National Security Agency/
Central Security Service

CYBERSECURITY SOLUTIONS

MOBILE ACCESS CAPABILITY PACKAGE V2.1

This Commercial Solutions for Classified (CSfC) Capability Package (CP) describes how to protect classified data (including Voice and Video) in Mobile Access Solutions transiting Wired Networks, Domestic Cellular Networks, and Wireless Networks to include Government Private Cellular Networks and Government Private Wi-Fi networks.

Version 2.1
26 June 2018

Mobile Access Capability Package

CHANGE HISTORY

Title	Version	Date	Change Summary
Commercial Solutions for Classified (CSfC) Mobile Access (MA) Capability Package (CP) release for Public Comment	0.8	November 3, 2014	• Initial release of CSfC MA guidance for public comment. • Incorporates End User Device (EUD) Solution Designs from VPN version 3.0 CP. • Incorporates content from Mobile Security Guide version 2.3.
CSfC MA CP	1.0	April 2, 2015	• Removed "Non-MDF Validated" EUD type • Removed EUD design utilizing two VPN Gateways • Removed option to use separate computing platform with VPN Client installed to provide Outer layer of encryption • Changed restrictions on control plane traffic • Added Tactical Solution Implementation Appendix • Added requirements for End User Device • Added requirements for RD
CSfC MA CP	1.1		• Minor update incorporating customer feedback • Corrected language in requirement MA-CR-9 and made consistent with the MA CP Compliance Matrix

Mobile Access Capability Package

Title	Version	Date	Change Summary
CSfC MA CP release for Public Comment	1.8	March 2016	• Added support for Multiple Security Levels • Removed Option to terminate Inner Tunnel in the Red Network • Updated Continuous Monitoring architecture and requirements • Added support for EUDs with Dedicated Outer VPN with wireless connectivity to Computing Device • Relocated Threat Section to associated Risk Assessment document • Update Key Management sections IAW CNSS AM 02-15 • Temporarily removed Test Section; updated Test Section will be introduced in MA CP v 2.0
CSfC MA CP	2.0	November 2017	• Updated based on stakeholder feedback to MA CP v1.8 • Mandated use of Retransmission Device for all black transports except government private wireless and government private cellular • Moved Retransmission Device within CSfC solution boundary • Added objective mandatory access control requirements for EUD policy enforcement • Clarified requirements for EUD connecting to infrastructure supporting multiple security levels • Updated Test Requirements in new MA CP Annex
CSfC MA CP	2.1	June 26, 2018	• Relocated Key Management Requirements from the CP to a separate “Key Management Requirements Annex”. • Updated requirements to use “must” instead of “shall.” • Minor administrative changes were made in formatting. • Defined role of Security Administrator.

TABLE OF CONTENTS

1 Introduction 8
2 Purpose and Use 9
3 Legal Disclaimer 9
4 Description of the Mobile Access Solution 10
4.1 Networks 12
4.1.1 Red Network 12
4.1.2 Gray Network 13
4.1.3 Black Network 14
4.1.4 Data, Management, and Control Plane Traffic 16
4.2 High-Level Design 17
4.2.1 End User Devices 18
4.2.2 Independent Site 21
4.2.3 Multiple Sites 22
4.2.4 Multiple Security Levels 23
4.3 Rationale for Layered Encryption 24
4.4 Authentication 25
4.5 Other Protocols 26
4.6 Availability 26
5 Infrastructure Components 27
5.1 Outer Firewall 27
5.2 Outer VPN Gateway 27
5.3 Gray Firewall 28
5.4 Inner Firewall 29
5.5 Gray Management Services 29
5.5.1 Gray Administration Workstation 30
5.5.2 Gray Security Information and Event Management (SIEM) 30
5.5.3 Gray Authentication Server 31
5.6 Inner Encryption Components 31
5.6.1 Inner VPN Gateway 32

5.6.2 Inner TLS-Protected Server 32
5.6.3 Inner SRTP Endpoint 33
5.7 Red Management Services 33
5.7.1 Red Administration Workstations 34
5.7.2 Red Security Information and Event Management (SIEM) 34
5.8 Public Key Infrastructure Components 35
6 End User Device Components 35
6.1 Outer VPN Component 35
6.1.1 Dedicated Outer VPN 35
6.1.2 Outer VPN Client 36
6.2 VPN EUD 36
6.3 TLS EUD 37
6.3.1 TLS Client 37
6.3.2 SRTP Client 38
7 Mobile Access Configuration and Management 38
7.1 Solution Infrastructure Component Provisioning 38
7.2 EUD Provisioning 39
7.3 Administration of Mobile Access Components 39
7.4 EUDs for Different Classification Domains 41
8 Continuous Monitoring 41
8.1 Monitoring Points 41
8.2 Log Data 43
8.3 Network Flow Data 43
8.4 Change Detection 44
8.5 Collection 44
8.6 Correlation 45
9 Key Management 45
10 Requirements Overview 45
10.1 Capabilities 46
10.2 Threshold and Objective Requirements 47

10.3 Requirements Designators 47
11 Requirements for Selecting Components 48
12 Configuration Requirements 53
12.1 Overall Solution Requirements 53
12.2 Configuration Requirements for All VPN Components 55
12.3 Configuration Requirements For Inner and Outer VPN Components 57
12.4 Inner VPN Components 58
12.5 Outer VPN Components 59
12.6 Multiple Security Level Requirements 61
12.7 TLS-Protected Server & SRTP Endpoint Requirements 62
12.8 Retransmission Device requirements 63
12.9 Wireless Connectivity to Dedicated Outer VPN 65
12.10 End User Devices Requirements 67
12.11 Port Filtering Requirements for Solution Components 73
12.12 Configuration Change Detection Requirements 75
12.13 Device Management Requirements 75
12.14 Continuous Monitoring Requirements 77
12.15 Auditing Requirements 80
12.16 Key Management Requirements 83
12.17 Two Factor Authentication 83
13 Requirements for Solution Operation, Maintenance, and Handling 84
13.1 Requirements for the Use and Handling of Solutions 84
13.2 Requirements for Incident Reporting 87
14 Role-Based Personnel Requirements 89
15 Information to Support The AO 93
15.1 Solution Testing 94
15.2 Risk Assessment 95
15.3 Registration of Solutions 95
Appendix A. Glossary of Terms 96
Appendix B. Acronyms 100

Appendix C. References 103
Appendix D. End User Device Implementation Notes 106
Appendix E. Tactical Solution Implementations 114

TABLE OF FIGURES

Figure 1. Overview of Mobile Access Solution 11
Figure 2. Acceptable Black Transport Networks 15
Figure 3. EUD Solution Designs 19
Figure 4. EUDs Connected to Independent Site 21
Figure 5. Multiple Mobile Access Solution Infrastructures supporting EUDs 22
Figure 6. Mobile Access Solution Supporting Multiple Security Levels 23
Figure 7. Overview of Gray Management Services 30
Figure 8. Overview of Red Management Services 34
Figure 9. Solution Continuous Monitoring Point 42
Figure 10. VPN EUD with Inner VPN Client and Separate Outer VPN Gateway 106
Figure 11. VPN EUD with Inner and Outer VPN Clients in Separate Virtual Machines with Retransmission Device 107
Figure 12. VPN EUD with Inner and Outer VPN Clients in Separate Virtual Machines without Retransmission Device 108
Figure 13. TLS EUD with Separate Outer VPN Gateway 109
Figure 14. TLS EUD with Integrated Outer VPN Client with Retransmission Device 110
Figure 15. TLS EUD with Integrated Outer VPN Client with Retransmission Device 111
Figure 16. Retransmission Device Connectivity 112
Figure 17. Mobile Access Solution Infrastructure Supporting VPN and TLS EUDs 113

LIST OF TABLES

Table 1. Overview of Mobile Access CP Terminology 11
Table 2. Acceptable Black Transport Networks 14
Table 3. Capability Designators 46
Table 4. Requirement Digraphs 47
Table 5. Product Selection Requirements 48
Table 6. Overall Solution Requirements 53

Table 7. Approved Commercial Algorithms (IPsec) for up to Top Secret 55
Table 8. Approved Commercial Algorithms (TLS) for up to Top Secret 56
Table 9. Approved Commercial Algorithms for a Dedicated Outer VPN with Wireless Connectivity 56
Table 10. Approved Commercial Algorithms (SRTP) for up to Top Secret 57
Table 11. Configuration Requirements for Inner and Outer VPN Components 57
Table 12. Inner VPN Components Requirements 58
Table 13. Outer VPN Components Requirements 59
Table 14. Multiple Security Level Requirements 61
Table 15. TLS-Protected Server & SRTP Endpoint Requirements 62
Table 16. Requirements for Retransmission Device 63
Table 17. Requirements for Wireless Connectivity to Dedicated Outer VPN 65
Table 18. Requirements for End User Devices 67
Table 19. Port Filtering Requirements for Solution Components 73
Table 20. Configuration Change Detection Requirements 75
Table 21. Requirements for Device Management 75
Table 22. Continuous Monitoring Requirements 77
Table 23. Auditing Requirements 80
Table 24. Two Factor Authentication Requirements 83
Table 25. Use and Handling of Solutions Requirements 84
Table 26. Incident Reporting Requirements 88
Table 27. Role-Based Personnel Requirements 92
Table 28. Test Requirements 95
Table 29. Tactical Implementation Requirements Overlay 115

1 INTRODUCTION

The Commercial Solutions for Classified (CSfC) Program within the National Security Agency's (NSA) Capabilities Directorate publishes Capability Packages (CPs) to provide configurations that empower NSA customers to implement secure solutions using independent, layered Commercial Off-the-Shelf (COTS) products. The CPs are product-neutral and describe system-level solution frameworks documenting security and configuration requirements for customers and/or Integrators.

The NSA is delivering this CSfC Mobile Access (MA) CP to meet the demand for mobile data in transit solutions (including Voice and Video) using approved cryptographic algorithms and National Information Assurance Partnership (NIAP) evaluated components. These algorithms, known as the Commercial National Security Algorithm (CNSA) suite, are used to protect classified data using layers of COTS products. In MA CP Version 2.1, the Key Management Requirements have been relocated from the CP to a separate Key Management Annex. The MA CP Version 2.0 takes lessons learned from solution support, a testing environment, and a CSfC Initial Solution that implemented secure voice and data capabilities using the CNSA suite, modes of operation, standards, and protocols.

While CSfC encourages industry innovation, trustworthiness of the components is paramount. Customers and their Integrators are advised that modifying a NIAP-validated component in a CSfC solution may invalidate its certification and require a revalidation process. To avoid delays, customers and integrators who feel it is necessary to modify a component should engage the component vendor and consult NIAP through their Assurance Continuity Process (https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/scheme-pub-6.pdf) to determine whether such a modification will affect the component's certification.

In case of a modification to a component, NSA's CSfC Program Management Office (PMO) will require a statement from NIAP that the modification does not alter the certification, or the security of the component. Modifications that will trigger the revalidation process include, but are not limited to: configuring the component in a manner different from its NIAP-validated configuration, and modifying the Original Equipment Manufacturers' (OEMs') code (to include digitally signing the code).

Mobile communication systems (e.g., cellular, Wi-Fi, etc.) are inherently risky. The Mobile Access (MA) Capability Package (CP) Version 2.1 has been developed and approved by the National Manager as a commercial strategy suitable for protecting classified information and National Security Systems (NSS), provided the customer's implementation of the solution is configured, maintained, and monitored as required by the CP. The residual risks for this CP are documented in the MA CP Version 2.0 Risk Assessment. The National Manager is responsible for ensuring that the design documented in the Capability Package is sufficiently robust to protect classified information and NSS. The Government Authorizing Official (AO) assumes the risk for implementing and deploying the solution in accordance with the requirements in the CP. The AO must consider the operational environment and provide appropriate usage guidance to End Users. End Users must understand the risks and adhere to handling

requirements established by the AO for the fielded MACP system. End Users must maintain positive physical control of the End User device. Further, End Users should consider their environment and ensure adequate physical standoff to mitigate threats associated with physical proximity. (Recommend a standoff distance of at least 15 feet.)

2 PURPOSE AND USE

This CP provides high-level reference designs and corresponding configuration requirements that allow customers to select COTS products from the CSfC Components List, available on the CSfC web page (http://www.nsa.gov/resources/everyone/csfc/components-list), for their MA solution and properly configure those products to achieve a level of assurance sufficient for protecting classified data while in transit. As described in Section 11, customers must ensure that the components selected from the CSfC Components List will provide the necessary functionality for the selected capabilities. To successfully implement a solution based on this CP, all Threshold Requirements, or the corresponding Objective Requirements applicable to the selected capabilities, must be implemented, as described in Section 10 and Section 12.

Customers who want to use this CP must register their solution with the NSA. Additional information about the CSfC process is available on the CSfC web page (http://www.nsa.gov/resources/everyone/csfc).

This document will be reviewed twice a year to ensure that the defined capabilities and other instructions still provide the security services and robustness required. Solutions designed according to this CP must be registered with the NSA. Once registered, a signed DNM Approval Letter will be sent validating that the MA solution is registered as a CSfC solution validated to meet the requirements of the latest MA CP and is approved to protect classified information. Any solution designed according to this CP may be used for one year and must then be revalidated against the most recently published version of this CP. Top Secret Solutions will be considered on a case-by-case basis. Customers are encouraged to engage their Client Advocate or the CSfC Program Management Office (PMO) team early in the process to ensure the solutions are properly scoped, vetted, and that the customers have an understanding of risks and available mitigations.

Please provide comments on usability, applicability, and/or shortcomings to your NSA Client Advocate and the MA CP Maintenance Team at Mobile_Access@nsa.gov. MA CP solutions must also comply with the Committee on National Security System (CNSS) Policies and Instructions. Any conflicts identified between this CP and the CNSS or local policy should be provided to the MA CP Maintenance Team.

3 LEGAL DISCLAIMER

This CP 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 must 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 CP, even if advised of the possibility of such damage.

The user of this CP 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 attorney's 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 CP is intended to constitute an endorsement, explicit or implied, by the U.S. Government of any particular manufacturer's product or service.

4 DESCRIPTION OF THE MOBILE ACCESS SOLUTION

This CP describes a general MA solution to protect classified information as it travels across either an untrusted network or a network consisting of multiple classification levels. The solution supports connecting end-user devices (EUDs) to a classified network via two layers of encryption terminated on the EUD provided that the EUD and the network operate at the same security level. The MA solution uses two nested, independent tunnels to protect the confidentiality and integrity of data (including voice and video) as it transits the untrusted network. The MA solution uses Internet Protocol Security (IPsec) as the Outer Tunnel and, depending on the solution design, IPsec or Transport Layer Security (TLS) as the Inner layer of protection.

Throughout this CP, the term "Inner Encryption Component" is used to refer generically to the component (device or software application) that terminates the Inner layer of encryption. An Inner Encryption Component can be a virtual private network (VPN) Component or a TLS Component that is in the infrastructure or part of an EUD. The term "VPN Component" refers generically to both VPN Gateways and VPN Clients in situations where the differences between the two are unimportant. The term "TLS Component" is used to denote a component that implements TLS between the infrastructure (TLS-Protected Server or Secure Real-time Transport Protocol (SRTP) Endpoint) and EUDs (TLS Client or SRTP Client) in accordance with this CP (see Sections 5.6 and 5.8 respectively). There are two EUD solution designs: VPN EUD and TLS EUD. The term "EUD" is used to refer generically to both designs where the differences between them are unimportant. Finally, the term "Dedicated Outer VPN" is used to describe a dedicated piece of hardware that can be part of an EUD and terminates the Outer layer of IPsec encryption.

Table 1. Overview of Mobile Access CP Terminology

Component	VPN EUD	TLS EUD
Inner Encryption Component	IPsec provided by VPN Client	TLS or SRTP provided by TLS-Protected Server, SRTP Endpoint, TLS Client, **OR** SRTP Client
Outer Encryption Component	IPsec provided by Dedicated Outer VPN **OR** VPN Client	IPsec provided by Dedicated Outer VPN **OR** VPN Client

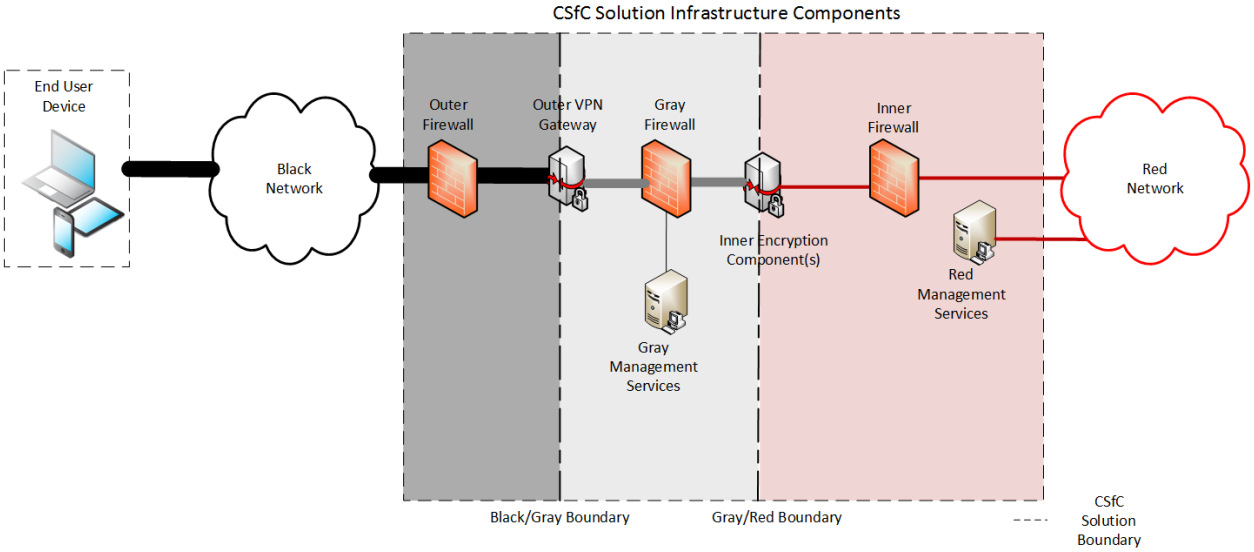

Figure 1. Overview of Mobile Access Solution

As shown in Figure 1, before being sent across the untrusted network, classified data is encrypted twice: first by an Inner Encryption Component, and then by an Outer VPN Component. At the other end of the data flow, the received packet is correspondingly decrypted twice: first by an Outer VPN Component, and then by an Inner Encryption Component.

All Encryption Components are within the CSfC Solution Boundary. The MA CP Version 2.0 no longer allows the use of existing Classified Enterprise Network Encryption Components to provide the Inner layer of protection.

MA solution components are managed using Red Management Services for Inner Encryption Components and Gray Management Services for Outer Encryption Components. The Gray Management Services include an administration workstation, a Gray firewall, a Security Information and Event Monitoring (SIEM) Component, Intrusion Detection System (IDS)/Intrusion Protection System (IPS) and any additional components located between the Outer VPN Gateway and Inner Encryption Components. Gray Management Services may also include a locally run Outer Certification Authority (CA), Certificate

Revocation List (CRL), CRL Distribution Point (CDP), and/or authentication server. The Red Management Services include an administration workstation, an Inner Firewall, and other components within the Red Network. The Red Management Services may also manage a locally run Inner Tunnel CA and, optionally, a locally-run Outer Tunnel CA. In addition, the MA CP allows customers to leverage an existing Enterprise Public Key Infrastructure (PKI) to issue certificates to Outer VPN Components and Inner Encryption Components. To use an existing Enterprise Root CA at least two separate subordinate CAs must be used: one to issue Certificates for Outer VPN Components and the other to issue certificates for Inner Encryption Components.

The EUDs used within the MA CP are form-factor agnostic. They include smart phones, tablets, and laptops. A MA CP EUD can be composed of multiple physical devices (e.g., a Dedicated Outer VPN and a Computing Device) all collectively referred to as the EUD. Although the CP allows flexibility in the selection of the EUD, customers and Integrators must ensure that EUDs meet all applicable requirements for the planned solution design. Section 4.2.1 describes in detail the differences between the VPN EUD and TLS EUD solution design options.

The MA CP instantiations are built using products from the CSfC Components List (see Section 11). Customers who are concerned that their desired products are not yet on the CSfC Components List are encouraged to contact the appropriate vendors and encourage them to sign a Memorandum of Agreement (MoA) with NSA and commence evaluation against a NIAP approved Protection Profile using the CSfC mandated selections which will enable them to be listed on the CSfC Components List. NIAP Certification alone does not guarantee inclusion on the CSfC Components List. Products listed on the CSfC Components List are not guaranteed to be interoperable with all other products on the CSfC Components List. Customers and integrators should perform interoperability testing to ensure the components selected for their MA Solution are interoperable. If you need assistance obtaining vendor POC information, please email csfc_components@nsa.gov.

4.1 Networks

This CP uses the following terminology to describe the various networks that compose a MA solution and the types of traffic present on each: Red, Gray, and Black. The terms Red, Gray, and Black refer to the level of protection applied to the data as described below.

4.1.1 Red Network

Red data consists of unencrypted classified data and a Red Network contains only Red data. Red Networks are under the control of the solution owner or a trusted third party.

The Red Network begins at the internal interface(s) of Inner Encryption Components located between the Gray Firewall and Inner Firewall. EUDs access the Red Network through the two layers of nested encryption described in this CP. For example, an Inner VPN Gateway located between the Gray Firewall and Inner Firewall terminates the Inner layer of IPsec encryption from a VPN EUD. Once a successful

IPsec connection is established, the EUD is given access to classified services such as web, email, Virtual Desktop Infrastructure (VDI), voice, etc.

In some instances, when the MA infrastructure is designed to support TLS EUDs, the TLS-Protected Server or SRTP Endpoint, which terminates the Inner layer of encryption, will implement a TLS-Protected Server that includes both Gray and Red Network interfaces located between the Gray Firewall and Inner Firewall. This TLS-Protected Server terminates the TLS connection from the EUD and acts as a proxy to Red Services located outside of the CSfC Solution Boundary. A similar situation exists for SRTP when using a Voice over Internet Protocol (VoIP) Gateway/Border Controller to terminate the SRTP traffic for an EUD and relaying the data to the Red Network. Since a VoIP Gateway/Border Controller, located between the Gray Firewall and the Inner Firewall, terminates the Inner layer of SRTP desktop phones in the Red Network are not included in the Solution Boundary.

Red Networks may only communicate with an EUD through the MA solution if both operate at the same security level.

4.1.2 GRAY NETWORK

Gray data is classified data that has been encrypted once. Gray Networks are composed of Gray data and Gray Management Services. Gray Networks are under the physical and logical control of the solution owner or a trusted third party.

The Gray Network is physically treated as a classified network even though all classified data is singly encrypted. If a solution owner's classification authority determines that data on a Gray Network is classified, perhaps by determining the Internet Protocol (IP) addresses are classified at some level, then the MA solution described in this CP cannot be implemented, as it is not designed to provide two layers of protection for any classified information on the Gray Network.

Gray Network components consist of the Outer VPN Gateway, Gray Firewall, and Gray Management Services. All Gray Network components are physically protected at the same level as the Red Network components of the MA infrastructure. Gray Management Services are physically connected to the Gray Firewall and include, at a minimum, an administration workstation. The Gray Management Services also includes a SIEM unless the SIEM is implemented in the Red Network in conjunction with a cross domain solution (CDS) (see Section 8). The MA CP requires the management of Gray Network components through the Gray administration workstation. As a result, neither Red nor Black Administration Workstations are permitted to manage the Outer VPN Gateway, Gray Firewall, or Gray Management Services. Additionally, the Gray administration workstation is prohibited from managing Inner Encryption Components. These Inner Encryption Components must be managed from a Red administration workstation.

4.1.3 BLACK NETWORK

A Black Network contains classified data that has been encrypted twice. The network connecting the Outer VPN Components together is a Black Network. Black Networks are not necessarily, and often will not be, under the control of the solution owner and may be operated by an untrusted third party.

The MA CP allows EUDs to operate over any Black Network when used in conjunction with a Government-owned Retransmission Device (RD) or a physically separate Dedicated Outer VPN to establish the Outer IPsec Tunnel.

The government-owned RD is a category of devices that includes Wi-Fi hotspots and mobile routers. On the external side, the RD can be connected to any type of medium (e.g., cellular, Wi-Fi, SATCOM, Ethernet) to gain access to a Wide Area Network. On the internal side, the RD is connected to EUDs either through an Ethernet cable or Wi-Fi. When the RD is a Wi-Fi access point connected to the EUD (or multiple EUDs), the Wi-Fi network must implement Wi-Fi Protected Access II (WPA2) with Pre-Shared Key (PSK). The EUD must be configured to only permit connections to authorized RDs. RDs are only permitted to establish connectivity to the Black Network, and may not be placed between an Outer Encryption Component and Inner Encryption Component.

