	The User Equipment Monitoring Service shall allow standard phone calls upon detection of a Major Fault.
	<ol style="list-style-type: none"> 1. Cause a major fault on the User Equipment 2. Verify the User Equipment can make standard phone calls after a major fault by calling the Mobility help desk commercial number to test the ability to make standard calls.
UEA.14	The User Equipment Monitoring Service shall be configured to notify the user of Major and Minor Faults.
	<ol style="list-style-type: none"> 1. Identify what events are defined as major and minor faults 2. Configure the User Equipment monitoring service to generate a notification when a major or minor fault occurs 3. Cause a major and a minor fault to occur on the User Equipment Verify that each fault generates an appropriate user notification
UEA.15	The User Equipment Monitoring Service shall be configured to log Major and Minor Faults.
	<ol style="list-style-type: none"> 1. Identify what events are defined as major and minor faults 2. Configure the User Equipment monitoring service to log the occurrence of major and minor faults 3. Cause a major and a minor fault to occur on the User Equipment Review the audit log and verify that each fault generates an appropriate log entry
UEA.16	The User Equipment Monitoring Service shall block standard phone calls.
	<ol style="list-style-type: none"> 1. Call a commercial number 4. Verify the phone blocks the number

B.7 Test Criteria for Infrastructure Requirements

Table B-8. 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).
	<ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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.
	<ol style="list-style-type: none"> 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.
	<ol style="list-style-type: none"> 1. Identify the network firewall platforms in the Enterprise Mobility Infrastructure Identify applicable DoD or using agency policy and guidance 2. Review the firewall configurations 3. 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.
	<ol style="list-style-type: none"> 1. Identify to where each host system reports <ol style="list-style-type: none"> a. Ensure each host generates a report 2. Identify applicable DoD or using agency policy and guidance 3. Review the host reports <ol style="list-style-type: none"> a. What is reported b. Report frequency c. Report format d. Classification markings 4. Verify the reports meet 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.

Requirement Number	Test Criteria
	<ol style="list-style-type: none"> 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 a 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.
	<ol style="list-style-type: none"> 1. On an Infrastructure Host System, log in using valid user credentials 2. 3. Log out of the account 4. Suspend user account access 5. Attempt to log back in with now suspended account credentials 6. Verify user log on is rejected
IFH.04	An Infrastructure Host System shall maintain separation of user roles.
	<ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> a. System admin actions b. Webpage access c. Command line execution 4. Verify the user receives 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.
	<ol style="list-style-type: none"> 1. Identify the host systems on the Enterprise Mobility Infrastructure 2. Configure the host systems to audit user actions <ol style="list-style-type: none"> a. Follow applicable DoD or using agency policy and guidance for what actions are auditable 3. Log onto the host system <ol style="list-style-type: none"> 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.

Requirement Number	Test Criteria
	<ol style="list-style-type: none"> 1. On the host system, identify the anti-malware service <ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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	<p>An Infrastructure Host System shall have a host-based firewall installed and configured in accordance with applicable DoD or using agency policy and guidance.</p>
	<ol style="list-style-type: none"> 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	<p>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.</p>
	<ol style="list-style-type: none"> 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 the IDS/IPS will detect 4. Review the IDS/IPS report 5. Verify the IDS/IPS reported the incident and that the IDS/IPS is configured in accordance with applicable DoD or using agency policy and guidance
IFH.09	<p>An Infrastructure Host System shall verify the integrity of its software environment.</p>
	<ol style="list-style-type: none"> 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	<p>An Infrastructure Host System shall implement hardware roots of trust for performing integrity verification and reporting (attestation).</p>
	<p>There is no test criteria for this requirement at this time.</p>

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.
	<ol style="list-style-type: none"> 1. Identify Enterprise Mobility Infrastructure Host Security Manager for antivirus distribution 2. Configure the Host Security Manager to automatically update network clients <ol style="list-style-type: none"> 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. 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.
	<ol style="list-style-type: none"> 1. Download an approved and unapproved software package to the Enterprise Mobility Infrastructure Management Services system <ol style="list-style-type: none"> 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.
	<ol style="list-style-type: none"> 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.