The CP also allows connectivity without the use of a RD or Dedicated Outer VPN if any of the following transport networks are used: Government Private Cellular Networks or Government Private Wireless Networks. Government Private Cellular Networks are defined as cellular base stations that are owned and operated exclusively by the United States Government (such as in tactical environments). Finally, Government Private Wireless Networks denote Wi-Fi connectivity by a Wireless Local Area Network (WLAN) accredited by an AO. These Wi-Fi networks must comply with applicable organization policies. Within the Department of Defense (DoD) the applicable policy is DoD Instruction (DoDI) 8420.01. At a minimum, these Wi-Fi networks must implement WPA2 with PSK; however, WPA2 with certificate-based authentication is preferred. When Government Private Wireless Networks use certificate-based authentication, they cannot share the Outer Tunnel CA or Inner Tunnel CA certificate Management Services. WPA2 between the RD and EUD protects the Black transport network, but does not count as one of the layers of CSfC data-in-transit encryption.

Table 2. Acceptable Black Transport Networks

	VPN EUD	TLS EUD
Any Black Transport network	Government RD **OR** Dedicated Outer VPN	Government RD **OR** Dedicated Outer VPN
Government Private Cellular or Government Private Wireless	No additional requirements	No additional requirements

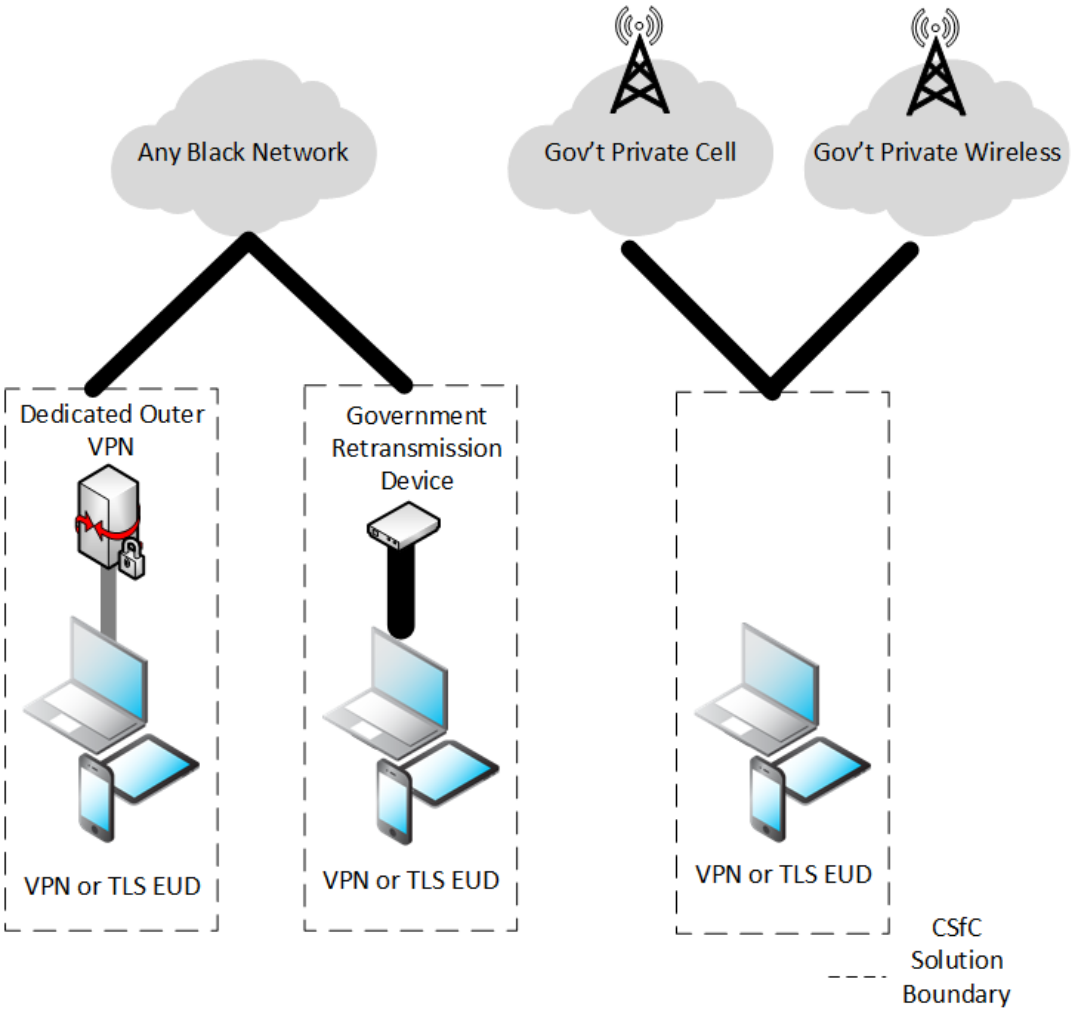

Figure 2. Acceptable Black Transport Networks

As shown in Figure 2, both EUD designs can connect to the MA solution over Government Private Cellular or Government Private Wireless Networks without the need for a separate Dedicated Outer VPN or RD. When connecting over any other black transport network, EUDs must use a Dedicated Outer VPN or a Government RD to connect to the MA solution. When an EUD includes a Dedicated Outer VPN, that VPN is used to establish the Outer layer of IPsec to the government infrastructure and is included within the CSfC Solution Boundary. The Dedicated Outer VPN must be connected to the computing platform utilizing an Ethernet cable or WPA2 (see Section 12.9 and Section 12.10). The computing platform then terminates the Inner layer of encryption. Although only required as described above, a Dedicated Outer VPN can be used to connect to any transport network for any of the EUD solution designs. Similarly, an EUD can use a Government RD to connect to any transport network. The Government RD is part of the CSfC Solution Boundary, and acts as an intermediary between the desired transport network and the

EUD and is to be protected from unauthorized use and tampering. Similar to the Government RD, the Dedicated Outer VPN must be protected from unauthorized use and tampering.

4.1.4 DATA, MANAGEMENT, AND CONTROL PLANE TRAFFIC

Data plane traffic is classified information, encrypted or not, that is being passed through the MA solution. The MA solution exists to encrypt and decrypt data plane traffic. All data plane traffic within the Black Network is encapsulated within an Outer layer of Encapsulating Security Payload (ESP) and either a second layer of ESP or a layer of TLS or SRTP. All data plane traffic within the Gray Network is encapsulated within ESP, TLS, or SRTP. When utilizing a Dedicated Outer VPN with wireless connectivity, Gray data plane traffic between the computing platform and Dedicated Outer VPN is encapsulated within ESP and WPA2.

Management plane traffic is used to configure and monitor solution components. It includes the communications between an Information System Security Officer (ISSO) and a component, as well as the logs and other status information forwarded from a solution component to a SIEM or similar repository. Management plane traffic on Red and Gray Networks must be encapsulated within the Secure Shell (SSH), ESP, or TLS protocol.

Control plane traffic consists of standard protocols necessary for the network to function. Unlike data or management plane traffic, control plane traffic is typically not initiated directly on behalf of a user or an ISSO. Examples of control plane traffic include, but are not limited to, the following:

- Network address configuration (i.e., Dynamic Host Configuration Protocol (DHCP), Neighbor Discovery Protocol (NDP), etc.)
- Address resolution (i.e., Address Resolution Protocol (ARP), NDP, etc.)
- Name resolution (e.g., Domain Name System (DNS))
- Time synchronization (i.e., Network Time Protocol (NTP), Precision Time Protocol (PTP), etc.)
- Route advertisement (i.e., Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), Border Gateway Protocol (BGP), etc.)
- Certificate status distribution (i.e., Online Certificate Status Protocol (OCSP), HTTP download of CRLs, etc.)

The MA CP explicitly prohibits the use of most control plane traffic for EUDs that use a single Computing Device to provide both the Inner and Outer layers of encryption. The MA CP does not allow route advertisement or certificate status distribution to ingress/egress from the Black transport network for these EUDs. As a result, the implementing organization must implement procedures to handle a situation in which the certificate of an Outer VPN Gateway is revoked. EUDs are configured for all IP

traffic to flow through the Outer IPsec VPN Client with the exception of control plane protocols necessary to establish the IPsec tunnel. The control plane necessary to establish the IPsec tunnel is limited to Internet Key Exchange (IKE), address configuration, time synchronization, and in some cases name resolution traffic. EUDs selected from the CSfC Components List use NIAP evaluated configurations to ensure that IP traffic flows through the Outer IPsec VPN Client. Upon establishing the Outer VPN tunnel, the CP does not impose detailed requirements restricting control plane traffic in the Gray and Red Networks.

Restrictions are also placed on control plane traffic for the Outer VPN Gateway. The Outer VPN Gateway is prohibited from implementing routing protocols on external and internal interfaces. The Outer VPN Gateway must rely on the Outer Firewall to implement any dynamic routing protocols.

Except as otherwise specified in this CP, the usage of specific control plane protocols is left to the solution owner to approve. The solution owner must disable or block any unapproved control plane protocols.

Data plane and management plane traffic are generally required to be separated from one another by using physical or cryptographic separation. Use of a Virtual Local Area Network (VLAN) alone is not sufficient to separate data plane and management plane traffic. As a result, a solution may, for example, have a Gray data network and a Gray Management network that are separate from one another, where the components on the Gray Management network are used to manage the components on the Gray data network. The Gray Management network is separated from the Gray data network via the Gray Firewall. The Gray Firewall uses an Access Control List (ACL) to ensure that only appropriate Gray Management Services (i.e., administration workstation, SIEM or Network Time Server) can communicate with the Outer VPN Gateway. The Gray Firewall is also responsible for ensuring that Gray Management Services are only capable of flowing in the appropriate direction. For example, SSH traffic is permitted to initiate from an administration workstation to the Outer VPN Gateway, but not from the Outer VPN Gateway to any Gray Management Services. Conversely, system log data is permitted from the Outer VPN Gateway to the Gray SIEM, but is not permitted from the Gray Management Services to the Outer VPN Gateway. Given that some control plane traffic is necessary for a network to function, there is no general requirement that control plane traffic be similarly separated, unless otherwise specified.

4.2 High-Level Design

The MA solution is adaptable to support multiple capabilities, depending on the needs of the customer implementing the solution. The supported EUD capabilities are mutually exclusive; if a customer chooses to implement an EUD using two layers of IPsec, then the Inner TLS Client would not be included as part of that EUD implementation. Similarly, if a customer only needs a secure voice capability, then the Inner IPsec Component would not be included as part of that EUD implementation. Although the EUD solution designs are mutually exclusive, the infrastructure may be configured to support both EUD solution designs (see Appendix D. End User Device Implementation Notes). This enables

implementation of both types of EUDs based on use cases and device features. Any implementation of the MA solution must satisfy all of the applicable requirements specified in this CP, as explained in Sections 11 and 12.

4.2.1 END USER DEVICES

This CP uses the concept of an EUD, which is either a single Computing Device, such as a smart phone, laptop, or tablet, or the combination of the Computing Device and a Dedicated Outer VPN. The EUD provides two layers of protection for data in transit to tunnel through the Black Network and access classified data on the Red Network. In some instances, an EUD encompasses more than one piece of hardware (e.g., Computing Device and Dedicated Outer VPN) each of which perform a layer of encryption. Where more than one piece of hardware is used, each component is included as part of the EUD and are within the CSfC Solution Boundary. EUDs are dedicated to a single classification level and can only be used to access a Red Network of the same classification. There are two EUD designs which can be implemented as part of a MA solution. Each of the EUD designs share many requirements in common, but also have unique requirements specific to that design:

1) **IPsec-IPsec (VPN EUD):** Uses two IPsec tunnels to connect to the Red Network. Such an EUD includes both an Inner VPN Client and Outer VPN Component to provide the two layers of IPsec. Throughout the document this EUD design is referred to as the "VPN EUD." VPN EUDs can be implemented utilizing combinations of IPsec VPN Clients and IPsec Gateways (see Appendix D. End User Device Implementation Notes). For example, a VPN EUD can be implemented on a Computing Device with two VPN Clients running on separate IP stacks. Similarly, the MA CP allows a VPN EUD to use a Dedicated Outer VPN to provide the Outer layer of IPsec encryption and a VPN Client installed on a Computing Device to provide the Inner layer of encryption.

2) **IPsec-TLS (TLS EUD):** Uses an Outer layer of IPsec encryption and an Inner layer of TLS encryption to access the Red Network. Throughout the document this EUD design is referred to as the "TLS EUD." The Outer layer of encryption can be provided by either an IPsec VPN Client or a Dedicated Outer VPN. The Inner layer of encryption is then provided by a TLS Client. The EUD TLS Client includes a number of different options which can be selected, in accordance with the CP requirements, to meet the operational needs of the customer. The EUD TLS Clients include, but are not limited to, web browsers, email clients, and VoIP applications. Traffic between the TLS EUD Client and the TLS-Protected Server is encrypted with TLS or in some instances SRTP.

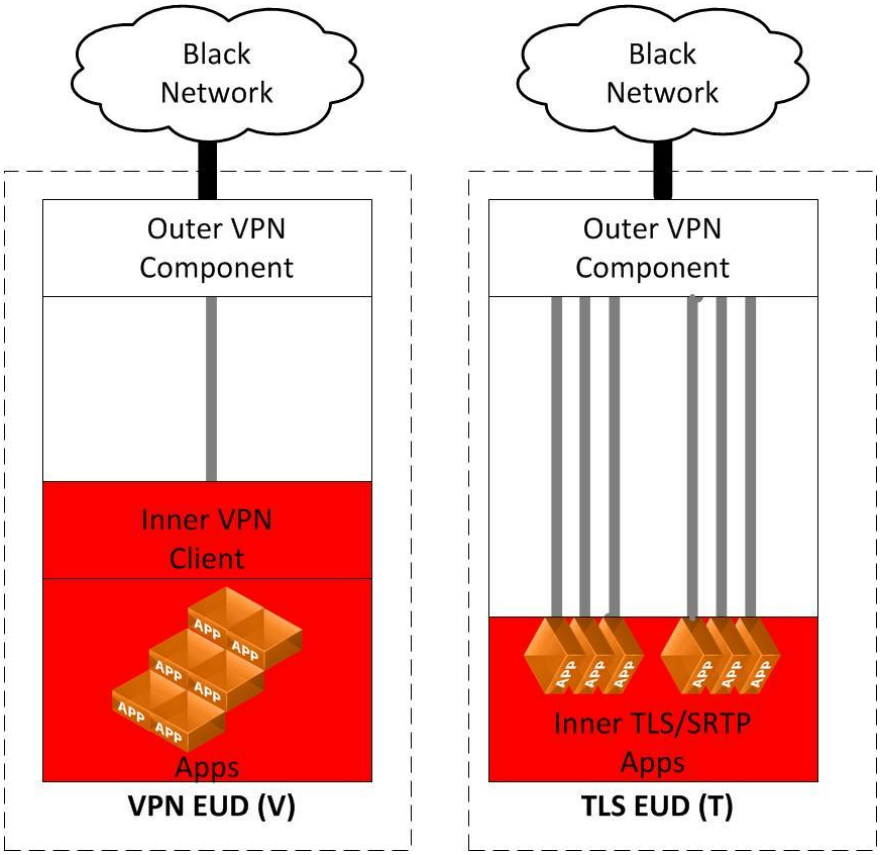

Figure 3. EUD Solution Designs

Figure 3 shows the two EUD solution designs available as part of the MA CP. In each design the Outer VPN Component is used to establish an IPsec tunnel to the Outer VPN Gateway of the MA solution infrastructure. In either EUD design, this Outer VPN Component must be selected from the CSfC Components list and could be either a VPN Client or a Dedicated Outer VPN. If a Dedicated Outer VPN is used to provide the Outer IPsec tunnel, then the computing platform must be connected to the Dedicated Outer VPN utilizing an Ethernet cable or WPA2.

The Inner layer of encryption for VPN EUDs is provided by a VPN Client. The Inner VPN Client must be selected from the CSfC Components List (see Section 11). If VPN Clients are used for both the Inner and Outer layers of encryption then they must use a different IP stack, and are generally implemented using virtualization.

The Inner layer of encryption for TLS EUDs is provided by either TLS or SRTP. Every application that performs TLS or SRTP must be selected from the CSfC Components List.

The MA CP allows three different deployment options pertaining to the use and handling of an EUD while powered off:

1. **EUD with DAR:** To implement Data-at-Rest (DAR) on an EUD, the DAR solution must be approved by NSA – either as compliant and registered with NSA's DAR CP or approved as a tailored solution for the protection of information classified at the level of the Red Network connected to the EUD. Specification of such a DAR solution is outside the scope of this CP, but can be found in the DAR CP. Continuous physical control of the EUD must be maintained at all times.
2. **Classified EUD:** The EUD can only be used when applying physical security measures approved by the AO. EUDs are not subject to special physical handling restrictions beyond those applicable for classified devices as they can rely on the environment they are used within for physical protection. If this design option is selected, then the EUDs must be treated as classified devices at all times. The EUD in this case must enable the native platform DAR protection (e.g., encryption) in order to protect the private keys and other classified information stored on it from disclosure and increase the difficulty of tampering with the software and configuration. Continuous physical control of the EUD must be maintained at all times.
3. **Thin EUD:** The EUD can be designed to prevent any classified information from being saved to any persistent storage media on the EUD. Possible techniques for implementing this include, but are not limited to: using VDI configured not to allow data from the Enterprise/Red Network to be saved on the EUD, restricting the user to a non-persistent virtual machine on the EUD, and/or configuring the EUD's operating system to prevent the user from saving data locally. Since the EUD does not provide secure local storage for classified data, its user is also prohibited by policy from saving classified data to it. The EUD in this case must enable the native platform DAR protection to protect the private keys stored on it from disclosure, and to increase the difficulty of tampering with the software and configuration. This option is not permitted if any of the private keys or certificates stored on the EUD are considered classified by the AO. Continuous physical control of the EUD must be maintained at all times.

While powered on, an EUD is classified at the same level of the connected Red Network, since classified data may be present in volatile memory and/or displayed on screen. To mitigate the risk of accidental disclosure of classified information to unauthorized personnel while the EUD is in use, the customer must define and implement an EUD user agreement that specifies the rules of use for the system. The customer must require that all users accept the user agreement and receive training on how to use and protect their EUD before being granted access. There is no limit to the number of EUDs that may be included in a MA solution.

The intent of a continuous physical control requirement for the MA CP is to prevent potential attacks via brief, undetected physical access of an EUD by a nation state adversary. Since MA CP EUDs by their nature are mobile they are frequently transported and operated outside of physically protected government spaces. As a result customers must maintain continuous physical control of the EUD at all times.

4.2.2 INDEPENDENT SITE

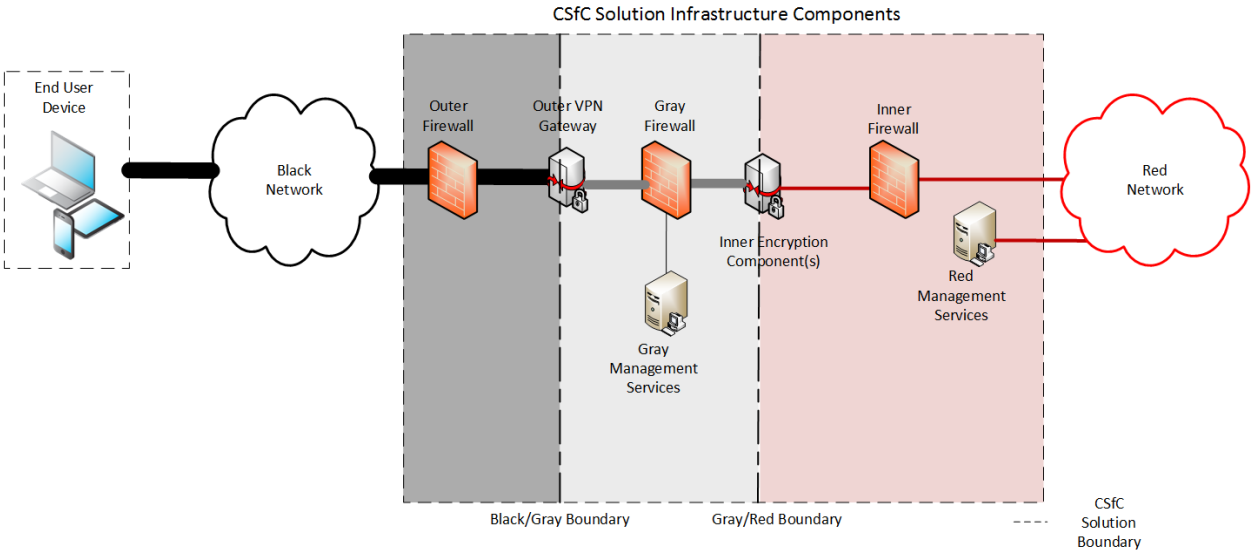

Figure 4. EUDs Connected to Independent Site

Figure 4 shows a single Red Network connected to EUDs that operate at the same security level through the MA solution. Here, the Red Network has at least two Encryption Components associated with it: one or more Inner Encryption Components connected to the Red Network, and an Outer VPN Gateway between the Inner Encryption Components and the Black Network. There are two layers of encryption between any EUD communicating with the Red Network: one IPsec tunnel between their Outer VPN Components, and a second IPsec, TLS or SRTP layer depending on the selected EUD design(s).

For independent sites, administration is performed at that site for all components within the Solution Boundary, including the Outer VPN Gateway, Gray Management Services, Inner Encryption Components, Red Management Services, firewalls, and EUDs. Independent sites are not interconnected with other infrastructure sites through the MA solution; therefore, management, data plane, and control plane traffic between solution infrastructure sites are outside the scope of the MA CP. If two or more sites must be interconnected, customers may also register the MA solution against the VPN CP or use a NSA-Certified encryptor.

Note that while Figure 4 shows only a single EUD, this solution does not limit the number of EUDs being implemented.

4.2.3 MULTIPLE SITES

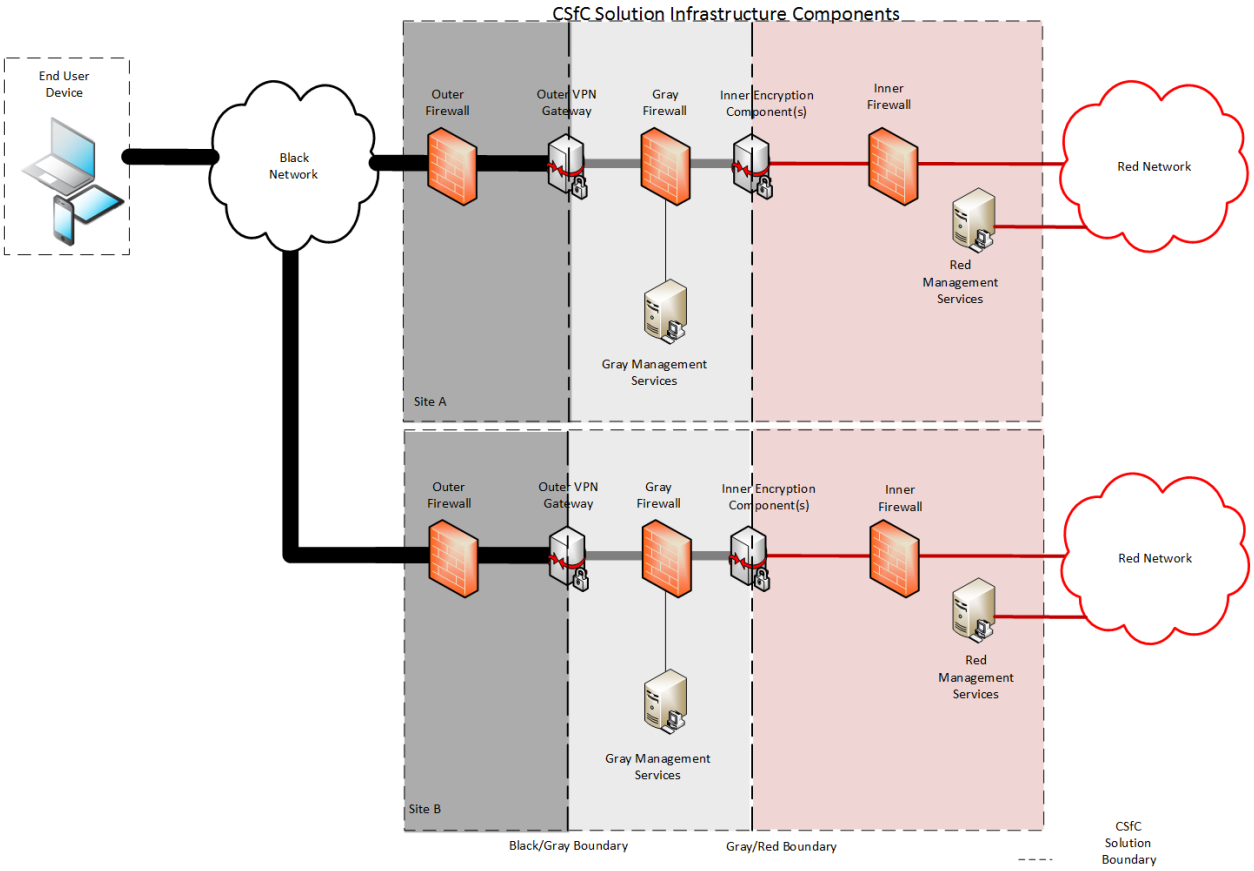

Figure 5. Multiple Mobile Access Solution Infrastructures supporting EUDs

Figure 5 shows two MA solution infrastructures that an EUD can connect to in order to access different Red Network services. Customers may want to implement multiple solution infrastructures to support Continuity of Operations or provide better performance based on geographic location of EUDs or Red services. The multiple solution infrastructures may be interconnected using a NSA-approved solution such as the VPN CP or a NSA-Certified encryptor; however, connectivity of Solution Infrastructure Components is outside the scope of the MA CP.