	<ol style="list-style-type: none"> 1. Identify Enterprise Mobility Infrastructure Host Security Manager for IDS/IPS signature distribution 2. Configure the Host Security Manager to automatically update network clients <ol style="list-style-type: none"> 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. Verify the clients were automatically updated with the most recent signatures
IFM.05	<p>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.</p> <ol style="list-style-type: none"> 1. Identify Enterprise Mobility Infrastructure Host Security Manager for firewall policy distribution 2. Configure the Host Security Manager to automatically update network clients <ol style="list-style-type: none"> 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 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. Verify the clients were automatically updated with the most recent policy
IFM.06	<p>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.</p> <ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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. Verify the network-based firewall components were automatically updated with the most recent policy
IFM.07	<p>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.</p>

	<ol style="list-style-type: none"> 1. Acquire virus and IDS/IPS signature update packages from an approved source <ol style="list-style-type: none"> 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.
	<ol style="list-style-type: none"> 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 function 6. Verify the monitoring report reflects the state and operation of the monitored 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.
	<ol style="list-style-type: none"> 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. Identify 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.
	<ol style="list-style-type: none"> 1. Identify all the Enterprise Mobility Infrastructure Management Services 2. Review the Management Services configuration and operation 3. Verify Management Services is configured in accordance with applicable DoD or using agency policy and guidance.
Enterprise Mobility Infrastructure Security Services Requirements	
IFS.01	The Enterprise Mobility Infrastructure Security Services shall record audit events reported by infrastructure components.
	<ol style="list-style-type: none"> 1. Identify the Enterprise Mobility Infrastructure Security Services system 2. Review the audit logs on the system for audit reports from the infrastructure components 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.
	<ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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.
	<ol style="list-style-type: none"> 1. Identify the Enterprise Mobility Infrastructure Security Services system audit records 2. Attempt to modify the records <ol style="list-style-type: none"> a. Delete records b. Alter records c. Add records 3. Verify actions taken to modify records require administrative privileges <ol style="list-style-type: none"> a. Records are digitally signed b. Records are read only for unprivileged users
IFS.04	The Enterprise Mobility Infrastructure Security Services shall support Windows Domain authentication if the infrastructure includes components running Microsoft Windows.
	<ol style="list-style-type: none"> 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.
	<ol style="list-style-type: none"> 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 RADIUS authentication if required by the system design (e.g., to support the SIP Service).
	<ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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 userid and password.
	<ol style="list-style-type: none"> 1. Log into an Enterprise Mobility Infrastructure component 2. Verify the logon requires a unique userid and password
IFS.08	The Enterprise Mobility Infrastructure Security Services shall authorize access by an authenticated user based on a black- or white-list.

	<ol style="list-style-type: none"> 1. Identify Enterprise Mobility Infrastructure authorization services <ol style="list-style-type: none"> a. Logon authorization b. Service authorization (HTTP, FTP, Email, group etc...) 2. Identify a test user and remove authorization to some service for that user <ol style="list-style-type: none"> 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.
	<ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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.
	<ol style="list-style-type: none"> 1. Configure the Enterprise Mobility Infrastructure Security Services to log successful authentication and authorization activities as specified in applicable DoD or using agency guidance <ol style="list-style-type: none"> a. Include network (system) logon success as an auditable activity 2. Perform actions on the network (system) that result in authentication and authorization successes <ol style="list-style-type: none"> a. Logon to the network (system) with valid credentials b. Access a service to which the user is authorized and successful access is logged 4. 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.
	<ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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.
	<ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> a. Ensure logon is to the Domain and not local 4. Verify successful authentication to the domain using directory services <ol style="list-style-type: none"> 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.
	<ol style="list-style-type: none"> 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.
	<ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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.
	<ol style="list-style-type: none"> 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
IFA.05	The Enterprise Mobility Infrastructure shall require authentication and authorization of users to stop, start, or change configuration for servers or services.
	<ol style="list-style-type: none"> 1. Configure Enterprise Mobility Infrastructure Servers to require authentication and authorization to change configurations or services 2. Logon to an Enterprise Mobility Infrastructure Server as a non-administrative, unauthorized user 3. Attempt to alter configuration files and services <ol style="list-style-type: none"> a. Delete configuration file b. Modify configuration file c. Turn off the auditing service d. Change the time 4. Verify attempt to alter configuration files and services 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.

	<ol style="list-style-type: none"> 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.
	<ol style="list-style-type: none"> 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.
	<ol style="list-style-type: none"> 1. Identify the Enterprise Mobility Infrastructure Server implementing certificate validation services 2. Identify what the certificate validation service is <ol style="list-style-type: none"> 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.
	<ol style="list-style-type: none"> 1. Identify the DNS Servers on the Enterprise Mobility Infrastructure network 2. Ensure infrastructure components are configured to use the local DNS Servers 3. On an infrastructure component, perform a DNS lookup command 4. Verify the results are from the local DNS Server
IFN.02	The Enterprise Mobility Infrastructure shall provide Network Time Servers that provide time synchronization within the infrastructure networks.
	<ol style="list-style-type: none"> 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.