Note that while Figure 5 shows only two sites, this solution can scale to include numerous sites, with each additional site having the same design as those in Figure 5.

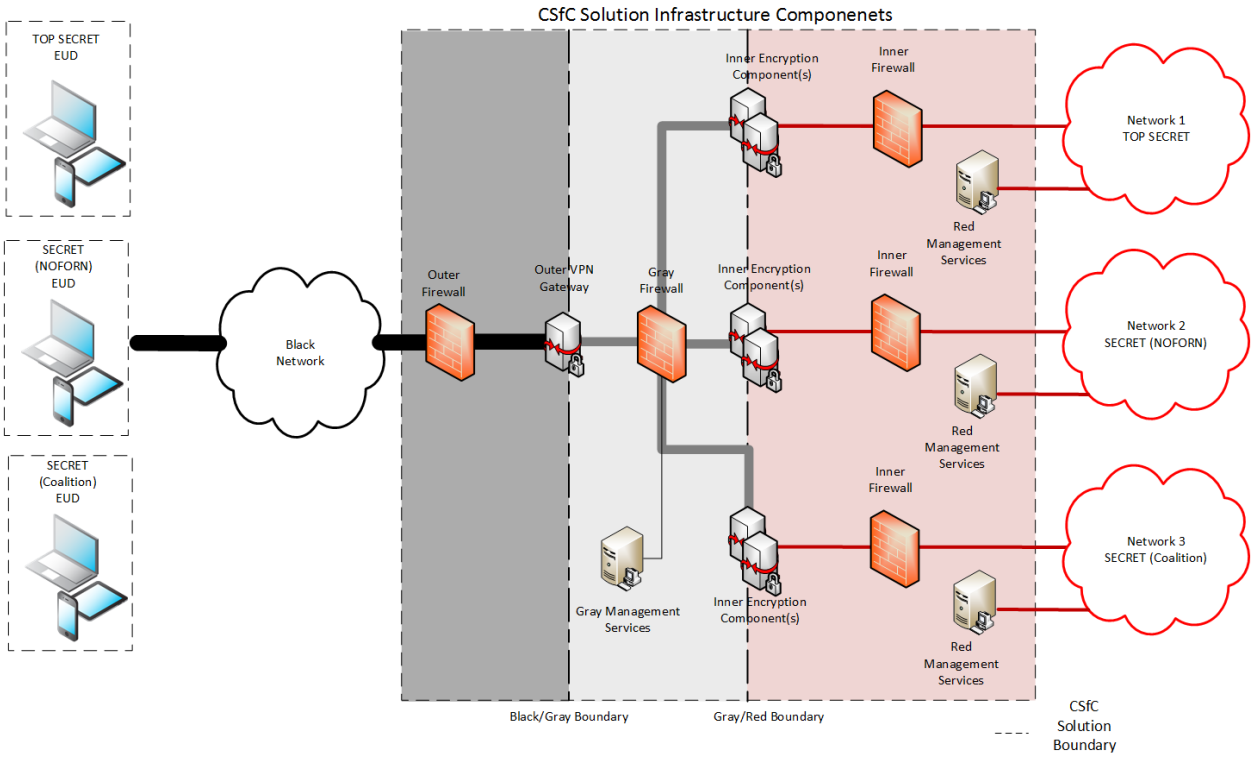

Figure 6. Mobile Access Solution Supporting Multiple Security Levels

4.2.4 Multiple Security Levels

A single implementation of the MA solution may support multiple Red Networks of different security levels. The MA solution provides secure connectivity between EUDs and the Red Network of the same security level while preventing EUDs from accessing Red Networks of different security levels. This enables a customer to use the same physical infrastructure to carry traffic from multiple networks. EUDs operating as part of a Multiple Security Level solution are still dedicated to a single classification level. Although each Red Network will still require its own Inner Encryption Component(s), a site may use a single Outer VPN Gateway in the infrastructure to encrypt and transport traffic that has been encrypted by Inner Encryption Components of varying security levels. As shown in Figure 6 a SECRET Coalition EUD is only capable of communicating with and authenticating to the Inner Encryption Components for Network 3 – SECRET Coalition. This EUD does not have any connectivity to the Inner Encryption Components of Network 1 and Network 2.

There is no limit to the number of different security levels that a MA solution may support.

MA solutions supporting multiple security levels may include independently managed sites (see Section 4.2.2) or multiple sites (see Section 4.2.3). In all cases, separate CAs and management devices are needed to manage the Inner Encryption Components and Inner Firewall at each security level. For example, Figure 6 shows an independent site with multiple security levels. Network 1, Network 2, and

Network 3 each have their own CA and management devices which prevent EUDs from being able to authenticate with the incorrect network.

In addition to separate Inner Encryption Components and CAs, an authentication server must be used to allow the use of a single Outer VPN Gateway for multiple security levels. The authentication server resides within the Gray Management network and validates that Outer Tunnel certificates are signed by the Outer Tunnel CA, are still within their validity period, and have not been revoked. The authentication server also parses the certificate for information assigned to a specific inner network (e.g. Organizational Unit (OU) field or policy Object Identifiers (OIDs)) to determine which inner network the EUD is authorized to connect. After successful authentication, the authentication server provides an accept message to the Outer VPN Gateway along with a Vendor-Specific Attribute (VSA). The Outer VPN Gateway uses the VSA to assign the proper network and firewall rules such that an EUD can only reach the appropriate Inner Encryption Components.

4.3 Rationale for Layered Encryption

A single layer of CNSA encryption, properly implemented, is sufficient to protect classified data in transit across an untrusted network. The MA solution uses two layers of CNSA encryption not because of a deficiency in the cryptographic algorithms themselves, but rather to mitigate the risk that a failure in one of the components, whether by accidental misconfiguration, operator error, or malicious exploitation of an implementation vulnerability, results in exposure of classified information. The use of multiple layers of protection reduces the likelihood of any one vulnerability being used to exploit the full solution.

If an Outer VPN Component is compromised or fails in some way, the Inner Encryption Component can still provide sufficient encryption to prevent the immediate exposure of classified data to a Black Network. In addition, the Gray Firewall can indicate that a failure of the Outer VPN Gateway has occurred, since the filtering rules applied to its external network interface will drop and log the receipt of any packets not associated with an Inner Encryption Component. Such log messages indicate that the Outer VPN Gateway has been breached or misconfigured to permit prohibited traffic to pass through to the Inner encryption component.

Conversely, if the Inner Encryption Component is compromised or fails in some way, the Outer VPN Gateway can likewise provide sufficient encryption to prevent the immediate exposure of classified data to a Black Network. As in the previous case, the Gray Firewall filtering rules applied to its internal network interfaces will drop and log the receipt of any packets not associated with an Inner Encryption Component. Such log messages indicate that the Inner Gateway has been breached or misconfigured to permit prohibited traffic to pass through to the Outer VPN Gateway.

If both the Outer and Inner Gateways are compromised or fail simultaneously, then it may be possible for classified data from the Red Network to be sent to a Black Network without an adequate level of encryption. The security of the MA solution depends on preventing this failure mode by promptly

remediating any compromises or failures in one Encryption Component before the other also fails or is compromised.

Diversity of implementation is needed between the components in each layer of the solution in order to reduce the likelihood that both layers share a common vulnerability. The CSfC Program recognizes two ways to achieve this diversity. The first is to implement each layer using components produced by different manufacturers. The second is to use components from the same manufacturer, where that manufacturer has provided NSA with sufficient evidence that the implementations of the two components are independent of one another. The CSfC web page (http://www.nsa.gov/resources/everyone/csfc) contains details for how a manufacturer can submit this evidence to NSA and what documentation must be provided. Customers that wish to use products from the same manufacturer in both layers must contact their NSA Client Advocate to confirm that NSA has accepted the manufacturer's claims before implementing their solution.

4.4 AUTHENTICATION

The MA solution provides mutual device authentication between Outer VPN components and between Inner Encryption components via public key certificates. This CP requires all authentication certificates issued to Outer VPN components and Inner Encryption components be Non-Person Entity (NPE) certificates, except in the case when TLS EUDs are implemented. In addition, NPE certificates issued to Outer VPN Gateways may need to assert the IP address of the Outer VPN Gateway in either the Common Name field of the certificate Distinguished Name, or in the Subject Alternative Name certificate extension. The EUD may be required to check the IP address asserted in the Outer VPN Gateway certificate and ensure it is the same IP address registered in the EUD.

Following the two layers of device authentication, VPN EUDs require the user to authenticate to the network before gaining access to any classified data (e.g., username/password, user certificate). TLS EUDs may use a device certificate or a user certificate. When a device certificate is used, the user must also authenticate to the Red Network before gaining access to any classified data in the same manner as a VPN EUD (e.g., username/password, user certificate). When a user certificate is used, the user certificate authenticates the Inner layer of TLS encryption and authenticates the user for access to the requested classified data. In this latter case, it is recommended that additional access controls, such as whitelists, be implemented in conjunction with the user certificate to control access to Red Network services.

In addition to authentication for the Outer and Inner layer of encryption, the MA CP requires user-to-device authentication. This authentication occurs between the user and the Computing Device (which processes Red data) of an EUD. In some instances the Computing Device may be physically separate from the component of the EUD which provides the Outer layer of encryption (for example, a Dedicated Outer VPN Gateway provides the Outer layer of encryption). The MA CP requires EUD components use a minimum of a six-character, case-sensitive, alpha-numeric password to authenticate to the device. This password can be used both for decrypting the platform encryption as well as for unlocking the

screen. EUD components, which are selected from the Mobile Platform section of the CSfC Components, are able to use a relatively short authentication factor since they use a hardware based root encryption key which is evaluated during the NIAP certification.

To add additional security to the VPN EUD, a MA solution can include a second factor of authentication to the Inner VPN tunnel. The purpose of adding a second factor of authentication to the solution is to prevent continued access to a network if an End User Device (EUD) is compromised as a result of an attack. If a device has been compromised, it can be assumed that the certificates used to authenticate to the enterprise would be accessible to an adversary to be used on a legitimate device or they could be extracted and used on a different device masquerading as the user. Adding a second authentication factor prevents persistent access to a network if an adversary has managed to compromise the certificates on an EUD.

The second factor will be a “something-you-have” factor manifesting as a physically separate token from the VPN EUD supplying a one-time password for the user to enter. For future versions of the MA CP, transferring this one-time password via a short-range RF communication will be explored. Allowing “something-you-are” (e.g., biometric) as a second factor is also being explored for future versions.

4.5 Other Protocols

Throughout this document, when IP traffic is discussed, it can refer to either IPv4 or IPv6 traffic, unless otherwise specified, as the MA solution is agnostic to most named data handling protocols.

Public standards conformant Layer 2 control protocols are allowed as necessary to ensure the operational usability of the network. This CP is agnostic with respect to Layer 2; specifically, it does not require Ethernet. Public standards conformant Layer 3 control protocols may be allowed based on local AO policy, but the default configuration of this solution is for all Layer 3 control protocols to be disabled. Red and Gray Network multicast messages and Internet Group Management Protocol (IGMP) or Multicast Listener Discovery (MLD) may also be allowed depending on local AO policy. Multicast messages received on external interfaces of the Outer VPN component must be dropped.

It is expected that the MA solution can be implemented in such a way as to take advantage of standards-based routing protocols that are already being used in the Black and/or Red Network. For example, networks that currently use Generic Routing Encapsulation (GRE) or Open Shortest Path First (OSPF) protocols can continue to use these in conjunction with the Outer Firewall and Inner Firewall solution to provide routing as long as the AO approves their use.

4.6 Availability

The high-level designs described in Section 4.2 are not designed with the intent of automatically providing high availability. Supporting solution implementations for which high availability is important is not a goal of this version of the CP. However, this CP does not prohibit adding redundant components in parallel to allow for component failover or to increase the throughput of the MA solution, as long as

each redundant component adheres to the requirements of this CP. The CP does not limit the number of Outer VPN Gateways or Inner Encryption components that can be implemented for high availability in a MA Solution.

5 INFRASTRUCTURE COMPONENTS

In the high-level designs discussed in the previous section, all communications flowing across a Black Network are protected by at least two layers of encryption, implemented using an Outer IPsec VPN tunnel and an Inner layer of IPsec, TLS, or SRTP encryption. Mandatory aspects of the solution infrastructure also include administration workstations, IDS/IPS, SIEM, firewalls, and CAs for key management using PKI.

Each infrastructure component is described in more detail below. The descriptions include information about the security provided by the components as evidence for why they are deemed necessary for the solution. Components are selected from the CSfC Component List and configured per NIAP configuration guidance in accordance with the Product Selection requirements of this CP (see Section 11).

This section also provides details on additional components that can be added to the solution to help reduce the overall risk. However, where indicated in the text, these are not considered mandatory components for the security of the solution; therefore, this CP does not place configuration requirements on those optional components.

5.1 OUTER FIREWALL

The Outer Firewall is located at the edge of the MA solution infrastructure and is connected to the Black transport network.

The external interface of the Outer Firewall only permits IPsec IKE and ESP traffic with a destination address of the Outer VPN Gateway.

The internal interface of the Outer Firewall only permits IPsec traffic with a source address of the Outer VPN Gateway and any necessary control plane traffic. The minimum requirements for port filtering on the Outer Firewall can be found in Section 12.11.

The Outer Firewall, selected from the CSfC Components List, must be physically separate from the Outer VPN Gateway, as shown in Figure 4.

5.2 OUTER VPN GATEWAY

Authentication of peer VPN Components, cryptographic protection of data in transit, and configuration and enforcement of network packet handling rules are all aspects fundamental to the security provided by VPN Gateways.

The external interface of the Outer VPN Gateway is connected to the internal interface of the Outer Firewall. The VPN Gateway establishes an IPsec tunnel with peer Outer VPN Components, which provides device authentication, confidentiality, and integrity of information traversing Black Networks. VPNs offer a decreased risk of exposure of information in transit since any information that traverses a Black Network is placed in a secure tunnel that provides an authenticated and encrypted path between the site and an EUD. The Outer VPN Gateway is implemented identically for all the high-level designs supporting a single security level. When supporting Multiple Security Levels, the Outer VPN Gateway must use a gray authentication server.

Similar to the Outer Firewall, the external interface of the Outer VPN Gateway only permits IPsec traffic. The internal interface of the Outer VPN Gateway is configured to only permit traffic with an IP address and port associated with Inner Encryption Components, Gray Management Services (i.e., SIEM and administration workstation), or control plane component (i.e., DNS and NTP Servers in the Gray).

The Outer VPN Gateway is prohibited from implementing routing protocols on external and internal interfaces and must rely upon the Outer Firewall to provide any dynamic routing functionality. The Outer VPN Gateway, selected from the CSfC Components List, must be physically separate from the Outer Firewall and Gray Firewall as shown in Figure 4.

The Outer VPN Gateway is implemented in conjunction with a Gray authentication server when multiple security levels are implemented (as described in Section 4.2.4). The Outer VPN Gateway acts as an EAP pass-through for authentication between the EUD and the authentication server. Upon successful mutual authentication, the Outer VPN Gateway receives an accept message and VSA for that specific EUD. The Outer VPN Gateway uses the VSA attribute to assign the correct IP address and ACL to ensure that the EUD is capable of reaching only the correct Inner Encryption Component.

The Outer VPN Gateway cannot route packets between Gray and Black Networks; any packets received on a Gray Network interface and transmitted to a Black Network interface must be transmitted within an IPsec VPN tunnel configured according to this CP.

5.3 Gray Firewall

The Gray Firewall is located between the Outer VPN and Inner encryption components. In addition to filtering EUD traffic, the Gray Firewall also provides packet filtering for the Gray Management Services.

The external interface of the Gray Firewall should only accept packets with a source address of the Outer VPN Gateway's IP pool assigned to EUDs. The internal interface of the Gray Firewall should only accept packets with a source address of the TLS-Protected server or the Inner VPN Gateway as part of an established communication session. When supporting multiple security levels the Gray Firewall must also ensure that only EUDs and Inner Encryption components of the same security level are able to communicate.

In addition to EUD data traffic, the Gray Firewall adjudicates traffic related to both the management of the Gray boundary and EUD control plane traffic. The Gray Firewall, selected from the CSfC Components List, must be physically separate from the Outer VPN Gateway and Inner Encryption Components, as shown in Figure 4.

5.4 Inner Firewall

The Inner Firewall is located between the Inner encryption components and the Red Network. The external interface of the Inner Firewall should only accept inbound traffic with a source address of the TLS-Protected server or Inner VPN Component. The internal interface of the Inner Firewall should only allow outbound traffic from the Red enclave to the Inner VPN Component or the TLS-Protected server. The TLS-Protected servers include, but are not limited to: VoIP call managers, mobile device management (MDM) services, VDI, and web server content.

The Inner Firewall, selected from the CSfC Components List, must be physically separate from the Inner Encryption Components.

5.5 Gray Management Services

Secure administration of components in the Gray Network and continuous monitoring of the Gray Network are essential roles provided by the Gray Management Services. The Gray Management Services are composed of multiple components that provide distinct security to the solution. The MA CP allows flexibility in the placement of some Gray Management Services, as described below. All components within the Gray Management Services are either directly or indirectly connected to the Gray Firewall (e.g., multiple Gray Management Services connected to a switch which is connected to the Gray Firewall). The Gray Management Services are physically protected as classified devices.

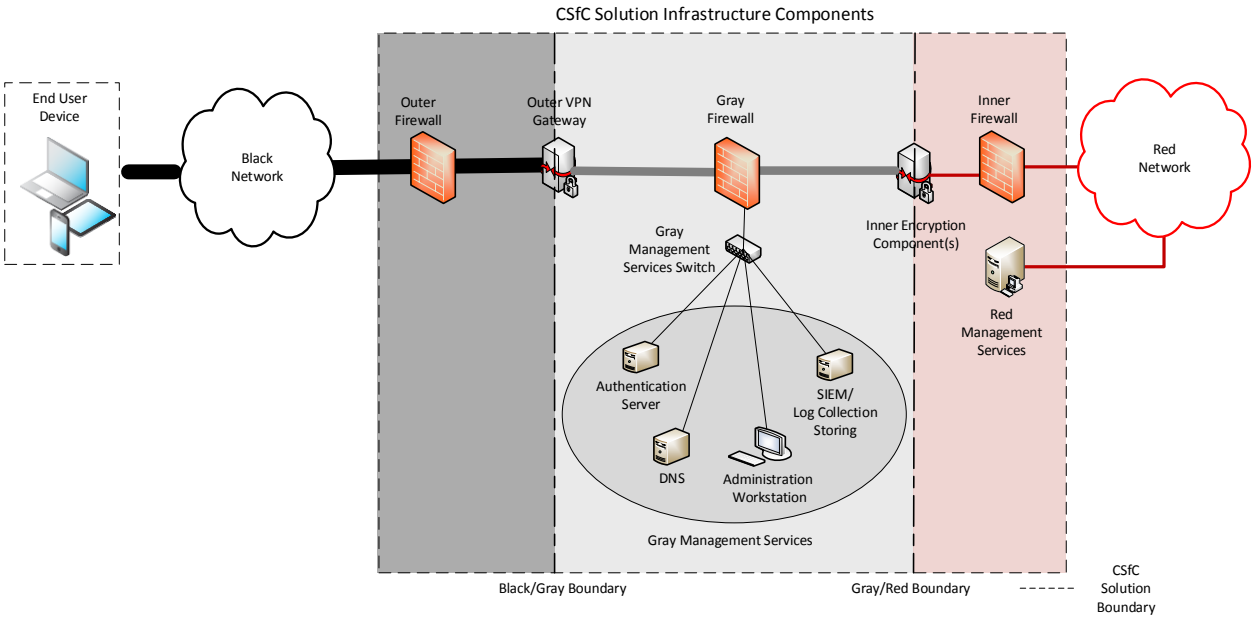

Figure 7. Overview of Gray Management Services

Figure 7 shows the infrastructure components of the Gray Management Services in the MA Solution. Within the Gray Network, which is between the Outer VPN Gateway and Inner Encryption Components, has an Administration workstation, SIEM, Authentication Server, and DNS. Components within the Gray Network are further described below.

5.5.1 Gray Administration Workstation

Gray administration workstations are responsible for maintaining, monitoring, and controlling all security functionality for the Outer VPN Gateway, Gray Firewall, and all Gray Management service components. The Gray administrative workstations are not permitted to maintain, monitor, or control Inner Encryption Components or Red Management Services. All MA solutions will have at least one Gray administrative workstation. Section 7 provides more detail on management of MA solution components.

5.5.2 Gray Security Information and Event Management (SIEM)

The Gray SIEM collects and analyzes log data from the Outer VPN Gateway, Gray Firewall, and other Gray Management service components. Log data may be encrypted between the originating component and the Gray SIEM with SSHv2, TLS, or IPsec to maintain confidentiality and integrity of the log data. At a minimum, an auditor reviews the Gray SIEM alerts and dashboards on a daily basis. The SIEM is configured to provide alerts for specific events including if the Outer VPN Gateway or Gray Firewall receive and drop any unexpected traffic which could indicate a compromise of the Outer Firewall or Outer VPN Gateway respectively. These functions can also be performed on a Red SIEM if a CDS is used as described in this CP (see Section 8.5).

5.5.3 GRAY AUTHENTICATION SERVER

The Gray authentication server is only required for solutions supporting multiple security levels. The authentication server is responsible for performing mutual authentication with EUDs utilizing the Outer VPN Gateway as an EAP pass-through. In addition to verifying that certificates are signed by the correct CA, are within their validity period, and are not revoked, the authentication server parses the certificate for information (e.g., OU field or Policy OID) that is associated with the Red Network with which the EUD is permitted to establish an Inner IPsec connection or TLS session. Upon successful authentication of the EUD, the authentication server sends an Access-Accept packet to the Outer VPN Gateway. The Access-Accept packet includes an attribute derived from the OU or policy OID which the Outer VPN Gateway uses to apply ACLs and route the EUDs traffic to the proper Inner Encryption Component.

5.6 INNER ENCRYPTION COMPONENTS

The MA CP allows for the use of up to three different types of Inner Encryption Components: Inner VPN Gateway, Inner TLS-Protected Server, or Inner SRTP Endpoint. Inner VPN Gateways are always located between the Gray Firewall and Inner Firewall. An Inner VPN Gateway will always have at least two interfaces, one external interface connected to the Gray Firewall and one internal interface connected to the Inner Firewall.

Inner TLS-Protected Servers and Inner SRTP endpoints are permitted to use a single data plane interface or multiple data plane interfaces. Similar to the Inner VPN Gateway, Inner TLS-Protected Servers and SRTP endpoints with multiple interfaces have one external interface connect to the Gray Firewall and one internal interface connected to the Inner Firewall. If implemented with a single data plane interface, then that interface establishes the Inner layer of encryption and provides the classified data to the TLS EUD. An example of a TLS-Protected Server with a single data plane interface is a web server located between the gray Firewall and Inner Firewall that terminates the Inner layer of encryption with Hypertext Transfer Protocol Secure (HTTPS) and directly returns the content to the TLS EUD. The TLS-Protected Servers and SRTP endpoints must be placed between the Gray Firewall and Inner Firewall, but are not required to connect to the Red Network or Inner Firewall if it is acting as the server for the EUDs. Inner VPN Gateways and TLS-Protected Servers are always managed from the Red Management Services. The management interface of the Inner VPN Gateway or TLS-Protected server can either be connected to the Inner Firewall or run directly to a standalone Red Management Services enclave.

A MA solution infrastructure may support both TLS EUDs and VPN EUDs. When supporting both TLS EUDs and VPN EUDs the solution infrastructure will always include an Inner VPN Gateway between the Gray Firewall and Inner Firewall. This Inner VPN Gateway will terminate the Inner layer of IPsec traffic for all VPN EUDs. Additionally, the solution infrastructure will include one or more TLS-Protected Servers. The TLS-Protected Servers are placed between the Gray Firewall and Inner Firewall. The TLS-Protected Server(s) must be placed in parallel with the Inner VPN Gateway such that the TLS-Protected Server is not dependent on the Inner VPN Gateway to reach the Gray Firewall or Inner Firewall (see Appendix D. End User Device Implementation Notes).

For load balance or other performance reasons, multiple Inner Encryption Components that comply with the requirements of the CP are acceptable.

5.6.1 INNER VPN GATEWAY

Similar to the Outer VPN Gateway, the Inner VPN Gateway provides authentication of peer VPN Components, cryptographic protection of data in transit, and configuration and enforcement of network packet handling rules. The Inner VPN Gateway is located between the Gray firewall and the Inner Firewall. The Inner VPN Gateway is required to be implemented if supporting VPN EUDs.

The external interface of the Inner VPN Gateway is connected to the internal interface of the Gray Firewall. The VPN Gateway establishes an IPsec tunnel with peer Inner VPN Components. Similar to the Outer VPN Gateway, the external interface of the Inner VPN Gateway only permits the egress of IPsec traffic and AO-approved control plane traffic. The internal interface of the Inner VPN Gateway is configured to only permit traffic with an IP address and port associated with Red Network services.