	<ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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 unauthorized user
IFN.04	The Enterprise Mobility Infrastructure Directory Services shall be configured to require user authentication and authorization to read directory entries or attributes.
	<ol style="list-style-type: none"> 1. Configure Enterprise Mobility Infrastructure directory servers to require authentication and authorization to view entries or attributes 2. Logon to an Enterprise Mobility Infrastructure directory server as an unprivileged user 3. Attempt to view directory service entries or attributes 4. Verify attempt to view directory service entries and attributes failed for an unauthorized user
IFN.05	The Enterprise Mobility Infrastructure Directory Services shall be configured to allow storage of X.509 certificates.
	<ol style="list-style-type: none"> 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 certificate services resident on the server
IFN.06	The Enterprise Mobility Infrastructure Directory Services shall be configured to allow storage of X.509 CRLs.
	<ol style="list-style-type: none"> 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 certificate 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.
	<ol style="list-style-type: none"> 1. Same as IFA.05

B.8 Test Criteria for PKI Requirements

Table B-9. PKI Test Criteria

Requirement Number	Test Criteria
	Certificate, Key, and Trust Management
ECA.01	The Certificate Authority cryptomodule shall be FIPS 140-2 compliant.
	<ol style="list-style-type: none"> 1. Identify the Certificate Authority service and its documentation 2. Review the documentation in regards to FIPS 140-2 cryptographic algorithm compliance 3. Verify the Certificate Authority's cryptographic algorithms are designated FIPS 140-2 compliant

Requirement Number	Test Criteria
ECA.02	<p>A Certificate Authority service shall be configured to generate user certificates.</p> <ol style="list-style-type: none"> 1. On the certificate authority, create a user certificate 2. Verify the generated user certificate is of the required format and version
ECA.03	<p>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 for user certificates.</p> <ol style="list-style-type: none"> 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	<p>The Certificate Authority service shall maintain a data store of all certificates it has issued including date of issuance and current status.</p> <ol style="list-style-type: none"> 1. Identify the Certificate Authority Server 2. Review the server certificate store 3. Create a user certificate and place in the certificate store 4. Find the newly created certificate and review its properties 5. Verify the certificate properties contain the date of issuance and current status
ECA.05	<p>The Certificate Authority service shall maintain a Certificate Revocation List (CRL).</p> <ol style="list-style-type: none"> 1. Identify the Certificate Authority Server 2. Identify the CRL on the server <ol style="list-style-type: none"> a. If a CRL does not exist create one 3. Verify the Certificate Authority maintains CRLs
ECA.06	<p>The Certificate Authority service shall process certificate revocation requests.</p> <ol style="list-style-type: none"> 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
ECA.07	<p>The Certificate Authority service shall be configured to process PKCS #7 and #10 messages.</p> <ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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	<p>The Certificate Authority shall be capable of generating certificates for the digital signature algorithms as defined in CNSSP-15, Annexes B and C.</p>

Requirement Number	Test Criteria
	<ol style="list-style-type: none"> 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
Enrollment Workstation Requirements	
EWS.01	The Enrollment Workstation shall be able to accept entry of requests for device certificates.
	<ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> a. Format b. Cryptographic strength c. 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.
	<ol style="list-style-type: none"> 1. Configure the Enrollment Workstation to create certificates with a PIN, passphrase, or password that meet applicable complexity policies 2. On the 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.
	<ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> a. Format b. Cryptographic strength c. Identification
EWS.04	The Enrollment Workstation shall be able to interface to non-secure removable media.

Requirement Number	Test Criteria
	<ol style="list-style-type: none"> 1. Identify the Enrollment Workstation and its removable media drives 2. Insert a removable media disk into the appropriate Enrollment Workstation drive 3. Navigate to the removable media's path 4. Transfer a file to the removable media <ol style="list-style-type: none"> d. 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.
	<ol style="list-style-type: none"> 1. Identify the Enrollment Workstation Server 2. Identify the algorithms in CNSSP-15 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 1. Verify the 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.
	<ol style="list-style-type: none"> 1. Identify the Enrollment Workstation Server 2. Identify the algorithms in CNSSP-15 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 digital signature algorithm and key strength meet the requirements as specified in CNSSP-15, Annex B

B.9 Test Criteria for User Equipment Provisioning Requirements

Table B-10. Provisioning Test Criteria

Requirement Number	Test Criteria
	User Equipment Provisioning Requirements
UEP.01	<p>During provisioning any applications, processes, and files that are not essential for operation of the User Equipment shall be removed.</p> <ol style="list-style-type: none"> 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.