The Inner VPN Gateway cannot route packets between Red and Gray Networks. Any packets received on a Red Network interface and sent to a Gray Network interface must be transmitted within an IPsec VPN tunnel that is configured according to this CP. The Inner VPN Gateway, selected from the CSfC Components List, must be physically separate from the Gray Firewall and Inner Firewall.

5.6.2 INNER TLS-PROTECTED SERVER

The Inner TLS-Protected Server(s) uses TLS with select cryptographic cipher suites to provide confidentiality, integrity, and mutual authentication between a TLS EUD and TLS-Protected Server(s). The TLS-Protected Server is located between the Gray Firewall and the Inner Firewall. The MA CP allows the TLS-Protected Server to use any protocol that is encapsulated within TLS.

The TLS-Protected Server should have a different cryptographic library from the one used in the Outer VPN Gateway and must only be managed from the Red Management Services.

The TLS-Protected server can be managed, through a dedicated network management interface, or internally, through a trusted inline interface. If the TLS-Protected Server is managed from the internal interface, the Host-Based Firewall must be configured to allow only those ports and protocols that are required for the solution to operate as specified in this CP (see Section 12.7). Inner TLS-Protected Servers must be managed from the red administration workstation. The TLS-Protected Server must also be configured with a Host-Based Firewall. The Host-Based Firewall must have a deny-by-default rule set for both inbound and outbound data plane, control plane, and management traffic. Only ports and protocols that are required for the system to operate, have an explicit allow enabled in the firewall.

Examples of TLS-Protected Servers include, but are not limited to, web servers, Session Initiation Protocol (SIP) servers, VDI Servers, and MDM servers. Web servers implemented as part of the MA CP terminate the Inner layer of encryption utilizing HTTPS. SIP servers use SIP over TLS for registration of EUDs and SRTP endpoints, session setup, and session termination. When SIP servers are included,

Session Description Protocol Security Descriptions (SDES) is used over the SIP TLS session for key exchange between TLS EUDs or between a TLS EUD and a SRTP Endpoint. The Inner TLS Protected-Server, selected from the CSfC Components List, must be physically separate from the Gray Firewall and Inner Firewall as shown in Figure 4.

5.6.3 Inner SRTP Endpoint

Inner SRTP endpoints provides cryptographic protection of data in transit. Within the MA solution infrastructure, SRTP endpoints are located between the Gray Firewall and the Inner Firewall. The Inner layer of SRTP encryption can also be terminated between two TLS EUDs (see Section 6.3). Registration, session setup (including authentication and key exchange), and session termination for the SRTP endpoints is performed utilizing SIP over TLS.

All SRTP endpoints that terminate the Inner layer of encryption originating from a TLS EUD reside within the CSfC Solution Boundary and must meet all applicable requirements as described in the MA CP.

The VoIP gateway/border controller terminates SRTP Traffic from a TLS EUD and relays the data to the Red Network. Inclusion of a VoIP gateway/border controller allows integration with existing enterprise voice systems.

The Inner SRTP endpoint, selected from the CSfC Components List, must be physically separate from the Gray Firewall and Inner Firewall as shown in Figure 4.

5.7 Red Management Services

Secure administration of Inner Encryption Components and continuous monitoring of the Red Network are essential roles provided by the Red Management Services. Red Management Services are composed of a number of components that provide distinct security to the solution. The MA CP allows flexibility in the placement of some Red Management Services as described below.

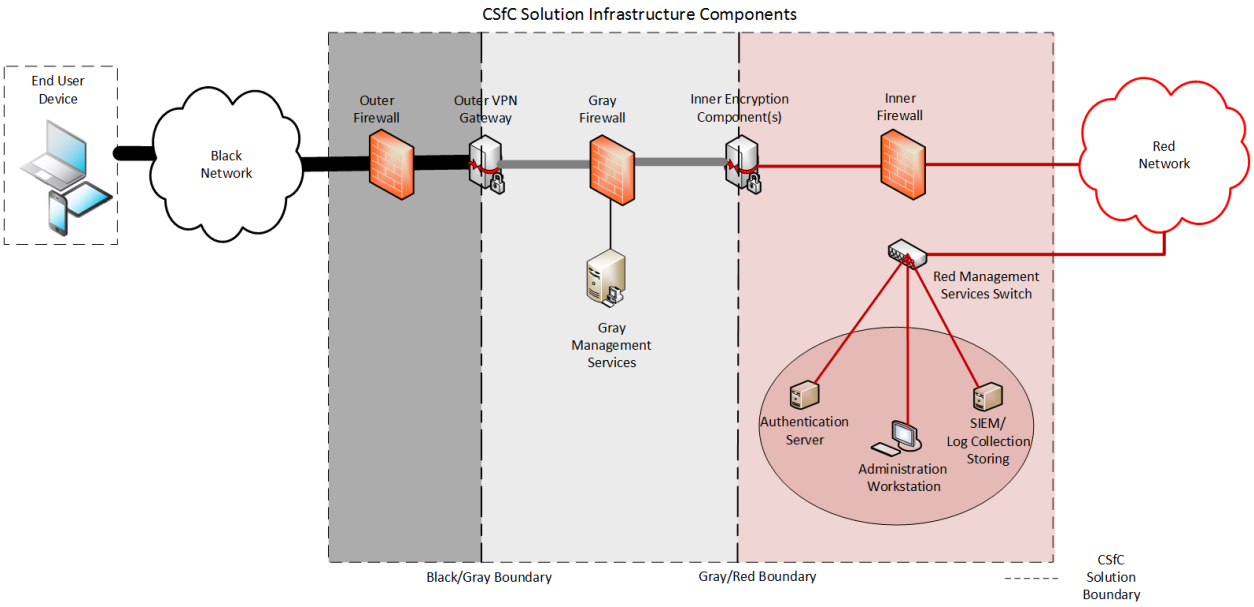

Figure 8. Overview of Red Management Services

Figure 8 shows the infrastructure components of the Red Management Services in the MA Solution. Within the Red Network, which is located beyond the Inner Encryption Components, has a management services components associated with it. Each of the management services components are described below.

5.7.1 Red Administration Workstations

The Red administration workstation is responsible for maintaining, monitoring, and controlling all security functionality for the Inner Encryption Components, Inner Firewall, and all Red Management service components. The Red administrative workstations are not permitted to maintain, monitor, or control Outer Encryption Components or Gray Management Services. All MA solutions will have at least one Red administrative workstation. Section 7 provides more detail on management of MA solution components.

5.7.2 Red Security Information and Event Management (SIEM)

Red SIEMs collect and analyze log data and flow data from the Inner Encryption Components, the Inner Firewall, and other Red Management service components. Log data may be encrypted between the originating component and the Red SIEM with SSHv2, TLS, or IPsec to ensure confidentiality and integrity. The SIEM is configured to provide alerts for specific events. Customers are encouraged to leverage existing Enterprise SIEM capabilities to monitor log data from Inner Encryption Components, the Inner Firewall, and Red Management Services. A Red SIEM may also be used to analyze log data from Gray Network components when used in conjunction with an approved CDS as described in this CP (see Section 8.5).

5.8 Public Key Infrastructure Components

Key Management Requirements have been relocated to a separate Key Management Requirements Annex.

6 END USER DEVICE COMPONENTS

The MA CP supports both VPN EUDs and TLS EUDs; however, the EUD must be dedicated as either a VPN EUD or TLS EUD. VPN and TLS EUDs are composed of a Computing Device and optionally include a physically separate Dedicated Outer VPN to provide the Outer layer of IPsec encryption. When a Dedicated Outer VPN is included as part of the EUD it must either be physically connected to the computing platform utilizing an Ethernet cable or connected over Wi-Fi with WPA2.

A RD is required when connecting to the Black Network, except for the solution designs and use cases specified in Section 4.1.3 and 6.1.1.

6.1 Outer VPN Component

The allowable Outer VPN Components for both the VPN and TLS EUD are identical. Authentication of peer VPN Components and cryptographic protection of data in transit are fundamental aspects of the security provided by the EUD Outer VPN Component.

The Outer VPN Component establishes an IPsec tunnel with the solution infrastructure Outer VPN Gateway, which provides device authentication, confidentiality and maintains the integrity of information traversing Black Networks. The MA CP allows the use of VPN Gateways or VPN Clients to be used as the Outer VPN Component of EUDs.

The classification of private keys and certificates used for the authentication of the Outer VPN Component are considered Controlled Unclassified Information (CUI) and must be protected with a FIPS 140-2-validated cryptographic module. Customers deploying MA solutions in high-threat environments may also choose to implement controls to mitigate against tampering attacks.

Solutions supporting Multiple Security Levels (as described in Section 4.2.4) configure EUDs to perform authentication of the Outer IPsec tunnel utilizing an EAP-TLS as part of the IPsec IKE to the Outer VPN Gateway. Mutual authentication occurs between the EUD and the authentication server utilizing the Outer VPN Gateway as an EAP pass-through.

6.1.1 Dedicated Outer VPN

A Dedicated Outer VPN can be used as the Outer VPN Component for EUDs. Utilizing a physically separate VPN as part of the EUD improves security by providing physical separation between the Computing Device and the Outer layer of encryption. When a Dedicated Outer VPN is used as part of an EUD, there is no requirement to use a Government RD. When utilizing a Dedicated Outer VPN, the Outer VPN and Computing Device are collectively referred to as the EUD.

The Dedicated Outer VPN included as part of the EUD must either be physically connected to the computing platform utilizing an Ethernet cable or connected over Wi-Fi with WPA2. The Wi-Fi connection between the computing platform and Outer VPN Gateway can be either WPA2 Enterprise or WPA2 PSK. The Dedicated Outer VPN is selected from either the *IPsec VPN Gateway* section or the *IPsec VPN Client* section of the CSfC Components List. Dedicated Outer VPNs that support wireless connectivity with the computing platform must also be selected from the *WLAN Access System* section of the CSfC Components List.

When a Dedicated Outer VPN is included as part of an EUD, it provides configuration and enforcement of network packet handling rules for the Outer layer of encryption. The configuration settings of the Dedicated Outer VPN may need to be updated when entering new environments (e.g., updating the Default Gateway). Dedicated Outer VPNs are dedicated to a single security level and can only provide the Outer layer of IPsec for clients connecting to a Red Network of the same security level.

6.1.2 Outer VPN Client

An Outer VPN Client can be used as the Outer VPN Component for MA EUDs. The purpose of the Outer VPN Client is to establish an IPsec tunnel to the Outer VPN Gateway of the MA solution infrastructure. The tunnel can be configured to automatically be established as part of the EUD's power-on process. A combination of the VPN Client, and the operating system on which it is installed on the computing platform, is responsible for providing configuration and enforcement of network packet handling rules for the Outer layer of encryption. The Outer VPN Client is selected from the *IPsec VPN Client* section of the CSfC Components list. The VPN Client is installed on the Computing Device selected from the *Mobile Platform* section of the CSfC Components List.

6.2 VPN EUD

VPN EUDs use IPsec using a VPN Client to provide the Inner layer of encryption. The purpose of the Inner VPN Client is to establish an IPsec tunnel to the Inner VPN Gateway of the MA solution infrastructure. The tunnel can be configured to automatically be established as part of the EUD's power-on process, following establishment of the Outer VPN tunnel. Once the Inner VPN Client establishes the Inner IPsec tunnel, any application installed on the Computing Device can send and receive classified data with the Red Network. The private keys and certificates used for the authentication of the Inner VPN Component are considered CUI and must be, at a minimum, protected by enabling the native platform DAR protection.

Appendix D. End User Device Implementation Notes, provide more detail on the allowable configuration of VPN EUDs.

A VPN Client can be used as the Inner VPN Component for VPN EUDs. The purpose of the Inner VPN Client is to establish an IPsec tunnel to the Inner VPN Gateway of the MA Solution Infrastructure. The tunnel can be configured to automatically be established as part of the EUD's power-on process. A combination of the VPN Client and the Operating System on which it is installed is responsible for

providing configuration and enforcement of network packet handling rules for the Inner layer of encryption. The Inner VPN Client is selected from the *IPsec VPN Client* section of the CSfC Components list. The VPN Client is installed on the Computing Device selected from the *Mobile Platform* section of the CSfC Components List.

Virtualization must be used when an Outer VPN Client and Inner VPN Client both reside on the same Computing Device. Use of virtualization ensures that two separate IP stacks are used. Appendix D. End User Device Implementation Notes provide additional guidance on implementing EUDs.

6.3 TLS EUD

TLS EUDs use TLS clients or SRTP clients to provide the Inner layer of encryption. The Inner layer of TLS or SRTP is implemented by TLS clients and SRTP clients provided by individual applications installed on the Computing Device. Each application that sends and receives data to the Red Network must be selected and configured in accordance with the requirements of the CP. Each application then terminates the Inner layer of encryption to TLS-Protected Servers and SRTP endpoints within the MA solution infrastructure.

The private keys and certificates used for user authentication of the Inner TLS and SRTP clients are determined by the AO. If the private keys and certificates are considered CUI then the EUD component must, at a minimum, implement the native platform encryption. If the private keys and certificates are considered to be classified, then the EUD must be treated as classified at all times or implement a NSA-approved DAR Solution (see Section 4.2.1).

TLS EUDs must use either a Government RD or Dedicated Outer VPN to connect to the Black Network, except for the use cases defined in Section 4.1.3 which provides more detail on the allowable configuration of TLS EUDs.

6.3.1 TLS Client

Applications with a TLS client can be installed on the Computing Device and used for the Inner layer of TLS encryption. On TLS EUDs, every application that sends or receives data through the Outer VPN Component must be independent. For example, if a voice application, web browser, MDM agent, and email client are installed on the Computing Device, each application is configured to establish a TLS session to the TLS-Protected Server in the MA solution infrastructure. In some instances an application may perform both TLS and SRTP encryption. Those applications must be configured to meet requirements for both TLS clients and SRTP clients.

The TLS-client uses a device certificate or user certificate for authentication to the TLS-Protected Server. The certificates are issued by the Inner CA, which may be the same CA that issues certificates to the TLS-Protected Servers (e.g., customer enterprise CA). When a device certificate is used, the user must then authenticate to the Red Network before gaining access to any classified data (e.g., username and password, token). When a user certificate is used, the user certificate authenticates the Inner layer of

TLS encryption and authenticates the user for access to the requested classified data. A combination of the TLS Client and Computing Device Operating System is responsible for providing configuration and enforcement of network packet handling rules for the Inner layer of encryption.

6.3.2 SRTP CLIENT

Applications with a SRTP client can be installed on the Computing Device and used for the Inner layer of SRTP encryption. If multiple SRTP clients are installed on the TLS EUD, then each must be configured independently. SRTP Clients are generally used to encrypt real time traffic, such as voice or video. In some instances, an application may perform both TLS and SRTP encryption. Those applications must be configured to meet requirements for both TLS clients and SRTP clients.

SRTP clients use certificates for mutual authentication. In most cases, the SRTP client uses a user certificate for authentication. User certificates are issued by an Inner CA, which may be the same PKI that issues certificates to TLS-Protected Servers (e.g., customer enterprise PKI), which may be different than the Inner CA. Alternatively, the SRTP client can use a device certificate for authentication followed by user authentication (i.e., username and password, token, smartcard, etc.). A combination of the SRTP Client and Computing Device Operating System is responsible for providing configuration and enforcement of network packet handling rules for the Inner layer of encryption.

7 MOBILE ACCESS CONFIGURATION AND MANAGEMENT

The MA CP includes design details for the provisioning and management of Solution Components, which requires the use of Security Administrators to initiate certificate requests, and Registration Authorities (RAs) to approve certificate request. The CSfC solution owner must identify authorized SAs and RAs to initiate and approve certificate requests, respectively. The following sections describe the design in detail and Section 12 articulates specific configuration requirements that must be met to comply with the MA CP.

7.1 SOLUTION INFRASTRUCTURE COMPONENT PROVISIONING

Provisioning is an out-of-band process performed in a physically secured area (e.g., the Red Network) through which MA solution infrastructure components are configured and initialized before their first use. During the provisioning process, the Security Administrator configures the Outer VPN Gateway, Gray Management Services, Inner Encryption Components, and Red Management Services in accordance with the requirements of this CP.

During provisioning, the Outer VPN Gateways and Inner Encryption Components generate a public/private key pair and output the public key in a Certificate Signing Request (CSR). The Security Administrator delivers the Outer VPN Gateways' CSR to the Outer CA and the Inner Encryption Components' CSR to the Inner CA. The appropriate CA processes the CSR for each encryption component and returns a signed X.509 certificate. The Security Administrator then installs the unique

signed certificate and the certificate chain, which consists of the signing CA's certificate and the Trust Anchor certificate (i.e., Root CA certificate). The Security Administrator may also install an initial CRL.

7.2 EUD Provisioning

Provisioning of EUDs can be performed via direct hard-wire connection or over the air using a controlled access wireless network. During the provisioning process, the Security Administrator loads and configures the required software for the EUD. The Security Administrator instructs the EUD to generate the requisite public/private key pairs for the EUD's Outer VPN Component and Inner Encryption Component as well as output the public keys in a specified CSR format for delivery to the Outer CA and the Inner CA, respectively.

If the VPN EUD uses a Dedicated Outer VPN to establish the Outer IPsec tunnel, the public/private key pairs and CSRs are generated on and output from the Dedicated Outer VPN device. For TLS EUDs that require an enterprise user certificate in addition to the Outer and Inner Tunnel device certificates, the CSR is delivered to the CA in the customer's organization that has the authority to issue enterprise user certificates. This CA may not be the same as the Inner CA.

If the EUD cannot generate its own key pairs or CSRs, then a dedicated management workstation is required to generate the key pairs for the EUD and construct the CSRs for delivery to the Outer CA and the Inner CA. The CAs process the CSRs and return signed certificates to the Security Administrator, who installs the certificates onto the EUD, and if required, the Dedicated Outer VPN device. If required, the Security Administrator also installs the private keys onto the EUD. The Security Administrator then finalizes the security configuration of the EUD before it is used for the first time.

If the MA solution owner is unable to remotely manage EUDs over the two layers of encryption within a MA solution, then the EUDs must be periodically locally re-provisioned in order to receive software and configuration updates. Re-provisioning consists of revoking the EUD's existing certificates and provisioning the EUD using a trusted baseline configuration that does not make use of any retained data originally stored on the EUD (e.g., factory reset and provision as a new device). This CP does not impose a particular frequency for re-provisioning. Without remote management of EUDs, re-provisioning is the only means of applying security-critical patches to EUDs.

Due to the time and effort needed to re-provision EUDs, it is preferable to remotely manage them when possible. With remote management capabilities, updated software (e.g., VPN client, VoIP application) and configuration data (e.g., Mandatory Access Control (MAC) policy, MDM policy) can be provided from a central management site through the MA solution to the EUD after the EUD establishes the two MA solution tunnels (see Section 4.2.1).

7.3 Administration of Mobile Access Components

Each component in the solution has one or more administration workstations that are responsible for maintaining, monitoring, and controlling all security functions for that component. It should be noted

that all of the required administrative functionality does not need to be present in each individual workstation, but the entire set of administration workstations must collectively meet administrative functionality requirements.

The administration workstation is used for configuration review and management. Implementations will employ a SIEM in the Gray Management Services for log management of Gray Infrastructure Components except where AOs use a CDS to move Gray Network log data to a Red SIEM.

Given the architecture of the solution, each layer has its own distinct administration LAN or VLAN; the Inner Encryption Components are managed from the Red Management Services and the Outer VPN Gateway and supporting components are managed from the Gray Management Services.

The Gray Administration Workstation, along with all Gray Management Services, is physically connected to the Gray Firewall. The Gray Firewall maintains separate ACLs to permit management traffic to/from the Gray Management Services, but prohibits such traffic from all other components. These ACLs ensure that approved management traffic is only capable of flowing in the intended direction. This architecture provides the separation necessary for two independent layers of protection.

Administration workstations must be dedicated terminals for the purposes given in the CP. For example, administration workstations are not to be used as the registration authority for the CA, a SIEM, or as a general user workstation for performing any functions besides management of the solution. Additionally, Administration workstations cannot be used as an enrollment workstation or provisioning workstation.

Management of all MA solution components is always encrypted to protect confidentially and integrity, except in the case where components are locally managed through a direct physical connection (e.g., serial cable from Gray administration workstation to Outer VPN Gateway). Management traffic must be encrypted with SSH, TLS, or IPsec. When components are managed over the Black Network, a CSfC Solution must be implemented in order to provide two layers of approved encryption. This requirement is not applicable if the MA solution infrastructure components are being managed from the same LAN or VLAN. For example, a Gray administration workstation residing within the Gray Management Services at the same site as the Outer VPN Gateway need not use CNSA Suite algorithms since this traffic does not traverse an untrusted network.

In most cases, Computing Devices are managed over the Black Network by utilizing the Outer layer of IPsec and a MDM server selected from the CSfC Components List. When a MDM server is used to manage TLS EUDs, the MDM server is considered a TLS-Protected Server and the MDM agent is considered a TLS Client. As a result, the MDM server must be placed between the Gray Firewall and Inner Firewall. Like other Inner Encryption Components, the MDM server is managed from the Red administration workstation. As a TLS-Protected Server, the MDM server must be configured to establish a session with the MDM agent in accordance with the requirements in Table 15. TLS-Protected Server &

SRTP Endpoint Requirements. Although not mandatory, the use of a MDM enables organizations to dynamically change policies enforced on the Computing Device, allowing more flexibility. Additionally, there are several security advantages by using a MDM including the ability to perform a remote wipe of the EUD.

7.4 EUDs for Different Classification Domains

As specified in this CP, an EUD is only authorized to communicate with Red Networks operating at the same classification level. Implementation of the Multiple Security Levels design does not change the requirement for EUDs to be dedicated to a single classification level. However, the CP does not preclude the possibility that an approved CDS can be used within an infrastructure to provide cross domain transfer of data between EUDs operating at differing classification levels. It also does not preclude the use of an EUD as an access CDS for multiple enclaves operating at different classification levels if approved through the appropriate CDS approval process.

The requirements for a CDS capable of providing separation between enclaves of two or more classification levels are outside the scope of this CP. If developing a MA solution with a CDS capability, the solution must register against this CP and use the appropriate CDS approval processes.

8 CONTINUOUS MONITORING

The MA CP allows customers to use EUDs physically located outside of a secure government facility. With this increase in accessibility comes a need to continuously monitor network traffic and system log data within the solution infrastructure. This monitoring allows customers to detect, react to, and report any attacks against their solution. This continuous monitoring also enables the detection of any configuration errors within solution infrastructure components.

At a minimum, this CP requires an auditor to review alerts, events, and system logs on a daily basis. This minimum review period allows customers in tactical environments to implement solutions in situations where it may not be feasible to perform real-time monitoring. Operational and strategic implementations of the MA solution, however, should have an auditor review alerts, events, and system logs on a much more frequent basis and in many cases are recommended to leverage Operations Centers to perform continuous monitoring of the solution.

8.1 Monitoring Points

The MA CP requires network traffic monitoring occur, at a minimum, in two (M2 and M3) of the four listed areas within the solution infrastructure. Network traffic can be monitored using an IDS; however, it is preferable to use an IPS to enable real-time responses. While it is only required to monitor two of the four locations, customers monitoring all four points have the best visibility, enabling maximum detection of malicious activity or misconfiguration of components.

Figure 9 shows the four locations that customers must choose from when implementing network monitoring capabilities. There are multiple configurations for deploying the IDS/IPS at two or more of the monitoring points (M1, M2, M3, and M4) listed in this CP. IDS/IPS systems can ingest traffic from network taps, span ports, or in-line with the solution.

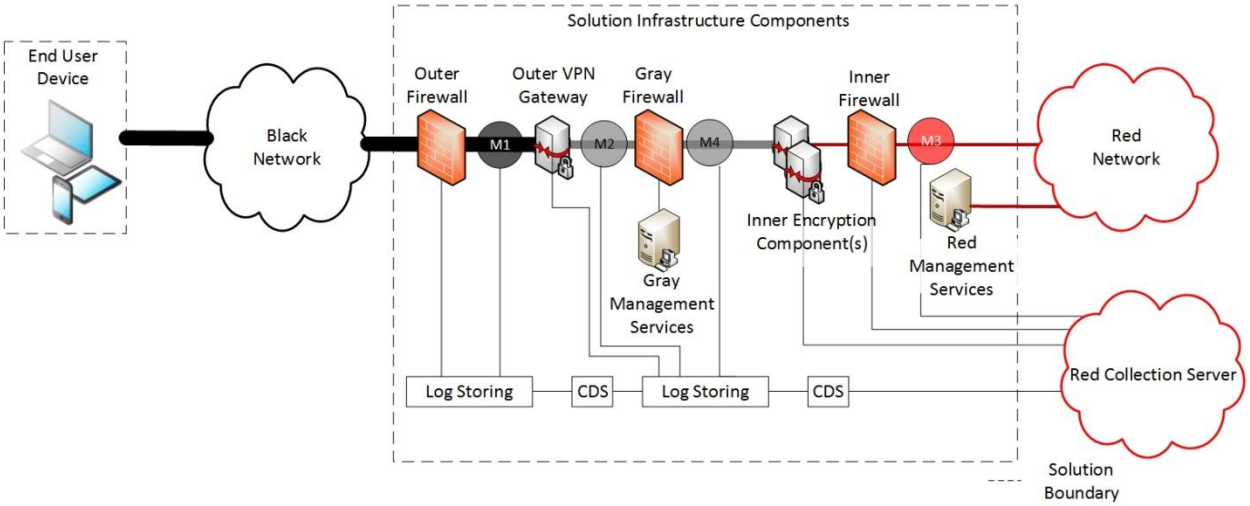

Figure 9. Solution Continuous Monitoring Point

The following paragraphs define each of the four monitoring points. These descriptions outline the analysis and alerts that would be generated by the IDS/IPS in each location. If a customer decides to implement an IPS, then it should be configured to block specific traffic flows as well as generate an appropriate alert.

Monitoring Point 1 (M1): Located between the Outer Firewall and Outer VPN Gateway, a M1 IDS/IPS is, at a minimum, configured to generate an alert upon detection of any traffic that should have been blocked by the Outer Firewall. These alerts indicate a failure of the Outer Firewall's filtering functions and are evidence of either an improper configuration or a potential compromise. Normal traffic at M1 is well-defined (e.g., IPsec encryption and a limited number of approved control plane protocols) and, as a result, is unlikely to produce false positives. Since nearly all traffic traversing M1 is encrypted with IPsec, the IDS/IPS is limited to analyzing only IP addresses, ports, protocols, and flow data. Management of the M1 IDS/IPS occurs within the Black Network.

Monitoring Point 2 (M2): Located between the Outer VPN Gateway and Gray Firewall, a M2 IDS/IPS is, at a minimum, configured to generate an alert upon detection of any traffic that should have been blocked by the Outer VPN Gateway. These alerts can indicate a failure of the Outer Firewall or Outer VPN's filtering functions and are evidence of either an improper configuration or a potential compromise. Normal traffic at M2 is not as narrowly defined, but includes IPsec traffic, data plane traffic encrypted with TLS or SRTP, control plane traffic, and management traffic. Nearly all traffic traversing M2 is encrypted either with IPsec, TLS, SRTP, or SSH, which prevents deep packet inspection.

Management of the M2 IDS/IPS occurs within the Gray Management Services. Monitoring of M2 is mandatory.

Monitoring Point 3 (M3): Located between the Inner Firewall and Red Network, a M3 IDS/IPS is, at a minimum, configured to generate an alert upon detection of any traffic that should have been blocked by the Inner Firewall. These alerts indicate a failure of the Inner Firewall's filtering functions. Of the four monitoring points, M3 is the most difficult to define, but in many implementations, utilizing M3 allows for deep packet inspection as traffic may not be encrypted. Management of the M3 IDS/IPS occurs from within the Red Management Services. Monitoring of M3 is mandatory.

Monitoring Point 4 (M4): Located between the Gray firewall and Inner Encryption Components, a M4 IDS/IPS is, at a minimum, configured to generate an alert upon detection of any traffic that should have been blocked by the Gray Firewall. These alerts indicate a failure of the Gray Firewall's filtering functions and are evidence of either an improper configuration or a potential compromise. Management of the M4 IDS/IPS occurs from within the Gray Management Services.

Monitoring Multiple Points: Although the MA CP only requires monitoring two of the four points, customers are encouraged to monitor all four locations (see Section 8.1). Implementation of four separate components to monitor each point safeguards against malicious traffic from inadvertently being transferred to the Red Network.

Movement of network traffic from M3 to the Gray or Black Network is explicitly prohibited. Additionally, movement of network traffic from M2 and M4 to the Black Network is explicitly prohibited. The advantages of consolidated monitoring at all four points are fully realized when data from all devices is collected within the Red monitoring enclave using a CDS (see Section 8.5) and event correlation (see Section 8.6).

8.2 Log Data

The MA CP requires the implementation of a SIEM component within the Gray Management Services except in instances where an approved CDS is used to transport Gray security data to a Red SIEM. The Gray SIEM collects, aggregates, correlates, and analyzes security data from Gray Management Components, the Outer VPN, and Gray Firewall. The SIEM also provides alerts to auditors when anomalous behavior is detected.

The Gray SIEM is not permitted to collect logs from the Outer Firewall or M1 unless used in conjunction with an approved CDS. To protect the confidentiality and integrity of the data, all logs sent to the SIEM should be encrypted with TLS, SSH, or IPsec.

8.3 Network Flow Data

Network flow data (e.g., NetFlow, J-Flow, NetStream) is generated from network devices (e.g., routers, switches and standalone probes) and must be collected and analyzed to provide a picture of network

traffic flow and volume. Network flow data consists of IP protocols, source and destination IP addresses, and source and destination ports.

Monitoring network flow data requires establishing a baseline and updating it on a consistent basis. Network flow data should be reviewed regularly for systems generating excessive amounts of traffic, systems trying to connect to improper IP addresses, and systems trying to connect to closed ports on internal servers.

Network flow data can be collected from any network within the solution infrastructure. Network flow data from the Black Network can be collected from the Outer Firewall and sent to a Black Network collection server. Network flow data from the Gray Network must be collected from the Outer VPN Gateway or Gray Firewall and sent to a collection server in the Gray Management Services. Finally, network flow data can be collected from the Red Inner Firewall and sent to a collection server on the Red Network.

To maximize the effectiveness of collecting flow data from multiple network segments, all data should be centralized within the Red monitoring enclave for ingest into a single SIEM solution. Section 8.5 below outlines the various use-cases for implementing an approved CDS to move Black and Gray data to the Red Network.

8.4 Change Detection

One method of automating the detection of configuration changes without the complexity and expense of dedicated configuration management systems is to leverage the collection of syslog. In addition to collecting basic security events, the syslog facility is also capable of sending events related to system configuration changes. Queries, which generate alerts for administrators and auditors to review, can be developed on either the log collection server or the SIEM. Change detection is a required component of MA CP solutions (see Section 12.12).

8.5 Collection

This section provides a description of the primary sources for security event data and the recommended procedure for collecting data from the solution infrastructure.

Security event data includes, but is not limited to, syslog, IDS/IPS alerts, and network flow data. The syslog facility can be very broad and include security relevant events, configuration changes, health and status alerts, and other data that may prove useful when assembling the overall status of the security posture of a system. To protect the confidentiality and integrity of the data, all feeds should be encrypted with SSH, TLS, or IPsec.

Black Network Segment – The two key components within the Black Network segment are the Outer Firewall and the optional M1 monitoring point. The recommended solution would receive data from

both devices on a single data collection server and forward this data to the Gray collection server through an approved CDS.

Gray Network Segment – The key components within the Gray Network segment are the Outer VPN, Gray Firewall, the required M2 monitoring point, the optional M4 monitoring point, and the associated Gray Management Services.

This CP requires, at a minimum, that security data be sent directly to a SIEM located within the Gray Network. The Gray SIEM may receive data feeds from a central data collection server, as shown in Figure 12. The Gray SIEM is not permitted to collect data from the Black Network segment unless an approved CDS is used.

The recommended solution would receive data from all devices on a single data collection server and forward this data to the Red collection server through an approved CDS.

Red Network Segment – The key components within the Red Network segment vary based upon the services offered to EUDs, but must, at a minimum, include the Inner Firewall and the required M3 monitoring point. All security event data must be sent to a single collection server located within the Red monitoring enclave and may be fed into the Red SIEM solution; however, the Red SIEM is permitted to receive data flows directly from the Red components.

The recommended solution uses the Red SIEM to collect, aggregate, correlate, and analyze security data from all three boundaries (i.e., Black, Gray, and Red). The Red SIEM is not permitted to collect data from the Black or Gray segments unless an approved CDS is used.

8.6 CORRELATION

In order to support correlation of data from the Black, Gray, and Red components, the MA CP allows for the use of an approved CDS to feed the lower boundaries into the Red enclave. A Red SIEM should be located within an enclave protected from the larger enterprise of the Red Network (see Section 8.2).

9 KEY MANAGEMENT

Key Management Requirements have been relocated to a separate Key Management Requirements Annex.

10 REQUIREMENTS OVERVIEW

The following sections (Sections 11 through 15 and the Key Management Requirements Annex) specify requirements for implementations of MA solutions compliant with this CP. However, not all requirements in the following sections will apply to each compliant solution. Sections 10.1 and 10.2 describe how to determine which set of requirements applies to a particular solution. Key Management Requirements have been relocated to a separate Key Management Requirements Annex.

10.1 CAPABILITIES

This CP provides the flexibility needed to implement a variety of designs for the implementation of the MA solution. Although most requirements are applicable to all solutions, some requirements are only applicable to implementations whose high-level designs implement certain features. For example, requirements dealing with TLS EUDs do not include requirements for an Inner VPN Client. Table 3 lists the capabilities covered by this CP and the designators used in the requirements tables to refer to each.

Table 3. Capability Designators

Capability	Designator	Description
TLS Solution	T	Requirement that applies to the MA Solution that connects to the Red Network using IPsec as the Outer layer and TLS or SRTP as the Inner layer, as described in Section 6.3
VPN Solution	V	Requirement that applies to the MA solution that connects to the Red Network using two IPsec tunnels, as described in Section 6.2
TLS Infrastructure	TI	Requirement that applies specifically to the infrastructure associated with the TLS solution
VPN Infrastructure	VI	Requirement that applies specifically to the infrastructure associated with the VPN solution
TLS EUD	TE	Requirement that applies specifically to the EUD associated with the TLS solution
VPN EUD	VE	Requirement that applies specifically to the EUD associated with the VPN solution
All Solution Components	All	Requirement that applies to the EUD and to the Infrastructure, regardless if it is a VPN solution or a TLS solution
CDPs	C	Requirement that applies to the MA Solution that includes CDPs, as described in Key Management Requirements Annex.
Multiple Security Levels	MS	Requirement that applies to MA solution infrastructure which supports multiple security levels thorough the same Outer VPN Gateway
Wireless Connectivity to Dedicated Outer VPN	WC	Requirement that applies to EUDs which include a Dedicated Outer VPN and wireless connectivity to a Computing Device

Any solution that follows this CP must implement each applicable capability for their solution (e.g., all VPN EUD (V), VPN Infrastructure (VI), and VPN Solution (V) requirements for a solution supporting only VPN EUDs), and may implement multiple capabilities. The “Capabilities” column in the requirements tables in Sections 11 through 15 identifies which capabilities the requirement applies to. A requirement is only applicable to a solution if the “Capabilities” column for that requirement lists one or more of the capabilities being implemented by the solution.

10.2 Threshold and Objective Requirements

Multiple versions of a requirement may exist in this CP, with alternative versions designated as being either a Threshold requirement or an Objective requirement:

- A Threshold (T) requirement specifies a feature or function that provides the minimal acceptable capability for the security of the solution.
- An Objective (O) requirement specifies a feature or function that provides the preferred capability for the security of the solution.

In general, when separate Threshold and Objective versions of a requirement exist, the Objective requirement provides a higher degree of security for the solution than the corresponding Threshold requirement. However, in these cases, meeting the Objective requirement may not be feasible in some environments or may require components to implement features that are not yet widely available. Solution owners are encouraged to implement the Objective version of a requirement, but in cases where this is not feasible, solution owners may implement the Threshold version of the requirement instead. These Threshold and Objective versions are mapped to each other in the "Alternatives" column. Objective requirements that have no related Threshold requirement are marked as "Optional' in the "Alternatives" column.

In most cases, there is no distinction between the Threshold and Objective versions of a requirement. In these cases, the "Threshold/Objective" column indicates that the Threshold equals the Objective (T=O). Such requirements must be implemented in order to comply with this CP, as long as the requirement is applicable per Section 10.1.

Requirements that are listed as Objective in this CP may become Threshold requirements in a future version of this CP. Solution owners are encouraged to implement Objective requirements where possible in order to facilitate compliance with future versions of this CP.

10.3 Requirements Designators

Each requirement defined in this CP has a unique identifier consisting of the prefix "MA," a digraph that groups related requirements together (e.g., KM), and a sequence number (11). Table 4. Requirement Digraphs, lists the digraphs used to group together related requirements and identifies the sections in which those requirement groups can be found.

Table 4. Requirement Digraphs

Digraph	Description	Section	Table
PS	Product Selection Requirements	Section 11	Table 5
SR	Overall Solution Requirements	Section 12.1	Table 6
CR	Configuration Requirements for Inner and Outer VPN Components	Section 12.3	Table 11
IR	Inner VPN Component Requirements	Section 12.4	Table 12

Digraph	Description	Section	Table
OR	Outer VPN Component Requirements	Section 12.5	Table 13
MS	Multiple Security Level Requirements	Section 12.6	Table 14
TE	TLS-Protected Server & SRTP Endpoint Requirements	Section 12.7	Table 15
RD	Retransmission Device Requirements	Section 12.8	Table 16
WC	Wireless Connectivity to Dedicated Outer VPN Requirements	Section 12.9	Table 17
EU	End User Device Requirements	Section 12.10	Table 18
PF	Port Filtering Requirements for Solution Components	Section 12.11	Table 19
CM	Configuration Change Detection Requirements	Section 12.12	Table 20
DM	Device Management Requirements	Section 12.13	Table 21
MR	Continuous Monitoring Requirements	Section 8	Table 22
AU	Auditing Requirements	Section 12.15	Table 23
2F	Two-Factor Authentication	Section 12.17	Table 24
GD	Requirements for the Use and Handling of Solutions	Section 13.1	Table 25
RP	Incident Reporting Requirements	Section 13.2	Table 26
RB	Role-Based Personnel Requirements	Section 14	Table 27
TR	Test Requirements	Section 15.1	Table 28
KM	Key Management Requirements (See Key Management Requirements Annex)		

11 REQUIREMENTS FOR SELECTING COMPONENTS

In this section, a series of requirements are given for maximizing the independence between the components within the solution. This will increase the level of effort required to compromise this solution.

Table 5. Product Selection Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-PS-1	The products used for the Inner VPN Gateway must be chosen from the list of IPsec VPN Gateways on the CSfC Components List.	VI	T=O	
MA-PS-2	The products used for any Outer VPN Gateway must be chosen from the list of IPsec VPN Gateways on the CSfC Components List.	VI, TI	T=O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-PS-3	The products used for any Inner VPN Client must be chosen from the list of IPsec VPN Clients on the CSfC Components List.	VE	T=O	
MA-PS-4	The products used for any Outer VPN Client must be chosen from the list of IPsec VPN Clients on the CSfC Components List.	TE, VE	T=O	
MA-PS-5	The products used for the Inner and Outer CAs must either be chosen from the list of CAs on the CSfC Components List or the CAs must be pre-existing Enterprise CAs of the applicable network.	VI, TI	T=O	
MA-PS-6	Products used for Mobile Platform EUDs must be chosen from the list of Mobile Platforms on the CSfC Components List.	VE, TE	T=O	
MA-PS-7	Intrusion Prevention Systems (IPS) must be chosen from the list of IPS on the CSfC Components List.	VI, TI	O	Optional
MA-PS-8	Products used for the TLS Client must be chosen from the TLS Client sections (i.e., TLS Software Applications, VoIP Applications, Email Clients, Web Browsers, etc.) of the CSfC Components List.	TE	T=O	
MA-PS-9	Products used for the SRTP Client must be chosen from the list of VoIP Applications on the CSfC Components List.	TE	T=O	
MA-PS-10	If the solution is using a TLS-Protected Server, it must be chosen from the list of TLS-Protected Servers on the CSfC Components List.	TI	T=O	
MA-PS-11	If the solution is using a SIP Server, it must be chosen from the list of SIP Servers on the CSfC Components List.	TI	T=O	
MA-PS-12	If the solution is using a SRTP Endpoint, it must be chosen from the list of SRTP endpoints on the CSfC Components List.	TI	T=O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-PS-13	Products used for the Outer Firewall, Gray Firewall, and Inner Firewall must be chosen from the list of Stateful Traffic Filtering Firewalls (TFFW) on the CSfC Components List.	VI, TI	T=O	
MA-PS-14	If the solution is using a MDM, it must be chosen from the list of MDMs on the CSfC Components List.	VI, TI	T=O	
MA-PS-15	Withdrawn			
MA-PS-16	The Outer VPN Gateway and Inner Encryption endpoints must either come from different manufacturers, where neither manufacturer is a subsidiary of the other, or be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence.	VI, TI	T=O	
MA-PS-17	The Outer Firewall, Outer VPN Gateway, Gray Firewall, Inner Encryption Component, and Inner Firewall must use physically separate components, such that no component is used for more than one function (see Figure 1).	VI, TI	T=O	
MA-PS-18	The Outer VPN Gateway and the Inner Encryption endpoints must not use the same Operating System. Differences between Service Packs (SP) and version numbers for a particular vendor's OS do not provide adequate diversity.	VI, TI	T=O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-PS-19	The Inner and the Outer CAs must follow one of the following guidelines: • The CAs come from different manufacturers, where neither manufacturer is a subsidiary of the other. • The CAs are different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence. • The CAs use an Enterprise PKI approved by the AO.	VI, TI	O	Optional
MA-PS-20	The Gray Network Firewall and the Inner Encryption endpoints must either come from different manufacturers, where neither manufacturer is a subsidiary of the other, or be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence.	VI, TI	T=O	
MA-PS-21	The EUD's Outer VPN Component and Inner Encryption Components must either come from different manufacturers, where neither manufacturer is a subsidiary of the other, or be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence.	VE, TE	T=O	
MA-PS-22	The cryptographic libraries used by the Inner Tunnel CA and Outer Tunnel CA must either come from different manufacturers, where neither manufacturer is a subsidiary of the other, or be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence.	VI, TI	O	Optional

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-PS-23	The cryptographic libraries used by the Outer VPN Component and the Inner Encryption Components must either come from different manufacturers, where neither manufacturer is a subsidiary of the other, or be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence.	VE, TE	O	Optional
MA-PS-24	Each component that is selected from the CSfC Components List must go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO-approved Product Supply Chain Threat Assessment process (see CNSSD 505 SCRM for additional guidance).	All	T=O	
MA-PS-25	Components must be configured to use the NIAP-certified evaluated configuration.	All	T=O	
MA-PS-26	If the solution supports multiple security levels, the authentication server must be chosen from the list of authentication servers on the CSfC Components List.	MS	T=O	
MA-PS-27	If the solution uses a Dedicated Outer VPN as part of an EUD, it must be chosen from the list of IPsec VPN Gateways or IPsec VPN Clients on the CSfC Components List.	VE, TE	T=O	
MA-PS-28	If the solution uses a Dedicated Outer VPN as part of an EUD with wireless connectivity to a Computing Device, the Dedicated Outer VPN must be chosen from the list of WLAN Access Systems on the CSfC Components List.	WC	T=O	
MA-PS-29	Black Network Enterprise PKI is prohibited from being used as the Outer or Inner Tunnel CA.	All	T=O	

12 CONFIGURATION REQUIREMENTS

Once the products for the solution are selected, the next step is setting up the components and configuring them in a secure manner. This section consists of generic guidance for how to configure the components of the MA solution.

12.1 OVERALL SOLUTION REQUIREMENTS

Table 6. Overall Solution Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-SR-1	Network services provided by control plane protocols (such as DNS and NTP) must be located on the inside network (i.e., Gray Network for the Outer VPN Gateway and Red Network for the Inner Encryption Endpoints).	VI, TI	T=O	
MA-SR-2	The time of day on Inner Encryption Endpoints, Inner Firewall, and Red Management services must be synchronized to a time source located in the Red Network.	VI, TI	T=O	
MA-SR-3	The time of day on the Outer VPN Gateway, Gray Firewall, and Gray Management Services must be synchronized to a time source located in the Gray Management network.	VI, TI	T=O	
MA-SR-4	Default accounts, passwords, community strings, and other default access control mechanisms for all components must be changed or removed.	All	T=O	
MA-SR-5	All components must be properly configured in accordance with local policy and applicable U.S. Government guidance. In the event of conflict between the requirements in this CP and local policy, this CP takes precedence.	All	T=O	
MA-SR-6	Solution components must receive virus signature updates as required by the local agency policy and the AO.	All	T=O	
MA-SR-7	The only approved physical paths leaving the Red Network must be through a MA solution in accordance with this CP or via an AO-approved solution for protecting data in transit.[1]	All	T=O	

[1] In some cases, the customer will need to communicate with other sites that have NSA-certified Government off-the-Shelf (GOTS) solutions. In particular, it is acceptable for a given site to have both an egress path via an NSA-certified product solution and an egress path via a CSfC Solution conforming to a CP.

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-SR-8	When multiple Inner Encryption Components are placed between the Gray Firewall and Inner Firewall, they must be placed in parallel.	VI, TI	T=O	
MA-SR-9	Inner Encryption Components must not perform switching or routing for other Encryption Components.	VI, TI	T=O	
MA-SR-10	Infrastructure components must only be configured over an interface dedicated for management.	VI, TI	T=O	
MA-SR-11	DNS lookup services on network devices must be disabled.	All	O	Optional
MA-SR-12	DNS server addresses on infrastructure devices must be specified or DNS services must be disabled.	All	T=O	
MA-SR-13	Automatic remote boot-time configuration services should be disabled (e.g., automatic configuration via TFTP on boot).	All	T=O	

12.2 Configuration Requirements for All VPN Components

Table 7. Approved Commercial Algorithms (IPsec) for up to Top Secret

Security Service	Approved Algorithms	Specifications
Confidentiality (Encryption)	AES-256	FIPS PUB 197 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460
Authentication (Digital Signature)	RSA 3072 or, ECDSA over the curve P-384 with SHA-384	FIPS PUB 186-4 FIPS PUB 186-4 IETF RFC 6239 IETF RFC 6380 IETF RFC 6460
Key Exchange/ Establishment	ECDH over the curve P-384 (DH Group 20) or, Diffie-Hellman 3072	NIST SP 800-56A IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460 NIST SP 800-56A
Integrity (Hashing)	SHA-384	FIPS PUB 180-4 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460

Table 8. Approved Commercial Algorithms (TLS) for up to Top Secret

Security Service	TLS Cipher Suites	Specifications
TLS Cipher Suite	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 or TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 or TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	FIPS PUB 180-4 FIPS PUB 186-3 FIPS PUB 197 FIPS 800-56A IETF RFC 6460 IETF RFC 5246 IETF RFC 4492
Authentication (Digital Signature)	RSA 3072 or ECDSA over the curve P-384 with SHA-384	
Key Exchange	ECDHE over the curve P-384 (DH Group 20) or Diffie-Hellman 3072	

Table 9. Approved Commercial Algorithms for a Dedicated Outer VPN with Wireless Connectivity

Security Service	Algorithm Suite	Specifications
Confidentiality (Encryption)	AES-128-CCMP (Threshold) AES-256-GCMP (Objective)	FIPS PUB 197 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460
EAP-TLS Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (Threshold) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (Objective)	IETF RFC 5216 IETF RFC 5246

Table 10. Approved Commercial Algorithms (SRTP) for up to Top Secret

Security Service	Approved Algorithms	Specifications
Confidentiality (Encryption)	AES-256 in Counter Mode (CM)	IETF RFC 3711 IETF RFC 2675
Integrity	HMAC-SHA1	IETF RFC 3711 IETF RFC 2104
Key Exchange (using SIP Over TLS)	TLS-SDES or DTLS	IETF RFC 4568 IETF RFC 6347

12.3 Configuration Requirements For Inner and Outer VPN Components

Table 11. Configuration Requirements for Inner and Outer VPN Components

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-CR-1	The proposals offered by the Outer and Inner VPN Components in the course of establishing the IKE Security Association and the ESP SA for Inner and Outer Tunnels must be configured to only offer algorithm suite(s) containing the CNSA algorithms listed in Table 7.	All	T=O	
MA-CR-2	Default, self-signed, or proprietary device certificates, which are frequently preinstalled by the vendor, for any Outer and Inner VPN Component, must not be used for establishing SAs.	All	T	MA-CR-3
MA-CR-3	Default, self-signed, or proprietary device certificates, which are frequently preinstalled by the vendor, for any Outer and Inner VPN Component, must be removed.	All	O	MA-CR-2
MA-CR-4	Unique device certificates must be loaded onto the Outer and Inner VPN Gateway along with the corresponding Trust Anchor (signing) certificates.	VI, TI	T=O	
MA-CR-5	A device certificate must be used for each Outer and Inner VPN Component authentication during IKE.	All	T=O	
MA-CR-6	Authentication performed by Outer and Inner VPN Gateways must include a check that device certificates are authorized. This check may use a CRL, OCSP, or a whitelist.	VI, TI	T=O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-CR-7	Outer and Inner VPN Component authentication with device certificates must include a check that certificates are not expired.	All	T=O	
MA-CR-8	Withdrawn			
MA-CR-9	All IPsec connections must use IETF standards, IKE implementations (RFC 5996 or RFC 2409).	All	T=O	
MA-CR-10	All Outer and Inner VPN Components must use Cipher Block Chaining for IKE encryption.	All	T=O	
MA-CR-11	All Outer and Inner VPN Components must use Cipher Block Chaining for ESP encryption with a HMAC for integrity.	All	T	MA-CR-12
MA-CR-12	All Outer and Inner VPN Components must use Galois Counter Mode for ESP encryption.	All	O	MA-CR-11
MA-CR-13	All Outer and Inner VPN Components must set the IKE SA lifetime to at most 24 hours.	All	T=O	
MA-CR-14	All Outer and Inner VPN Components must set the ESP SA lifetime to at most 8 hours.	All	T=O	
MA-CR-15	All VPN Components must re-authenticate the identity of the VPN Component at the other end of the established tunnel before rekeying the IKE SA.	All	T=O	