Requirement Number	Test Criteria
	<ol style="list-style-type: none"> 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	<p>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.</p> <ol style="list-style-type: none"> 1. On the User Equipment, obtain administrative permissions 2. Navigate to the global setting for clearing the contents of the cache 3. Clear the contents of the cache 4. Verify the contents of the cache were cleared
UEP.04	<p>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.</p> <ol style="list-style-type: none"> 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 CP. Each requirement is intended to be testable, resulting in a yes/no answer of whether the requirement was met.

Table C-1. Requirement Designators

Designator	Requirements Addressed
FMOB	Overarching Mobility requirements that an solution fielded using this CP should implement (F unctional M OBility)
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 S VoIP 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 S VoIP)
FSVS	Requirements for SVoIP Server (F unctional S VoIP S erver)
FUEA	Requirements the 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 S martphone)
FVPC	Requirements applicable to the VPN client running on the User Equipment (F unctional V PN C lient)
FVPG	Requirements applicable to the VPN Gateway (F unctional V PN G ateway)
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 V PN)

Designator	Requirements Addressed
FWNC	<u>W</u> eb Arbitrated <u>N</u> on-Resident Data User Equipment <u>C</u> lient requirements
FWND	<u>W</u> eb Arbitrated <u>N</u> on-Resident <u>D</u> ata
FWNS	<u>W</u> eb Arbitrated <u>N</u> on-Resident Data <u>S</u> erver requirements

C.1 Overarching Mobility Requirements

Table C-2. 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

C.2 VPN Requirements

Table C-3. 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
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	<i>Withdrawn, version 2.1</i>	
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, blacklists, or 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	<i>Withdrawn, version 2.1</i>	
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	The VPN Gateway shall be interoperable with applicable existing Public Key Infrastructures (PKIs) for the installation of root key certificates (trust anchors)	O
FVPG.13	The VPN Gateway shall be interoperable with the applicable existing Public Key Infrastructures (PKIs) for checking certificate validity.	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 C-4. 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

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE
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
FSVP.07	The Enterprise Mobility System and User Equipment client shall implement the Session Description Protocol (SDP) Security Descriptions for Media Streams Protocol (SDS) 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	The SIP Server shall provide a SIP Redirect Service.	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

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE
FSVS.11	For communication between User Equipment and a device operating at a classification level lower than the highest classification level of the User Equipment, the Mobility SIP Server and Secure Voice Gateway shall use public key cryptography to mutually authenticate.	O
FSVS.12	For communication between User Equipment and a device operating at a classification level lower than the highest classification level of the User Equipment, the Mobility SIP Server and Secure Voice Gateway shall negotiate AES keys to protect the confidentiality and integrity of TLS traffic.	O
FSVS.13	For communication between User Equipment and a device operating at a classification level lower than the highest classification level of the User Equipment, 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
FSVS.14	For communication between User Equipment and a device operating at a classification level lower than the highest classification level of the User Equipment, 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 mobile device, in order to establish the TLS channel for SIP messages.	T=O

C.4 Web Based Non-Resident Data Requirements

Table C-5. 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 for a limited period of time (at most 24 hours) before requiring re-authentication	T=O
FWND.08	The web server shall accept either certificates, user credentials, or a combination for authentication	T=O

C.5 User Equipment Requirements

Table C-6. 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
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	The User Equipment screen lock shall support locking the screen for a configurable amount of time after a configurable number of incorrect attempts.	O
FUES.10	The User Equipment shall provide the capability to disable Bluetooth.	T=O
FUES.11	The User Equipment shall provide the capability to prevent users from enabling Bluetooth.	T=O
FUES.12	The User Equipment shall provide a mechanism to determine if the user has enabled Bluetooth.	T=O
FUES.13	The User Equipment shall provide the capability to disable Wi-Fi.	T=O
FUES.14	The User Equipment shall provide the capability to prevent users from enabling Wi-Fi.	T=O
FUES.15	The User Equipment shall provide a mechanism to determine if the user has enabled Wi-Fi.	T=O
FUES.16	The User Equipment shall provide the capability to disable Auto Answer.	T=O