12.4 Inner VPN Components

Table 12. Inner VPN Components Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-IR-1	The Inner VPN Component must use Tunnel Mode IPsec or Transport Mode IPsec using an associated IP tunneling protocol (e.g., Transport Mode IPsec with GRE).	VI	T=O	
MA-IR-2	The packet size for packets leaving the external interface of the Inner VPN Component must be configured to reduce packet fragmentation and impacting performance. This requires proper configuration of the Maximum Transmission Unit (MTU) (for IPv4) or Path MTU (PMTU) (for IPv6) and should consider Black Network and Outer VPN Component MTU/PMTU values to achieve this.	VI	O	Optional

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-IR-3	The Inner VPN Gateway must not allow any packets received on an interface connected to a Red Network to bypass encryption and be forwarded out through an interface connected to a Gray Network.	V	T	MA-IR-5
MA-IR-4	The Inner VPN Client of EUDs must encrypt all traffic, with the exception of traffic necessary for the EUD to connect to the physical network (e.g., DHCP) and locate the Inner VPN Gateway (i.e., DNS lookup of the VPN Component's IP address), in accordance with this CP.	VE	T=O	
MA-IR-5	The Inner VPN Component must not allow any packets received on an interface connected to a Gray Network to bypass decryption and be forwarded out through an interface connected to a Red Network.	V	T	MA-IR-7
MA-IR-6	The Inner VPN Gateway must use MAC policy to not allow any packets received on an interface connected to a Red Network to bypass encryption and be forwarded out through an interface connected to a Gray Network.	V	O	MA-IR-3
MA-IR-7	The Inner VPN Component must use MAC policy to not allow any packets received on an interface connected to a Gray Network to bypass decryption and be forwarded out through an interface connected to a Red Network.	V	O	MA-IR-5

12.5 Outer VPN Components

Table 13. Outer VPN Components Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-OR-1	Outer VPN Components must use Tunnel Mode IPsec.	All	T=O	
MA-OR-2	Outer VPN Components must not permit split-tunneling.	All	T=O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-OR-3	The Outer VPN Component must not allow any packets received on an interface connected to a Gray Network to bypass encryption and be forwarded out through an interface connected to a Black Network.	All	T	MA-OR-11
MA-OR-4	All traffic received by the Outer VPN Component on an interface connected to a Gray Network, with the exception of control plane traffic not prohibited in the CP, must have already been encrypted once.	All	T=O	
MA-OR-5	The Outer VPN Client of EUDs must encrypt all traffic, with the exception of traffic necessary for the EUD to connect to the physical network (e.g., DHCP) in accordance with this CP (see Section 4.1.4).	VE, TE	T=O	
MA-OR-6	If one or more virtual machines are used to separate Outer and Inner VPN Clients on an EUD then the Outer VPN Client must not run on the host operating system.	VE, TE	T=O	
MA-OR-7	Outer VPN Component must not allow any packets received on an interface connected to a Black Network to bypass decryption.	All	T	MA-OR-12
MA-OR-8	Withdrawn			
MA-OR-9	Outer VPN Gateways must not use routing protocols (e.g., OSPF, BGP).	VI, TI	T=O	
MA-OR-10	If a Dedicated Outer VPN is used it must be dedicated to a single security level and only provide the Outer layer of IPsec to Computing Devices connecting to a Red Network of the same security level.	VI, TI	T=O	
MA-OR-11	The Outer VPN Component must use MAC Policy to not allow any packets received on an interface connected to a Gray Network to bypass encryption and be forwarded out through an interface connected to a Black Network.	All	O	MA-OR-3
MA-OR-12	Outer VPN Component must use MAC policy to not allow any packets received on an interface connected to a Black Network to bypass decryption.	All	O	MA-OR-7

12.6 Multiple Security Level Requirements

The following section provides requirements for customers utilizing the same Outer VPN Gateway for multiple security levels as described in Section 4.2.4.

Table 14. Multiple Security Level Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-MS-1	The solution must include an authentication server in the Gray Management Network.	MS	T=O	
MA-MS-2	A unique device certificate must be loaded on the authentication server along with the corresponding CA (signing) certificate.	MS	T=O	
MA-MS-3	The EUD must establish an EAP-TLS session with the Outer VPN Gateway within IKE to exchange credentials.	MS	T=O	
MA-MS-4	The Outer VPN Gateway must act as an EAP pass-through and forward authentication packet between the EUD and authentication server.	MS	T=O	
MA-MS-5	Upon successful authentication the authentication server must send an Access Accept Radius or Diameter packet to the Outer VPN Gateway including an attribute for which network the EUD is associated.	MS	T=O	
MA-MS-6	The Outer VPN Gateway must use unique physical internal interfaces for each enclave of the solution (e.g., VLAN trunking of multiple enclaves is not permitted).	MS	T=O	
MA-MS-7	The Outer VPN Gateway must route EUD traffic over the appropriate interface and network based on the attribute provided by the authentication server in the Access Accept RADIUS or Diameter packet.	MS	T=O	
MA-MS-8	The Outer VPN Gateway must assign a Firewall ACL to EUDs based on the attribute information provided by the authentication server.	MS	T=O	
MA-MS-9	The EUD and Outer VPN Gateway must use TLS 1.2.	MS	T=O	
MA-MS-10	The EUD and authentication server must use X.509 device certificates for mutual authentication.	MS	T=O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-MS-11	The EUD and Outer VPN Gateway must only use ciphers suites selected from the "TLS Cipher Suite (Threshold)" row of Table 8.	MS	T	MA-MS-12
MA-MS-12	TLS Components must only use cipher suites selected from the "TLS Cipher Suite (Objective)" row of Table 8.	MS	O	MA-MS-11
MA-MS-13	Gray Network components must be physically protected to the level of the highest classified network.	MS	T=O	

12.7 TLS-Protected Server & SRTP Endpoint Requirements

Table 15. TLS-Protected Server & SRTP Endpoint Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-TE-1	TLS Components must use TLS 1.2 or later.	T	T=O	
MA-TE-2	TLS Solution Infrastructure components must terminate the Inner layer of encryption originating from TLS EUDs.	TI	T=O	
MA-TE-3	TLS Solution Infrastructure components must use X.509 device certificates for mutual authentication with TLS EUDs.	TI	T=O	
MA-TE-4	Default, self-signed, or proprietary certificates, which are frequently preinstalled by the vendor, for the TLS Component must be disabled.	T	T	MA-TE-5
MA-TE-5	Default, self-signed, or proprietary certificates, which are frequently preinstalled by the vendor, for the TLS Component must be removed.	T	O	MA-TE-4
MA-TE-6	Unique device certificates must be loaded onto TLS Components along with the corresponding Trust Anchor (signing) certificates.	T	T=O	
MA-TE-7	TLS Components must only use cipher suites selected from the "TLS Cipher Suite (Threshold)" row of Table 8.	T	T=O	
MA-TE-8	Withdrawn			
MA-TE-9	SRTP Components must only use algorithms selected from Table 10 that are approved to protect the highest classification level of the Red Network Data.	T	T=O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-TE-10	TLS Solution Infrastructure components must not allow any packets received on an interface connected to a Gray Network to bypass decryption and be forwarded out through an interface connected to a Red Network.	TI	T=O	

12.8 RETRANSMISSION DEVICE REQUIREMENTS

Table 16. Requirements for Retransmission Device

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-RD-1	An EUD must only connect to Retransmission Devices (RDs) authorized by a Government AO.	VE, TE	T=O	
MA-RD-2	A RD must provide EUDs with connectivity to the MA Solution infrastructure via any Black Network using Wi-Fi or an Ethernet cable.	VE, TE	T=O	
MA-RD-3	If the RD is configured to be a Wi-Fi access point, the Wi-Fi network must implement WPA2 PSK.	VE, TE	T=O	
MA-RD-4	A RD must not be used to protect Gray data between an Outer VPN Gateway and EUD.	VE, TE	T=O	
MA-RD-5	If the RD is configured to be a Wi-Fi access point using PSK, then the PSK must use a length of at least 64 hexadecimal characters (or its equivalent).	VE, TE	T	MA-RD-25
MA-RD-6	RD must only permit connections to devices on a Media Access Control (MAC) white list.	VE, TE	O	Optional
MA-RD-7	If the RD is configured as a Wi-Fi access point, then the PSK must not be displayed on the RD.	VE, TE	T=O	
MA-RD-8	If the RD is configured as a Wi-Fi access point, then the Service Set Identification (SSID) must not be displayed on the RD.	VE, TE	T=O	
MA-RD-9	If the RD is configured as a Wi-Fi access point, then the MAC address of connected devices must not be displayed on the RD.	VE, TE	T=O	
MA-RD-10	The Administrator password must not be displayed on the RD.	VE, TE	T=O	
MA-RD-11	The RD must display the number of currently connected devices.	VE, TE	O	Optional

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-RD-12	If the RD is configured to be a Wi-Fi access point, then Wi-Fi Protected Setup (WPS) must be disabled.	VE, TE	T=O	
MA-RD-13	The RD must be administered using HTTPS.	VE, TE	T=O	
MA-RD-14	The RD must require authentication with Administrator credentials to make changes to RD settings.	VE, TE	T=O	
MA-RD-15	The RD default Administrator credentials must be changed during provisioning.	VE, TE	T=O	
MA-RD-16	The RD must be configured to limit the number of connected devices to the minimum required for the mission.	VE, TE	T=O	
MA-RD-17	If the RD is configured as a Wi-Fi access point, then traffic of multiple EUDs sharing the RD must be separated (commonly referred to as Wi-Fi Privacy Separation or AP Isolation).	VE, TE	T=O	
MA-RD-18	If the RD is configured as a Wi-Fi access point, then the RD must disable broadcasting of the SSID.	VE, TE	O	Optional
MA-RD-19	The RD must only permit charging on USB ports and interfaces.	VE, TE	O	Optional
MA-RD-20	The RD must not permit connected EUDs to access files stored on the RD.	VE, TE	T=O	
MA-RD-21	The RD must require Administrator authentication prior to downloading logs or configuration files.	VE, TE	T=O	
MA-RD-22	The RD must only allow firmware updates signed by the RD manufacturer.	VE, TE	O	Optional
MA-RD-23	The RD must prevent the ability to boot into recovery mode.	VE, TE	O	Optional
MA-RD-24	The RD must require user or Administrator authentication prior to updating firmware.	VE, TE	O	Optional
MA-RD-25	If the RD is configured to be a Wi-Fi access point, the PSK must use a length of at least 96 hexadecimal characters (or its equivalent).	VE, TE	O	MA-RD-5
MA-RD-26	Withdrawn			
MA-RD-27	If the RD is configured to be a Wi-Fi access point, the Wi-Fi network must only use cipher suites selected from the "Dedicated Outer VPN and Wireless Network (Threshold)" row of Table 9.	VE, TE	T	MA-RD-28

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-RD-28	If the RD is configured to be a Wi-Fi access point, the Wi-Fi network must only use cipher suites selected from the "Dedicated Outer VPN and Wireless Network (Objective)" row of Table 9.	VE, TE	O	MA-RD-29
MA-RD-29	If the RD is connected to a Black Network which requires user interaction (e.g., captive portal wireless, 802.1X user authentication) the EUD must not be used to provide any input.	VE, TE	T=O	
MA-RD-30	Initial provisioning of the RD occurs in a physically secure area.	VE, TE	T=O	

12.9 Wireless Connectivity to Dedicated Outer VPN

The following section provides requirements for EUDs utilizing a Dedicated Outer VPN connected to the Computing Device over wireless.

Table 17. Requirements for Wireless Connectivity to Dedicated Outer VPN

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-WC-1	A Computing Device must only connect to a Dedicated Outer VPN authorized as part of the MA CP solution.	WC	T=O	
MA-WC-2	The Dedicated Outer VPN Wi-Fi Network must only use cipher suites selected from the "Dedicated Outer VPN and Wireless Network (Threshold)" row of Table 9.	WC	T	MA-WC-15
MA-WC-3	If the Dedicated Outer VPN is configured using WPA2 PSK, then the PSK must use a length of at least 64 hexadecimal characters (or its equivalent).	WC	T =O	
MA-WC-4	Withdrawn			
MA-WC-5	If the Dedicated Outer VPN is configured using WPA2 Enterprise, then mutual authentication must occur over the Outer IPsec tunnel between the Computing Device WLAN client and an authentication server in the Gray Management Network.	WC	T =O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-WC-6	If the Dedicated Outer VPN is configured using WPA2 Enterprise, the Computing Device WLAN Client must authenticate the identity of the authentication server by verifying that the authentication server's certificate is not expired and also chained to a trusted root CA certificate.	WC	T =O	
MA-WC-7	If the Dedicated Outer VPN is configured using WPA2 Enterprise, the Computing Device WLAN Client must be configured to authenticate only specific servers through setting the client to accept only a authentication server certificate that contains a particular Distinguished Name or Subject Alternate Name specific to one or more Dedicated Outer VPN (i.e., the client looks for the specified server name in the certificate during verification).	WC	T =O	
MA-WC-8	If the Dedicated Outer VPN is configured using WPA2 Enterprise, a unique device certificate must be loaded into the Computing Device WLAN Client along with the corresponding CA certificate chain, to include the trusted Root CA certificate.	WC	T=O	
MA-WC-9	The Computing Device WLAN Client must negotiate new session keys with the Dedicated Outer VPN at least once per hour.	WC	T=O	
MA-WC-10	The Computing Device WLAN Client must be prevented from using ad hoc mode (client-to-client connections).	WC	T=O	
MA-WC-11	The Computing Device WLAN Client must be prevented from using network bridging.	WC	T=O	
MA-WC-12	The Dedicated Outer VPN must only permit connections to Computing Devices on a MAC white list.	WC	T=O	
MA-WC-13	The Dedicated Outer VPN must prohibit management by Computing Devices connected over wireless.	WC	T=O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-WC-14	The Dedicated Outer VPN must comply with all requirements in Table 11. Configuration Requirements for Inner and Outer VPN Components and Table 13. Outer VPN Components Requirements.	WC	T=O	
MA-WC-15	The Dedicated Outer VPN Wi-Fi Network must only use cipher suites selected from the "Dedicated Outer VPN and Wireless Network Objective)" row of Table 9 Table 9.	WC	O	MA-WC-2
MA-WC-16	If the Dedicated Outer VPN is configured using WPA2 Enterprise, the authentication server must verify the WLAN Client certificate is 1) not expired; 2) not revoked; and 3) chains to a trusted Root CA certificate	WC	T=O	

12.10 End User Devices Requirements

Table 18. Requirements for End User Devices

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-EU-1	EUDs that do not implement a NSA-approved DAR solution and allow a user to store classified information on the EUD must be treated as classified at all times. (See Section 4.2.1).	TE, VE	T=O	
MA-EU-2	EUDs that implement a NSA-approved DAR solution (i.e., Data at Rest CP) must comply with the handling requirements specified for the DAR solution.	VE, TE	T=O	
MA-EU-3	Thin EUDs which prohibit a user from storing classified information must be treated as unclassified, or a higher classification level as determined by the AO, when powered down.	VE, TE	T=O	
MA-EU-4	The Outer VPN Client private key store must be separate from the private key store for the Inner VPN Client.	VE TE	T=O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-EU-5	The Inner and Outer VPN Clients on the EUD must be implemented on separate IP stacks. Implementations of IPv4 and IPv6 on the same operating system are considered to be part of the same IP stack.	VE	T=O	
MA-EU-6	If the EUD is not remotely administered, then it must only be updated and rekeyed through re-provisioning.	VE, TE	T=O	
MA-EU-7	The EUD must not allow split-tunneling.	VE, TE	T=O	
MA-EU-8	Rekeying of an EUD's certificates and associated private keys must be done through re-provisioning prior to expiration of keys.	VE, TE	T	MA-EU-9
MA-EU-9	Rekeying of an EUD's certificates and associated private keys must be done over the MA solution network prior to expiration of keys.	VE, TE	O	MA-EU-8
MA-EU-10	An EUD must be de-authorized from the network and submitted for Forensic Analysis if suspected of being compromised.	VE, TE	T=O	
MA-EU-11	An EUD must be destroyed if it has been determined to be compromised through Forensic Analysis.	VE, TE	T=O	
MA-EU-12	Users of EUDs must successfully authenticate themselves to the services they access on the Red Network using an AO-approved method.	VE, TE	T=O	
MA-EU-13	Red Network services must not transmit any classified data to EUDs until user authentication succeeds.	VE, TE	T=O	
MA-EU-14	Withdrawn			
MA-EU-15	All EUD Users must sign an organization-defined user agreement before being authorized to use an EUD.	VE, TE	T=O	
MA-EU-16	All EUD Users must receive an organization-developed training course for operating an EUD prior to use.	VE, TE	T=O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-EU-17	At a minimum, the organization-defined user agreement must include each of the following: • Consent to monitoring • Operations Security (OPSEC) guidance • Required physical protections to employ when operating and storing the EUD • Restrictions for when, where, and under what conditions the EUD may be used • Responsibility for reporting security incidents • Verification of IA Training • Verification of appropriate clearance • Justification for Access • Requester information and organization • Account Expiration Date • User Responsibilities	VE, TE	T=O	
MA-EU-18	EUDs must be dedicated for use solely in the MA solution, and not used to access any resources on networks other than the Red Network it communicates with through the two layers of encryption.	VE, TE	T=O	
MA-EU-19	EUDs must be remotely administered.	VE, TE	O	Optional
MA-EU-20	The EUD must disable all transmitted Global Positioning System (GPS) and location services except Enhanced 9-1-1 (E911) or those authorized by the AO.	VE, TE	T	MA-EU-60
MA-EU-21	The EUD must disable Firmware-Over-the-Air (FOTA) updates from the cellular carrier.	VE, TE	T=O	
MA-EU-22	The EUD must disable all wireless interfaces (e.g., Bluetooth, NFC, Cellular, 802.11) that do not pass through the Outer VPN component.	VE, TE	T	MA-EU-61
MA-EU-23	The EUD must disable processing of incoming cellular services including voice messaging services that do not pass through the VPN client.	VE, TE	T=O	
MA-EU-24	All EUDs must have their certificates revoked and resident image removed prior to disposal.	VE, TE	T=O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-EU-25	Passwords for user to device (EUD selected from Mobile Platform section of CSfC Components List) authentication must be a minimum of six alpha-numeric case sensitive characters.	VE, TE	T	MA-EU-65
MA-EU-26	Withdrawn			
MA-EU-27	For a VPN EUD that uses a Dedicated Outer VPN, the Dedicated Outer VPN must be the Outer layer of encryption and the VPN client on the Computing Device will be the Inner Layer of encryption.	VE	T=O	
MA-EU-28	Withdrawn			
MA-EU-29	If the EUD is using a Dedicated Outer VPN, the communication between the EUD and the Dedicated Outer VPN must be through a wired connection (i.e., Ethernet) or Wi-Fi using WPA2.	VE, TE	T=O	
MA-EU-30	Withdrawn			
MA-EU-31	If the EUD is using a Dedicated Outer VPN to connect over the Black Transport Network, the Dedicated Outer VPN must be used to establish the Outer layer of encryption.	VE, TE	T=O	
MA-EU-32	If a NSA-approved DAR Solution is not implemented on EUDs, the native platform DAR protection must be enabled.	VE, TE	T=O	
MA-EU-33	EUDs must use a unique X.509 v3 device certificate, signed by the Outer CA, for mutual authentication with Outer VPN Gateways.	VE, TE	T=O	
MA-EU-34	TLS EUDs must use a unique X.509 v3 device certificate or user certificate, signed by the inner CA, for mutual authentication with TLS-Protected Servers.	TE	T =O	
MA-EU-35	VPN EUDs must use a unique X.509 v3 device certificate, signed by the Inner CA, for mutual authentication with Inner VPN Gateways.	VE	T=O	
MA-EU-36	Withdrawn			
MA-EU-37	EUDs must be configured for all IP traffic, with the exception of IKE, network address configuration, time synchronization, and name resolution traffic required to establish the IPsec tunnel, to flow through the IPsec VPN Client.	VE, TE	T	MA-EU-38

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-EU-38	EUDs must be configured for all IP traffic, with the exception of IKE, to flow through the IPsec VPN Client.	VE, TE	O	MA-EU-37
MA-EU-39	The EUD password lifetime must be less than 181 days.	VE, TE	T=O	
MA-EU-40	The EUD screen must lock after three minutes or less of inactivity.	VE, TE	T=O	
MA-EU-41	The EUD must perform a wipe of all protected data after 10 or less authentication failures.	VE, TE	T=O	
MA-EU-42	VPN protection must be enabled across the EUD.	VE, TE	T=O	
MA-EU-43	A security policy (e.g., MAC policy, MDM policy) must be configured on the EUD specific to each permitted RD and/or Government Private Wireless Network.	VE, TE	T=O	
MA-EU-44	During provisioning, all unnecessary keys must be destroyed from the EUD secure key storage.	VE, TE	T=O	
MA-EU-45	During provisioning, all unnecessary X.509 certificates must be removed from the EUD Trust Anchor Database.	VE, TE	T=O	
MA-EU-46	All display notifications must be disabled while in a locked state.	VE, TE	O	Optional
MA-EU-47	USB mass storage mode must be disabled on the EUDs.	VE, TE	T=O	
MA-EU-48	USB data transfer must be disabled on the EUDs.	VE, TE	T=O	
MA-EU-49	Prior to updating the Application Processor system software, the system software digital signature must be verified by the EUD.	VE, TE	T=O	
MA-EU-50	Prior to installing new applications, the application digital signature must be verified.	VE, TE	T=O	
MA-EU-51	The EUD must connect to the Black Network through a Government Private Wireless Network, Government Private Cellular Network, Dedicated Outer VPN, or Retransmission Device.	VE, TE	T=O	
MA-EU-52	If the EUD is using a physically attached Dedicated Outer VPN or Retransmission Device, the Computing Device must not use Ethernet over USB.	VE, TE	O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-EU-53	If EUDs use Government Private Wireless Networks for black transport, the Government Private Wireless Network must be accredited by a Government AO.	VE, TE	T=O	
MA-EU-54	The end user must only be able to access the applications that are necessary for the EUDs intended purpose.	VE, TE	T	MA-EU-62
MA-EU-55	The end user must not be able to change security relevant settings on the EUD.	VE, TE	T	MA-EU-63
MA-EU-56	The EUD must not be able to directly access the Black Transport Network. All traffic must pass through the Outer VPN tunnel.	VE, TE	T=O	
MA-EU-57	USB debugging capabilities must be disabled on the EUDs.	VE, TE	T	MA-EU-64
MA-EU-58	All EUDs must display a consent prompt that requires users to accept prior to utilizing the device.	VE, TE	O	Optional
MA-EU-59	An EUD must implement a MAC policy.	VE, TE	O	Optional
MA-EU-60	The EUD must use MAC policy to disable all transmitted Global Positioning System (GPS) and location services except Enhanced 9-1-1 (E911) or those authorized by the AO.	VE, TE	O	MA-EU-20
MA-EU-61	The EUD must use MAC policy to disable all wireless interfaces (e.g., Bluetooth, NFC, Cellular, 802.11) that do not pass through the Outer VPN component.	VE, TE	O	MA-EU-22
MA-EU-62	MAC policy must limit applications to only those necessary for the EUDs intended purpose.	VE, TE	O	MA-EU-54
MA-EU-63	The EUD must use MAC policy to prevent end users from changing security relevant settings on the EUD.	VE, TE	O	MA-EU-55
MA-EU-64	MAC policy must disable USB debugging capabilities on the EUD.	VE, TE	O	MA-EU-57
MA-EU-65	Passwords for user to device (EUD selected from Mobile Platform section of CSfC Components List) authentication must be a minimum of 14 alpha-numeric case sensitive characters.	VE, TE	O	MA-EU-25
MA-EU-66	EUD must not use other Computing Devices as a source of power for charging.	VE, TE	T=O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-EU-67	EUDs must prohibit the use of removable media through configuration, policy, or physical modification.	VE, TE	T=O	

12.11 Port Filtering Requirements for Solution Components

Table 19. Port Filtering Requirements for Solution Components

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-PF-1	All components within the solution must have all network interfaces restricted to the smallest address ranges, ports, and protocols possible.	All	T=O	
MA-PF-2	All Components within the solution must have all unused network interfaces disabled.	All	T=O	
MA-PF-3	CDPs must only allow inbound HTTP traffic.	C	T=O	
MA-PF-4	For the Outer VPN Gateway interface connected to a Black Network, traffic filtering rules must be applied to both inbound and outbound traffic, such that only IKE, ESP, and control plane protocols (as defined in this CP) approved by organization-defined policy are allowed.	All	T=O	
MA-PF-5	For the Inner VPN Gateway interface connected to a Gray Network, traffic filtering rules must be applied to both inbound and outbound traffic, such that only IKE, ESP, and management and control plane protocols (as defined in this CP) approved by organization-defined policy are allowed.	VI	T=O	
MA-PF-6	The Inner Firewall must implement an ACL which only permits ingress/egress traffic from/to Inner Encryption endpoints.	All	T=O	
MA-PF-7	Any service or feature that allows an Outer VPN Gateway or an EUD to contact a third party server (such as one maintained by the manufacturer) must be blocked.	All	T	MA-PF-8
MA-PF-8	Any service or feature that allows an Outer VPN Gateway or an EUD to contact a third party server (such as one maintained by the manufacturer) must be disabled.	All	O	MA-PF-7

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-PF-9	Multicast messages received on any interfaces of the Outer VPN Gateway, Gray Firewall, and Inner encryption components must be dropped.	VI, TI	T=O	
MA-PF-10	For solutions using IPv4, the Outer VPN Gateway must drop all packets that use IP options.	All	O	Optional
MA-PF-11	For solutions using IPv4, the Outer VPN Gateway must only accept packets with Transmission Control Protocol (TCP), User Data Protocol (UDP), ESP, or ICMP in the IPv4 Protocol field and drop all other packets.	All	T=O	
MA-PF-12	For solutions using IPv6, the Outer VPN Gateway must only accept packets with ESP, TCP, UDP, or ICMPv6 in the IPv6 Next Header field and drop all other packets.	All	T=O	
MA-PF-13	For all Outer Firewall interfaces, traffic filtering rules must be applied to both inbound and outbound traffic, such that only IKE, ESP, and control plane protocols (as defined in this CP) approved by organization-defined policy are allowed.	VI, TI	T=O	
MA-PF-14	EUDs consisting of a single Computing Device must prohibit ingress and egress of Certificate Revocation traffic (e.g., OCSP queries, HTTP GET to CDPs) on the Black interface.	VE, TE	T=O	
MA-PF-15	EUDs consisting of a single computing device must prohibit ingress and egress of Name Resolution traffic (e.g., DNS query/response) on the Black Interface.	VE, TE	O	Optional
MA-PF-16	EUDs consisting of a single computing device must prohibit ingress and egress of NTP traffic on the Black Interface.	VE, TE	O	Optional
MA-PF-17	For all Outer Firewall interfaces, traffic filtering rules must be applied to both inbound and outbound traffic, such that only IKE, ESP, and control plane protocols (as defined in this CP) approved by organization-defined policy are allowed.	VI, TI	T=O	MA-PF-13

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-PF-18	Management plane traffic must only be initiated from the Gray administrative work stations with the exception of logging or authentication traffic which may be initiated from Outer VPN components.	VI, TI	T=O	
MA-PF-19	The Gray Firewall must only permit EUDs traffic to the Inner Encryption Component associated with the appropriate classification level.	VI, TI	T=O	
MA-PF-20	EUDs must prohibit ingress and egress of routing protocols.	VI, TI	T=O	

12.12 Configuration Change Detection Requirements

Table 20. Configuration Change Detection Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-CM-1	A baseline configuration for all components must be maintained by the Security Administrator and be available to the Auditor.	All	T=O	
MA-CM-2	An automated process must ensure that configuration changes are logged.	All	T=O	
MA-CM-3	All solution components must be configured with a monitoring service that detects all changes to configuration.	All	O	Optional

12.13 Device Management Requirements

Only authorized SAs will be allowed to administer the components. The MA solution will be used as transport for the Secure Shell v2 (SSHv2), IPsec, or TLS data from the administration workstation to the component.