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE
FUES.17	The User Equipment shall provide the capability to prevent users from enabling Auto Answer.	T=0
FUES.18	The User Equipment shall provide the capability to disable Voice Mail.	T=0
FUES.19	The User Equipment shall provide the capability to prevent users from enabling Voice Mail.	T=0
FUES.20	The User Equipment shall provide the capability to disable Automatic Redial.	T=0
FUES.21	The User Equipment shall provide the capability to prevent users from enabling Automatic Redial.	T=0
FUES.22	The User Equipment shall provide the capability to disable all transmitting GPS and location services except E911 or as authorized by using agency's DAO.	T=0
FUES.23	The User Equipment shall provide the capability to prevent users from enabling transmitting GPS and Location Services.	T=0
FUES.24	The User Equipment shall provide the capability to disable processing of incoming cellular messaging services.	T=0
FUES.25	The User Equipment shall provide the capability to prevent users from enabling incoming cellular messaging services.	T=0
FUES.26	The User Equipment shall provide the capability to disable outgoing cellular messaging services.	T=0
FUES.27	The User Equipment shall provide the capability to prevent users from enabling outgoing cellular messaging services.	T=0
FUES.28	The User Equipment shall provide a mechanism to determine if the user has enabled incoming or outgoing cellular messaging services.	T=0
FUES.29	The User Equipment shall provide the capability to disable incoming cellular voice calls.	T=0
FUES.30	The User Equipment shall provide the capability to prevent users from enabling incoming cellular voice calls.	T=0
FUES.31	The User Equipment shall provide the capability to disable outgoing cellular voice calls.	T=0
FUES.32	The User Equipment shall provide the capability to prevent users from enabling outgoing calls.	T=0
FUES.33	The User Equipment shall provide a mechanism to determine if the user has enabled incoming or outgoing cellular voice calls.	T=0
FUES.34	The User Equipment shall provide the capability to disable dial-up modem or tethering capabilities.	T=0
FUES.35	The User Equipment shall provide the capability to prevent users from enabling dial-up modem or tethering capabilities.	T=0
FUES.36	The User Equipment shall provide a mechanism to determine if the user has enabled dial-up modem or tethering capabilities.	T=0
FUES.37	The User Equipment shall provide the capability to allow the USB cable to be used only to charge the device.	T=0
FUES.38	The User Equipment shall allow for Over the Air (OTA) updates from the carrier to be disabled.	T=0

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE
FUES.39	The User Equipment screen lock password shall have the capability to be configured for length and complexity.	T=O
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	The User Equipment shall support administration and user roles with separate authentication and privileges.	O
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 have a firewall capability.	O
FUES.51	The User Equipment shall be able to receive configuration policies and software updates from authorized remote systems.	O
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, 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

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE
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
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	The User Equipment Monitoring Service shall have the ability to block any outgoing phone calls other than to 911 or equivalent services 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

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE
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 C-7. 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 C-8. PKI Requirements

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE
FECA.00	Certificate, Key, and Trust Management	
FECA.01	The Certificate Authority service shall be able to generate X.509v3 format certificates.	T=O
FECA.02	The Certificate Authority service shall be able to process PKCS #7 and #10 messages.	T=O
FECA.03	A Certificate Authority service shall be able to generate device certificates.	T=O
FECA.04	A Certificate Authority service shall be able to accept a common specified field (e.g., International Mobile Equipment Identity, IMEI) as part of the Distinguished Name for device certificates.	T=O
FEWS.00	Enrollment Work Station Requirements	
FEWS.01	The Enrollment Workstation shall be able to load a certificate on to removable media.	T=O

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE
FEWS.02	The Enrollment Workstation shall be able to interface to a removable security module.	O
FEWS.03	The Enrollment Workstation shall be able to accept entry of requests for device certificates.	T=O

C.8 Provisioning Requirements

Table C-9. Provisioning Requirements

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE
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

Requirement Number	REQUIREMENT DESCRIPTION	THRESHOLD/ OBJECTIVE
FUEP.16	The Device Provisioning Workstation shall accept inputs from removable media and devices as input to the registration data store.	0
FUEP.17	The Device Provisioning Workstation shall accept requests for device registration information.	T=0
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=0
FUEP.19	The Device Provisioning Workstation shall have the ability to load device configuration and policy information onto the device.	T=0