Table 21. Requirements for Device Management

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-DM-1	Administration workstations must be dedicated for the purposes given in the CP and must be physically separated from workstations used to manage non-CSfC solutions.	VI, TI	T=O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-DM-2	The Inner Encryption endpoints must be managed from the Red Network and the Outer VPN Gateway and Gray Firewall must be managed from the Gray Network.	VI, TI	T=O	
MA-DM-3	A separate LAN or VLAN on the Red Network must be used exclusively for all management of Inner Encryption endpoints and solution components within the Red Network.	VI, TI	T=O	
MA-DM-4	A separate LAN or VLAN on the Gray Network must be used exclusively for all management of the Outer VPN Gateway, Gray Firewall, and solution components within the Gray Network.	VI, TI	T=O	
MA-DM-5	The Gray Management Network must not be directly connected to Non-Secure Internet Protocol Router Network (NIPRNet) or any other Unclassified Network not dedicated to the administration of CSfC solutions.	VI, TI	T=O	
MA-DM-6	All administration of solution components must be performed from an administration workstation remotely using a NSA approved solution (e.g., CP or Type 1 encryptor) or by managing the solution components locally.	VI, TI	T=O	
MA-DM-7	SAs must authenticate to solution components before performing administrative functions.	All	T	MA-DM-8
MA-DM-8	SAs must authenticate to solution components with CNSA-compliant certificates before performing administrative functions remotely.	All	O	MA-DM-7
MA-DM-9	SAs must establish a security policy for EUDs per the implementing organization's local policy to include procedures for continuous physical control.	VE, TE	T=O	
MA-DM-10	EUDs must generate logs and send to a central SIEM in the Red Network.	VE, TE	O	Optional
MA-DM-11	SAs must initiate CSRs for solution components as part of their initial keying within the solution.	All	T=O	
MA-DM-12	Devices must use Enrollment over Secure Transport (EST) as detailed in IETF RFC 7030 for certificate management.	All	O	Optional

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-DM-13	The same administration workstation must not be used to manage Inner Encryption Components and the Outer VPN Gateway.	VI, TI	T=O	
MA-DM-14	The Outer VPN Gateway and solution components within the Gray Network must forward log entries to a SIEM on the Gray Management Network (or SIEM in the Red Network if using a CDS) within 10 minutes of the events' occurrence.	VI, TI	T=O	
MA-DM-15	Inner Encryption Components and solution components within the Red Network must forward log entries to a SIEM on the Red Management Network within 10 minutes of the events occurrence.	VI, TI	T=O	
MA-DM-16	All logs forwarded to a SIEM on the Gray Management Network must be encrypted using SSHv2, IPsec, or TLS 1.2 or later.	All	O	Optional
MA-DM-17	All logs forwarded to a SIEM on a Red Management Network must be encrypted using SSHv2, IPsec, or TLS 1.2 or later.	All	O	Optional
MA-DM-18	Withdrawn			
MA-DM-19	The CSfC solution owner must identify authorized SAs to initiate certificate requests.	All	T=O	
MA-DM-20	Authentication of SAs must be enforced by either procedural or technical controls.	All	O	

12.14 Continuous Monitoring Requirements

Table 22. Continuous Monitoring Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-MR-1	Traffic from the Black, Gray, or Red Networks must be monitored from an IDS.	VI, TI	T	MA-MR-2
MA-MR-2	Traffic from the Black, Gray, or Red Networks must be monitored from an IPS.	VI, TI	O	MA-MR-1
MA-MR-3	An IDS must be deployed between the Outer VPN and Gray Firewall (M2) and inside the Inner Firewall (M3).	VI, TI	T	MA-MR-4 MA-MR-5 MA-MR-6

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-MR-4	An IDS must be deployed between the Outer Firewall and Outer VPN (M1), and between the Outer VPN and Gray Firewall (M2), and inside the Inner Firewall (M3), and between the Gray Firewall and Inner encryption gateway (M4).	VI, TI	O	MA-MR-3 MA-MR-5 MA-MR-6
MA-MR-5	An IPS must be deployed between the Outer VPN and Gray Firewall (M2) and inside the Inner Firewall (M3).	VI, TI	O	MA-MR-3 MA-MR-4 MA-MR-6
MA-MR-6	An IPS must be deployed between the Outer Firewall and Outer VPN (M1), and between the Outer VPN and Gray Firewall (M2), and inside the Inner Firewall (M3), and between the Gray Firewall and Inner encryption gateway (M4).	VI, TI	O	MA-MR-3 MA-MR-4 MA-MR-5
MA-MR-7	Each IDS in the solution must be configured to provide a dashboard or send alerts to the Security Administrator.	VI, TI	T	MA-MR-8
MA-MR-8	Each IPS in the solution must be configured to block malicious traffic flows and alert the Security Administrator.	VI, TI	O	MA-MR-7
MA-MR-9	Each IDS in the solution must be configured with rules that generate alerts upon detection of any unauthorized destination IP addresses.	VI, TI	T	MA-MR-10
MA-MR-10	Each IPS in the solution must be configured with rules that block and generate alerts upon detection of any unauthorized destination IP addresses.	VI, TI	O	MA-MR-9
MA-MR-11	Each IDS in the solution must be configured with rules that generate alerts upon detection of any unauthorized source IP addresses.	VI, TI	T	MA-MR-12
MA-MR-12	Each IPS in the solution must be configured with rules that block and generate alerts upon detection of any unauthorized source IP addresses.	VI, TI	O	MA-MR-11
MA-MR-13	A SIEM component must be placed within the Gray Network unless devices are configured to push events to a Red Network SIEM through an approved CDS.	VI, TI	T=O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-MR-14	The SIEM must be configured to send alerts to the Security Administrator when anomalous behavior is detected (i.e., blocked packets from the Outer VPN Gateway or Gray Firewall).	VI, TI	T=O	
MA-MR-15	The Gray SIEM must collect logs from the Outer VPN Gateway, Gray Firewall, and any components located within the Gray Management Services.	VI, TI	T=O	
MA-MR-16	Withdrawn			
MA-MR-17	The Gray SIEM must maintain an up to date table of Certificate Common Name and assigned IP address used for the Outer IPsec tunnel.	VI, TI	T=O	
MA-MR-18	The Gray SIEM must provide a dashboard or alert for EUDs attempting to establish a connection with the Outer VPN Gateway utilizing misconfigured VPN Client settings.	VI, TI	T=O	
MA-MR-19	The Gray SIEM must provide a dashboard or alert for three or more invalid login attempts in a 24 hour period to the Outer VPN Gateway or Gray Firewall.	VI, TI	T=O	
MA-MR-20	The Gray SIEM must provide a dashboard or alert of privilege escalations on the Outer VPN Gateway and Gray Firewall.	VI, TI	T=O	
MA-MR-21	The Gray SIEM must provide an alert or dashboard of configuration changes to the Outer VPN Gateway and Gray Firewall	VI, TI	T=O	
MA-MR-22	The Gray SIEM must provide an alert or dashboard of new accounts created on the Outer VPN Gateway, Gray Firewall, and any Gray authentication server.	VI, TI	T=O	
MA-MR-23	The Gray SIEM must provide an alert or dashboard for attempted IPsec connections to the Outer VPN Gateway which used an invalid certificate.	VI, TI	T=O	
MA-MR-24	The Gray SIEM must provide an alert, graph or table of blocked traffic at the Gray Firewall grouped by EUD Common Name.	VI, TI	T=O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-MR-25	The Gray SIEM must provide an alert or maintain a dashboard of DNS queries outside of expected values for IP addresses and domains.	VI, TI	O	Optional
MA-MR-26	Network flow data must be enabled on the Inner Firewall.	VI, TI	T=O	
MA-MR-27	A network flow data collector (e.g., SiLK, IPFlow, NetFlow Collector…) must be installed in the Red Network.	VI, TI	T=O	
MA-MR-28	A baseline for network flow data must be established.	VI, TI	O	Optional
MA-MR-29	A baseline for network flow data must be updated regularly at an interval determined by the AO.	VI, TI	O	Optional
MA-MR-30	Network flow data must be reviewed daily for: • Systems generating excessive amounts of traffic • Systems trying to connect to improper IP addresses • Systems trying to connect to closed ports on internal servers	VI, TI	O	Optional
MA-MR-31	Network flow data must be reviewed for systems generating excessive number of short packets (over 60% of packets containing 150 or less bytes).	VI, TI	O	Optional
MA-MR-32	Network flow data must be reviewed for excessive numbers of ICMP messages.	VI, TI	O	Optional

12.15 AUDITING REQUIREMENTS

Table 23. Auditing Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-AU-1	VPN Gateways must log establishment of a VPN tunnel.	TI, VI	T=O	
MA-AU-2	TLS-Protected Servers must log establishment of a TLS connection.	TI	T=O	
MA-AU-3	VPN Gateways must log termination of a VPN tunnel.	TI, VI	T=O	
MA-AU-4	TLS-Protected Servers must log termination of a TLS connection.	TI	T=O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-AU-5	VPN Clients must log establishment of a VPN tunnel.	VE, TE	O	Optional
MA-AU-6	TLS Clients must log establishment of a TLS tunnel	TE	O	Optional
MA-AU-7	VPN Clients must log termination of a VPN tunnel.	VE, TE	O	Optional
MA-AU-8	TLS Client must log termination of a TLS tunnel.	TE	O	Optional
MA-AU-9	Solution components must log all actions performed on the audit log (i.e., off-loading, deletion, etc.).	VI, TI	T=O	
MA-AU-10	Solution components must log all actions involving identification and authentication.	VI, TI	T=O	
MA-AU-11	Solution components must log attempts to perform an unauthorized action (i.e., read, write, execute, delete, etc.) on an object.	TI,VI	T=O	
MA-AU-12	Solution components must log all actions performed by a user with super-user or administrator privileges.	VI, TI	T=O	
MA-AU-13	Solution components must log escalation of user privileges.	VI, TI	T=O	
MA-AU-14	Solution components must log generation, loading, and revocation of certificates.	All	T=O	
MA-AU-15	Solution components must log changes to time.	VI, TI	T=O	
MA-AU-16	Each log entry must record the date and time of the event.	All	T=O	
MA-AU-17	Each log entry must include the identifier of the event.	All	T=O	
MA-AU-18	Each log entry must record the type of event.	All	T=O	
MA-AU-19	Each log entry must record the success or failure of the event to include failure code, when available.	All	T=O	
MA-AU-20	Each log entry must record the subject identity.	All	T=O	
MA-AU-21	Each log entry must record the source address for network-based events.	All	T=O	
MA-AU-22	Each log entry must record the user and, for role-based events, role identity, where applicable.	All	T=O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-AU-23	Auditors must detect when two or more simultaneous VPN connections from different IP addresses are established using the same EUD device certificate.	VI	O	Optional
MA-AU-24	Auditors must detect when two or more simultaneous TLS connections from different IP addresses are established using the same EUD device certificate.	TI	O	Optional
MA-AU-25	Upon notification of two or more simultaneous VPN connections from different IP addresses using the same EUD device certificate, the Certificate Authority Administrator must revoke the device certificate and provide an updated CRL to the Security Administrator.	V	O	Optional
MA-AU-26	Upon notification of two or more simultaneous TLS connections from different IP addresses using the same EUD device certificate, the CA Administrator must revoke the device certificate and provide an updated CRL to the Security Administrator.	T	O	Optional
MA-AU-27	The Security Administrator must immediately drop the session upon notification of two or more simultaneous VPN connections from different IP addresses using the same EUD device certificate.	V	O	Optional
MA-AU-28	The Security Administrator must immediately drop the session upon notification of two or more simultaneous TLS connections from different IP addresses using the same EUD device certificate.	T	O	Optional
MA-AU-29	VPN Gateways must log the failure to download a CRL from a CDP.	C	T=O	
MA-AU-30	TLS-Protected Servers must log the failure to download a CRL from a CDP.	C, TI	T=O	
MA-AU-31	VPN Gateways must log if the version of the CRL downloaded from a CDP is older than the current cached CRL.	C	T=O	
MA-AU-32	TLS-Protected Servers must log if the version of the CRL downloaded from a CDP is older than the current cached CRL.	C, TI	T=O	
MA-AU-33	VPN Gateways must log if signature validation of the CRL downloaded from a CDP fails.	C	T=O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-AU-34	TLS-Protected Servers must log if signature validation of the CRL downloaded from a CDP fails.	C, TI	T=O	
MA-AU-35	Auditors must compare and analyze collected network flow data against the established baseline on at least a daily basis.	VI, TI	T=O	
MA-AU-36	Locally-run CAs must comply with the audit and archival requirements defined in IETF RFC 3647 Sections 4.5.4 and 4.5.5, respectively.	VI, TI	T=O	
MA-AU-37	Locally-run CAs must comply with periodic audit and assessment requirements defined in IETF RFC 3647 Section 4.8.	VI, TI	T=O	
MA-AU-38	Audits and assessments for Outer and Inner CAs must be performed by personnel who are knowledgeable in the CAs' operations, as well as the CAs' CP and CPS requirements and processes, respectively.	VI, TI	T=O	

12.16 Key Management Requirements

Key Management Requirements have been relocated to a separate Key Management Requirements Annex.

12.17 Two Factor Authentication

Table 24. Two Factor Authentication Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-2F-1	The VPN EUD must implement a second authentication factor to prevent persistent access.	V	O	Optional
MA-2F-2	The second factor of authentication must use a physically separate token.	V, VI	O	Optional
MA-2F-3	The second factor of authentication must only be implemented on the Inner tunnel.	V, VI	O	Optional
MA-2F-4	The second factor of authentication must not be used as a replacement for the primary authentication method on the Inner layer of encryption.	V, VI	O	Optional
MA-2F-5	The second factor of authentication must implement a combined user generated password and a system generated one-time pass.	V, VI	O	Optional

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-2F-6	The management server for the second factor of authentication must be located in a Red Management services.	VI	O	Optional
MA-2F-7	The system generated one-time pass must implement a time-based algorithm.	V, VI	O	Optional
MA-2F-8	In the event of loss of continuous physical control the token must be considered compromised, reported to the AO/DAA, and must not be reused.	V	O	Optional
MA-2F-9	If the second factor of authentication's seed file is compromised, all tokens are considered compromised and must be replaced.	VI	O	Optional
MA-2F-10	During procurement, the vendor must not be permitted to store backups of seed files.	VI	O	
MA-2F-11	All seed files must be encrypted during transport.	VI	O	

13 REQUIREMENTS FOR SOLUTION OPERATION, MAINTENANCE, AND HANDLING

13.1 REQUIREMENTS FOR THE USE AND HANDLING OF SOLUTIONS

The following requirements must be followed regarding the use and handling of the solution.

Table 25. Use and Handling of Solutions Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-GD-1	All Solution Infrastructure components, with the exception of the Outer Firewall, must be physically protected as classified devices, classified at the level of the Red Network.	VI, TI	T=O	
MA-GD-2	Only authorized and appropriately cleared (or escorted) administrators and security personnel must have physical access to the solution Infrastructure components.	VI, TI	T=O	
MA-GD-3	Only authorized and appropriately cleared users, administrators, and security personnel must have physical access to EUDs when in a classified state.	VE, TE	T=O	
MA-GD-4	All components of the solution must be disposed of as classified devices, unless declassified using AO-approved procedures.	All	T=O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-GD-5	EUDs using a NSA-approved DAR solution must be disposed of in accordance with the disposal requirements for the DAR solution.	VE, TE	T=O	
MA-GD-6	All EUDs must have their certificates revoked prior to disposal.	VE, TE	T=O	
MA-GD-7	Users must periodically inspect the physical attributes of EUDs for signs of tampering or other unauthorized changes.	VE, TE	T=O	
MA-GD-8	Acquisition and procurement documentation must not include information concerning the purpose of the equipment.	All	T=O	
MA-GD-9	The solution owner must allow, and fully cooperate with, NSA or its authorized agent to perform an IA compliance audit (including, but not limited to, inspection, testing, observation, interviewing) of the solution implementation to ensure it meets the latest version of the MA CP.	All	T=O	
MA-GD-10	The AO will ensure that a compliance audit must be conducted every year against the latest version of the MA CP as part annual solution re-registration process.	All	T=O	
MA-GD-11	Results of the compliance audit must be provided to, and reviewed by, the AO.	All	T=O	
MA-GD-12	Customers interested in registering their solution against the MA CP must register with NSA and receive approval prior to operating the solution.	All	T=O	
MA-GD-13	The implementing organization must complete and submit a MA CP requirements compliance matrix to their respective AO.	All	T=O	
MA-GD-14	Registration and re-registration against the MA CP must include submission of MA CP registration forms and compliance matrix to NSA.	All	T=O	
MA-GD-15	When a new approved version of the MA CP is published by NSA, the AO must ensure compliance against this new CP within 6 months.	All	T=O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-GD-16	Solution implementation information, which was provided to NSA during solution registration, must be updated annually (in accordance with Section 15.3) as part of an annual solution re-registration process.	All	T=O	
MA-GD-17	Audit log data must be maintained for a minimum of 1 year.	All	T=O	
MA-GD-18	The amount of storage remaining for audit events must be assessed by the Security Administrator quarterly in order to ensure that adequate memory space is available to continue recording new audit events.	All	T=O	
MA-GD-19	Audit data must be frequently off-loaded to a backup storage medium.	All	T=O	
MA-GD-20	The implementing organization must develop a set of procedures to provide guidance for identifying and reporting security incidents associated with the audit events to the proper authorities and to the data owners.	All	T=O	
MA-GD-21	The implementing organization must develop a continuity of operations plan for auditing capability which includes a mechanism or method for determining when the audit log is reaching its maximum storage capacity.	All	T=O	
MA-GD-22	The implementing organization must develop a continuity of operations plan for auditing capability which includes a mechanism or method for off-loading audit log data for long-term storage.	All	T=O	
MA-GD-23	The implementing organization must develop a continuity of operations plan for auditing capability which includes a mechanism or method for responding to an overflow of audit log data within a product.	All	T=O	
MA-GD-24	The implementing organization must develop a continuity of operations plan for auditing capability which includes a mechanism or method for ensuring that the audit log can be maintained during power events.	All	T=O	
MA-GD-25	Strong passwords must be used that comply with the requirements of the AO.	All	T=O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-GD-26	The implementing organization must test and subsequently apply security critical patches to all components in the solution in accordance with local policy and this CP.	All	T=O	
MA-GD-27	Local policy must dictate how the Security Administrator will install patches to solution components.	All	T=O	
MA-GD-28	Solution components must comply with local TEMPEST policy.	All	T=O	
MA-GD-29	Software, settings, keys, and all other configuration data persistently stored on EUDs must be handled as controlled unclassified information or higher classification as designated by the AO.	All	T=O	
MA-GD-30	All hardware components must be tracked through an AO-approved inventory management process that identifies each component as part of a CSfC Solution.	All	T=O	
MA-GD-31	Users must maintain continuous physical control of the EUD as defined by local policy.	VE, TE	T=O	

Additional MA-GD requirements can be found in Section 14.

13.2 Requirements for Incident Reporting

Table 26. Incident Reporting Requirements, references requirements for reporting security incidents to NSA to be followed in the event that a solution owner identifies a security incident which affects the solution. These reporting requirements are intended to augment, not replace, any incident reporting procedures already in use within the solution owner's organization. It is critical that SAs, Certification Authority Administrators (CAAs), and Auditors are familiar with maintaining the solution in accordance with this CP. Based on familiarity with the known-good configuration of the solution, personnel responsible for the operations and maintenance of the solution will be better equipped to identify reportable incidents.

For the purposes of incident reporting, "malicious" activity includes not only events that have been attributed to activity by an adversary but also any events that are unexplained. In other words, an activity is assumed to be malicious unless it has been determined to be the result of known non-malicious activity.

This section only provides requirements directly related to the incident reporting process. See Section 12.14 for requirements supporting the detection of events that may reveal that a reportable incident has occurred.

Table 26. Incident Reporting Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-RP-1	Solution owners must report confirmed incidents meeting the criteria in MA-RP-3 through MA-RP-16 within 24 hours of detection via Joint Incident Management System (JIMS) or contacting NSA as specified in the CSfC Registration Letter issued for the solution.	All	T=O	
MA-RP-2	At a minimum, the organization must provide the following information when reporting security incidents: • CSfC Registration Number • Point of Contact (POC) name, phone, email • Alternate POC name, phone, email • Classification level of affected solution • Name of affected network(s) • Affected component(s) manufacturer/vendor • Affected component(s) model number • Affected component(s) version number • Date and time of incident • Description of incident • Description of remediation activities • Is Technical Support from NSA requested? (Yes/No)	All	T=O	
MA-RP-3	Solution owners must report a security failure in any of the CSfC solution components.	All	T=O	
MA-RP-4	Solution owners must report any evidence of a compromise or spillage of classified data caused by a failure of the CSfC Solution.	All	T=O	
MA-RP-5	For all Gray Network interfaces, solution owners must report any malicious inbound and outbound traffic.	All	T=O	
MA-RP-6	Solution owners must report any evidence of an unauthorized device/user gaining access to the classified network via the solution.	All	T=O	
MA-RP-7	Solution owners must report if a solution component sends traffic with an unauthorized destination address.	All	T=O	
MA-RP-8	Solution owners must report any malicious configuration changes to the components.	All	T=O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-RP-9	Solution owners must report any unauthorized escalation of privileges to any of the CSfC solution components.	All	T=O	
MA-RP-10	Solution owners must report if two or more simultaneous VPN connections from different IP addresses are established using the same EUD device certificate.	All	T=O	
MA-RP-11	Solution owners must report any evidence of malicious physical tampering with solution components.	All	T=O	
MA-RP-12	Solution owners must report any evidence that one or both of the layers of the solution failed to protect the data.	All	T=O	
MA-RP-13	Solution owners must report any significant degradation of services provided by the solution excluding connectivity issues associated with the Black Network.	All	T=O	
MA-RP-14	Solution owners must report malicious discrepancies in the number of VPN connections established by Outer VPN Gateways.	VI, TI	T=O	
MA-RP-15	Solution owners must report malicious discrepancies in the number of VPN connections established by the Inner VPN Gateway	VI	T=O	
MA-RP-16	Solution owners must report malicious discrepancies in the number of TLS connections established by the TLS-Protected Server	TI	T=O	

14 ROLE-BASED PERSONNEL REQUIREMENTS

The roles required to administer and maintain the solution are defined below, along with doctrinal requirements for these roles.

Information System Security Officer (ISSO) – The ISSO must be responsible for maintaining, monitoring, and controlling all security functions for the entire suite of products composing the MA solution. Security Administrator duties include but are not limited to the following:

1) Ensuring that the latest security-critical software patches and updates (such as Information Assurance Vulnerability Alerts (IAVAs)) are applied to each product.

2) Documenting and reporting security-related incidents to the appropriate authorities.

3) Coordinating and supporting product logistic support activities including integration and maintenance. Some logistic support activities may require that the Security Administrator escort uncleared personnel.

4) Employing adequate defenses of auxiliary network devices to enable proper and secure functionality of the MA solution.

5) Ensuring that the implemented MA solution remains compliant with the latest version of this CP as specified by MA-GD-15.

6) Provisioning and maintaining EUDs in accordance with this CP for implementations that include them.

Certification Authority Administrator (CAA) – The CAA must be responsible for maintaining, monitoring, and controlling all security functions for the CA products. CAA duties include but are not limited to the following:

1) Administering the CA, including authentication of all components requesting certificates.

2) Maintaining and updating CRLs.

3) Provisioning and maintaining EUD certificates in accordance with this CP for implementations that include them.

Auditor – The Auditor must be responsible for reviewing the actions performed by the Security Administrator and CAA and events recorded in the audit logs to ensure that no action or event represents a compromise to the security of the MA solution. Auditor duties include, but are not limited to, the following:

1) Reviewing, managing, controlling, and maintaining security audit log data.

2) Documenting and reporting security-related incidents to the appropriate authorities.

3) The Auditor will only be authorized access to Outer and Inner administrative components.

4) Develop, maintain and report System Audit Capability Survey.

Integrator – In certain cases, an external Integrator may be hired to implement a MA solution based on this CP. Integrator duties may include, but are not limited to:

1) Acquiring the products that compose the solution.

2) Configuring the MA solution in accordance with this CP.

3) Documenting, testing, and maintaining the solution.

4) Responding to incidents affecting the solution.

End User –An End User may operate an EUD from physical locations not owned, operated, or controlled by the government. The End User must be responsible for operating the EUD in accordance with this CP and an organization-defined user agreement. Remote User duties include, but are not limited to, the following:

1) Ensuring the EUD is only operated in physical spaces which comply with the end user agreement.

2) Alerting the Security Administrator immediately upon an EUD being lost, stolen, or suspected of being tampered with.

Security Administrator – The Security Administrator must be responsible for maintaining, monitoring, and controlling all security functions for the entire suite of products composing the MA Solution. In some organizations, the Security Administrator may be known as the Information System Security Officer. Security Administrator duties include, but are not limited to:

1) Ensuring that the latest security-critical software patches and updates (such as Information Assurance Vulnerability Alerts (IAVAs)) are applied to each product.

2) Documenting and reporting security-related incidents to the appropriate authorities.

3) Coordinating and supporting product logistic support activities including integration and maintenance. Some logistic support activities may require that the Security Administrator escort uncleared personnel.

4) Employing adequate defenses of auxiliary network devices to enable proper and secure functionality of the MA Solution.

5) Ensuring that the implemented MA Solution remains compliant with the latest version of this CP, as specified by MA-GD-15.

6) Provisioning and maintaining EUDs in accordance with this CP for implementations that include them.

Additional policies related to the personnel that perform these roles in a MA Solution are as follows:

Table 27. Role-Based Personnel Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-RB-1	The Security Administrator, CAAs, Auditor, EUD User, and Integrators must be cleared to the highest level of data protected by the solution. When an Enterprise CA is used in the solution, the CAA already in place may also support this solution, provided they meet this requirement. Black Network Administrators may be cleared at the Black Network classification level.	All	T=O	
MA-RB-2	The Security Administrator, CAA, and Auditor roles must be performed by different people.	All	T=O	
MA-RB-3	All SAs, CAAs, EUD Users, and Auditors must meet local Information Assurance (IA) training requirements.	All	T=O	
MA-RB-4	The CAA(s) for the Inner Tunnel CA must be different individuals from the CAA(s) for the Outer Tunnel CA.	All	O	Optional
MA-RB-5	Upon discovering an EUD is lost or stolen, an EUD User must immediately report the incident to their Security Administrator and CAA as well as any other reporting channels as dictated by organizational policy dictated by the AO.	VE, TE	T=O	
MA-RB-6	Upon notification of a lost or stolen EUD, the CAA must revoke that EUD's certificates.	All	T=O	
MA-RB-7	The Security Administrator(s) for the Inner Encryption endpoints and supporting components on Red Networks must be different individuals from the Security Administrator (s) for the Outer VPN Gateway and supporting components on Gray Networks.	VI, TI	T=O	
MA-RB-8	The Security Administrator(s) must periodically inspect the physical attributes of infrastructure hardware for signs of tampering or other unauthorized changes.	VI, TI	T=O	
MA-RB-9	The Auditor must review all log alerts and dashboards specified in this CP at least once a day.	All	T=O	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-RB-10	SAs must initiate the certificate revocation process prior to disposal of any solution component.	All	T=O	
MA-RB-11	Auditing of the Outer and Inner Tunnel CA operations must be performed by individuals who were not involved in the development of the CP and CPS, or integration the MA solution.	All	T=O	

15 INFORMATION TO SUPPORT THE AO

This section details items that likely will be necessary for the customer to obtain approval from the system AO. The customer and AO have obligations to perform the following:

- The customer, possibly with support from an Integrator, instantiates a solution implementation that follows the NSA-approved CP.
- The customer has a testing team develop a test plan and perform testing of the MA solution, see Section 15.1.
- The customer has system Assessment and Authorization performed using the risk assessment information referenced in Section 15.2.
- The customer provides the results from testing and system Assessment and Authorization to the AO for use in making an approval decision. The AO is ultimately responsible for ensuring that all requirements from the CP have been properly implemented in accordance with the CP.
- The customer registers the solution with NSA and re-registers yearly to validate its continued use as detailed in Section 15.3.
- Customers who want to use a variant of the solution detailed in this CP will contact their NSA Client Advocate to determine ways to obtain NSA approval.
- The AO will ensure that a compliance audit must be conducted every year against the latest version of the MA CP, and the results must be provided to the AO.
- The AO will ensure that certificate revocation information is updated on all the Solution Components in the solution in the case of a compromise.
- The AO will ensure that any Layer 2 or Layer 3 control plane protocols that are used in the solution are necessary for the operation of the network and that local policy supports their use.

- The AO will report incidents affecting the solution in accordance with Section 0.

The system AO maintains configuration control of the approved solution implementation over the lifecycle of the solution. Additionally, the AO must ensure that the solution remains properly configured with all required security updates implemented.

15.1 Solution Testing

This section provides a framework for a Test and Evaluation (T&E) plan and procedures to validate the implementation of a MA solution. This T&E will be a critical part of the approval process for the AO, providing a robust body of evidence that shows compliance with this CP.

The security features and operational capabilities associated with the use of the solution must be tested. The following is a general high-level methodology for developing the test plan and procedures and for the execution of those procedures to validate the implementation and functionality of the MA solution. The entire solution, to include each component described in Section 5 and 5.8, is addressed by this test plan including the following:

1) Set up the baseline network and configure all components.

2) Document the baseline network configuration. Include product model and serial numbers, software version numbers, and software configuration settings at a minimum.

3) Develop a test plan for the specific implementation using the test requirements from Table 28. Any additional requirements imposed by the local AO should also be tested, and the test plan must include tests to ensure that these requirements do not interfere with the security of this solution as described in this CP.

4) Perform testing using the test plan derived in Step 3. Network testing will consist of both Black box testing and Gray box testing. A two-person testing approach should be used to administer the tests. During test execution, security and non-security related discrepancies with the solution must be documented.

5) Compile findings, to include comments and vulnerability details as well as possible countermeasure information, into a Final Test Report to be delivered to the AO for approval of the solution.

The following testing requirement has been developed to ensure that the MA solution functions properly and meets the configuration requirements from Section 12. Testing of these requirements should be used as a minimum framework for the development of the detailed test plan and procedures.

Table 28. Test Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-TR-1	Requirement has been relocated to the Key Management Requirements Annex.			

15.2 Risk Assessment

The risk assessment of the MA solution presented in this CP focuses on the types of attacks that are feasible against this solution and the mitigations that can be employed. Customers should contact their NSA Client Advocate to request this document, or visit the Secret Internet Protocol Router Network (SIPRNet) CSfC site for information. The process for obtaining the risk assessment is available on the SIPRNet CSfC website. The AO must be provided a copy of the NSA risk assessment for their consideration in approving the use of the solution.

15.3 Registration of Solutions

All customers using CSfC solutions to protect information on National Security Systems must register their solution with NSA prior to operational use. This registration will allow NSA to track where MA CP solutions are instantiated and to provide the AOs at those sites with appropriate information, including any significant vulnerabilities that may be discovered in components or high-level designs approved for these solutions. The CSfC solution registration process is available at http://www.nsa.gov/resources/everyone/csfc.

Solution registrations are valid for one year from the date the solution registration is approved, at which time customers are required to re-register their solution in order to continue using it. Approved CPs will be reviewed twice a year, or as events warrant. Registered users of this CP will be notified when an updated version is published. When a new version of this CP that has been approved by the Deputy National Manager for National Security Systems is published, customers will have six months to bring their solutions into compliance with the new version of the CP and re-register their solution (see requirement MA-GD-15). Customers are also required to update their registrations whenever the information provided on the registration form changes.

APPENDIX A. GLOSSARY OF TERMS

Authorization (To Operate) – The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. (NIST SP 800-37)

Authorization Boundary – All components of an information system to be authorized for operation by an AO and excludes separately authorized systems, to which the information system is connected.

Authorizing Official – A senior (Federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Authorizing Official Designated Representative – An organizational official acting on behalf of an AO in carrying out and coordinating the required activities associated with security authorization.

Authorization Package – A security package of documents consisting of the security control assessment that provides the AO with essential information needed to make a risk-based decision on whether to authorize operation of an information system or a designated set of common controls.

Assurance – Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. (CNSSI 4009)

Audit – The activity of monitoring the operation of a product from within the product. It includes monitoring of a product for a set of pre-determined events. Each audit event may indicate rogue behavior, or a condition that is detrimental to security, or provide necessary forensics to identify the source of rogue behavior.

Audit Log – A chronological record of the audit events that have been deemed critical to security. The audit log can be used to identify potentially malicious activity that may further identify the source of an attack, as well as potential vulnerabilities where additional countermeasures or corrective actions are required.

Availability – Ensuring timely and reliable access to and use of information. (NIST SP 800-37).

Black Box Testing – Testing the functionality of a component of the solution, such that testing is limited to the subset of functionality that is available from the external interfaces of the box during its normal operational configuration without any additional privileges (such as given to the Security Administrator or Auditor).

Black Network – A network that contains classified data that has been encrypted twice. (See Section 4.1.3)

CP – The set of guidance provided by NSA that describes recommended approaches to composing COTS components to protect classified information for a particular class of security problem. CP instantiations are built using products selected from the CSfC Components List.

Central Management Site – A site within a MA solution that is responsible for remotely managing the solution components located at other sites (see Section 4.2.3).

Certification Authority (CA) – An authority trusted by one or more users to create and assign certificates. (ISO9594-8)

Certificate Policy (CP) – A named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range. (IETF RFC 3647)

Committee on National Security Systems Policy No. 15 (CNSSP-15) – Policy specifies which public standards may be used for cryptographic protocol and algorithm interoperability to protect National Security Systems (NSS).

Computing Device – An EUD such as a phone, laptop, or tablet.

Confidentiality – Assurance that the data stored in, processed by, or transmitted by the system are protected against unauthorized disclosure, and confidence that only the appropriate set of individuals or organizations would be provided the information.

Control Plane Protocol – A routing, signaling, or similar protocol whose endpoints are network infrastructure devices such as VPN Gateways or routers. Control plane protocols carry neither user data nor management traffic.

CRL Distribution Point (CDP) – A web server that hosts a copy of a CRL issued by a CA for VPN Components to download (see Key Management Requirements Annex).

Cross Domain Solution (CDS) – A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains. (CNSSI 4009)

Data Plane Protocol – A protocol that carries the data being transferred through the solution.

Dedicated Outer VPN - A dedicated piece of hardware that can be part of an EUD and terminates the Outer layer of IPsec encryption.

End User Device (EUD) – A form-factor agnostic component of the MA solution that can include a mobile phone, tablet, or laptop computer. EUDs can be composed of multiple components to provide physical separation between layers of encryption (see Section 4.2.1 for explanation of detailed differences between VPN EUD and TLS EUD solution design options).

External Interface – The interface of the Outer VPN Gateway that connects to the internal interface of the Outer Firewall.

Factory Reset - Removal of user data and any applications not already installed by the vendor. Malicious executables, at the application layer, may still be present after a factory reset.

Federal Information Processing Standards (FIPS) – A set of standards that describe the handling and processing of information within governmental agencies.

Gray Box Testing – The ability to test functionality within a component of the solution, such that full management privileges are granted (i.e., knowing passwords for Security Administrator and Auditor and access to the capabilities associated with those privileges). In addition, the use of any and all testing equipment and/or testing software used inside and outside the developed solution is available.

Gray Network – A network that contains classified data that has been encrypted once (see Section 4.1.2).

Gray Firewall – A stateful traffic filtering firewall placed on the Gray Network to provide filtering of ports, protocols, and IP addresses to ensure traffic reaches the correct Inner Encryption endpoint or is dropped.

Internal Interface – The interface on a VPN Gateway or Inner Encryption Component that connects to the Inner network (i.e., the Gray Network on the Outer VPN Gateway or the Red Network on the Inner Encryption Component).

Locally Managed Device – A device that is being managed by the direct connection of the Administration Workstation to the device in a hardwired fashion (such as a console cable).

Malicious – Any unauthorized events that are either unexplained or in any way indicate adversary activity.

Management Plane Protocol – A protocol that carries either traffic between an ISSO and a component being managed, or log messages from a solution component to a SIEM or similar repository.

Protection Profile – A document used as part of the certification process according to the Common Criteria. As the generic form of a security target, it is typically created by a user or user community and provides an implementation independent specification of information assurance security requirements.

Public Key Infrastructure (PKI) – Framework established to issue, maintain, and revoke public key certificates.

Registration Authority (RA) – An entity authorized by the CA to collect, verify, and submit information that is to be entered into public key certificates. The term RA refers to hardware, software, and individuals that collectively perform this function.

Red Network - Contains only Red data and is under the control of the solution owner or a trusted third party. The Red Network begins at the internal interface(s) of Inner Encryption Components located between the Gray Firewall and Inner Firewall.

Remotely Managed Device – A device that is being managed by any other method besides that given in the definition of a Locally Managed Device.

Retransmission Device (RD) – A standalone piece of hardware used to provide Black Network connectivity to EUDs.

Security Level – The combination of classification level, list of compartments, dissemination controls, and other controls applied to the information within a network.

Split-tunneling – Allows network traffic to egress through a path other than the established VPN tunnel (either on the same interface or another network interface). Split tunneling is explicitly prohibited in MA CP compliant configurations (see MA-OR-2 and MA-EU-7).

SRTP Client – A component on the EUD that facilitates encryption for voice communications.

TLS Client – A component on a TLS EUD that can provide the Inner layer of data in transit encryption.

TLS Component – Refers to both TLS Clients and TLS-Protected Servers.

VPN Client – A VPN application installed on an EUD.

VPN Component – The term used to refer to VPN Gateways and VPN Clients.

VPN Gateway – A VPN device physically located within the VPN infrastructure.

VPN Infrastructure – Physically protected in a secure facility and includes Inner and Outer VPN Gateways, Certificate Authorities, and Administration Workstations, but does not include EUDs.

Wipe – Removal of all user data, applications, and operating system.

APPENDIX B. ACRONYMS

Acronym	Definition
ACL	Access Control List
AES	Advanced Encryption Standard
AO	Authorizing Official
APN	Access Point Name
ARP	Address Resolution Protocol
BIOS	Basic Input/Output System
BGP	Border Gateway Protocol
CA	Certification Authority
CAA	Certification Authority Administrator
CDP	CRL Distribution Point
CDS	Cross Domain Solution
CNSA	Commercial National Security Algorithm
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COTS	Commercial Off-the-Shelf
CP	Certificate Policy
CP	Capability Package
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CRS	Certificate Signing Request
CSfC	Commercial Solutions for Classified
CUI	Controlled Unclassified Information
DAR	Data-At-Rest
DDoS	Distributed Denial of Service
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DM	Device Management
DN	Domain Name
DNS	Domain Name System
DoD	Department of Defense
DoE	Department of Energy
DoS	Denial of Service
DSA	Digital Signature Algorithm
DNM	Deputy National Manager for National Security Systems
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload
EST	Enrollment Over Secure Transport

Acronym	Definition
EUD	End User Device
FDE	Full Disk Encryption
FIPS	Federal Information Processing Standards
FOTA	Firmware Over The Air
GOTS	Government Off-the-Shelf
GRE	Generic Routing Encapsulation
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAVA	Information Assurance Vulnerability Alert
ICMP	Internet Control Message Protocol
ICT	Information Communication Technology
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IS-IS	Intermediate System to Intermediate System
KM	Key Management
MA	Mobile Access
MDF	Mobile Device Fundamentals
MDM	Mobile Device Manager
MOA	Memorandum of Agreement
MLD	Multicast Listener Discovery
MTU	Maximum Transmission Unit
NDP	Neighbor Discovery Protocol
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NPE	Non Person Entity
NSA	National Security Agency
NSS	National Security Systems
NTP	Network Time Protocol
O	Objective
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OPSEC	Operational Security
OS	Operating System
OSI	Open System Interconnection

Acronym	Definition
OSPF	Open Shortest Path First
PKCS	Public Key Cryptographic Standard
PKI	Public Key Infrastructure
PMTU	Path Maximum Transmission Unit
POC	Point of Contact
PSK	Pre-shared Key
PTP	Precision Time Protocol
RADIUS	Remote Authentication Dial-In User Service
RD	Retransmission Device
RFC	Request for Comment
RIP	Routing Information Protocol
RSA	Rivest Shamir Adelman algorithm
SCRM	Supply Chain Risk Management
SDES	Session Description Protocol Security Descriptions
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Manager
SIP	Session Initiation Protocol
SIPRNet	Secret Internet Protocol Router Network
SP	Service Packs
SRTP	Secure Real-Time Protocol
SSH	Secure Shell
SSHv2	Secure Shell Version 2
T	Threshold
T&E	Test and Evaluation
TCP	Transmission Control Protocol
TFFW	Traffic Filtering Firewall
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VDI	Virtual Desktop Infrastructure
VoIP	Voice over Internet Protocol
VM	Virtual Machine
VPN	Virtual Private Network
VSA	Vendor Specific Attribute
WLAN	Wireless Local Area Network
WPA2	Wi-Fi Protected Access II

APPENDIX C. REFERENCES

Document	Title	Date
CNSSI 1300	*CNSSI 1300, National Security Systems Public Key Infrastructure X.509 Certificate Policy*	December 2014
CNSSI 4009	*CNSSI 4009, National Information Assurance (IA) Glossary Committee for National Security Systems.* http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf	April 2015
CNSSP 15	*CNSS Policy (CNSSP) Number 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems Committee for National Security Systems*	October 2016
CNSSD 505	*CNSS Directive (CNSSD) Number 505, Supply Chain Risk Management (SCRM)*	March 2012
FIPS 140	*Federal Information Processing Standard 140, Security Requirements For Cryptographic Modules National Institute for Standards and Technology FIPS Publication* http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf	May 2001
FIPS 180	*Federal Information Processing Standard 180-4, Secure Hash Standard (SHS)*	March 2012
FIPS 186	*Federal Information Processing Standard 186-4, Digital Signature Standard (DSS)*	July 2013
FIPS 197	*Federal Information Processing Standard 197, Advanced Encryption Standard (AES)*	November 2001
FIPS 201	*Federal Information Processing Standard 201, Personal Identity Verification (PIV) of Federal Employees and Contractors National Institute for Standards and Technology FIPS Publication* http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf	March 2006
IPsec VPN Client PP	*Protection Profile for IPsec Virtual Private Network (VPN) Clients*. http://www.niap-ccevs.org/pp	January 2012
NSA Suite B	*NSA Guidance on Suite B Cryptography (including the Secure Sharing Suite (S3))*. http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml	November 2010
RFC 2409	*IETF RFC 2409 The Internet Key Exchange (IKE)*. D. Harkins and D. Carrel.	November 1998
RFC 3647	*IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* Internet Engineering Task Force	November 2003
RFC 3711	*IETF RFC 3711 The Secure Real-Time Transport Protocol (SRTP).* M. Baugher and D. McGrew.	March 2004
RFC 4252	*IETF RFC 4252 The Secure Shell (SSH) Authentication Protocol*. T. Ylonen and C. Lonvick.	January 2006

Document	Title	Date
RFC 4253	*IETF RFC 4253 The Secure Shell (SSH) Transport Layer Protocol*. T. Ylonen and C. Lonvick.	January 2006
RFC 4254	*IETF RFC 4254 The Secure Shell (SSH) Connection Protocol*. T. Ylonen and C. Lonvick.	January 2006
RFC 4256	*IETF RFC 4256 Generic Message Exchange Authentication for the Secure Shell Protocol (SSH)*. F. Cusack and M. Forssen.	January 2006
RFC 4302	*IETF RFC 4302 IP Authentication Header*. S. Kent	December 2005
RFC 4303	*IETF RFC 4303 IP Encapsulating Security Payload*. S. Kent	December 2005
RFC 4307	*IETF RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*. J. Schiller	December 2005
RFC 4308	*IETF RFC 4308 Cryptographic Suites for IPsec*. P. Hoffman	December 2005
RFC 4492	*IETF RFC 4492 Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS).* S. Blake-Wilson, N. Bolyard, V. Gupta, C. Hawk Corriente, B. Moeller, and Ruhr-Uni Bochum.	May 2006
RFC 4754	*IETF RFC 4754 IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)*. D. Fu and J. Solinas.	January 2007
RFC 5246	*IETF RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2*. T. Dierks and E. Rescorla.	August 2008
RFC 5280	*IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. D. Cooper, et. al.	May 2008
RFC 5759	*IETF RFC 5759 Suite B Certificate and Certificate Revocation List (CRL) Profile*. J. Solinas and L. Zieglar.	January 2010
RFC 5996	*IETF RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2)*. C. Kaufman, et. al.	September 2010
RFC 6188	*IETF RFC 6188 The Use of AES 192 and AES 256 in Secure RTP.* D. McGrew.	March 2011
RFC 6239	*IETF RFC 6239 Suite B Cryptographic Suites for Secure Shell (SSH)*. K. Igoe.	May 2011
RFC 6379	*IETF RFC 6379 Suite B Cryptographic Suites for IPsec*. L. Law and J. Solinas.	October 2011
RFC 6380	*IETF RFC 6380 Suite B Profile for Internet Protocol Security (IPsec)*. K. Burgin and M. Peck.	October 2011
RFC 6460	*IETF RFC 6460 Suite B Profile for Transport Layer Security (TLS)*. M. Salter and R. Housley.	January 2012
RFC 6818	*IETF RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. P. Yee	January 2013

Document	Title	Date
RFC 7030	*IETF RFC 7030 Enrollment over Secure Transport*. M. Pritikin, P. Yee, and D. Harkins.	October 2013
SP 800-53	*NIST Special Publication 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations*. Joint Task Force Transformation Initiative.	April 2013
SP 800-56A	*NIST Special Publication 800-56A Rev. 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*. E. Barker, et. al.	May 2013
SP 800-56B	*NIST Special Publication 800-56B, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*. E. Barker, et. al.	August 2009
SP 800-56C	*NIST Special Publication 800-56C, Recommendation for Key Derivation through Extraction-then-Expansion*. L. Chen.	November 2011
SP 800-131A	*NIST Special Publication 800-131A, Recommendation for Transitioning of Cryptographic Algorithms and Key Lengths*. E. Barker.	January 2011
SP 800-147	*NIST Special Publication 800-147, BIOS Protection Guidelines*. D. Cooper, et al.	April 2011

APPENDIX D. END USER DEVICE IMPLEMENTATION NOTES

VPN EUDs:

The VPN EUD can be set up using a Computing Device with the user's applications, an Inner VPN Component, and an Outer VPN Component. The Inner VPN Component is a VPN Client residing on the same Computing Device as the user's applications. The Outer VPN Component can be a Dedicated Outer VPN Component or be a VPN Client on the same Computing Device as the user's applications (as shown in Figure 11). If a Dedicated Outer VPN component is used it must be connected to the Computing Device using Ethernet or wireless WPA2. When the Dedicated Outer VPN provides wireless connectivity to the Computing Device, the requirements in Section 12.9 must be followed as shown in Table 17. Requirements for Wireless Connectivity to Dedicated Outer VPN. If all components are on the same device, virtual machines will be required to provide separate IP stacks for the Inner and Outer VPN Clients as noted in Figure 11. A RD will also be required in this case, unless, as noted in Section 4.1.3, the connection is to a Government Private Wireless Network or a Government Private Cellular Network. See Figure 12.

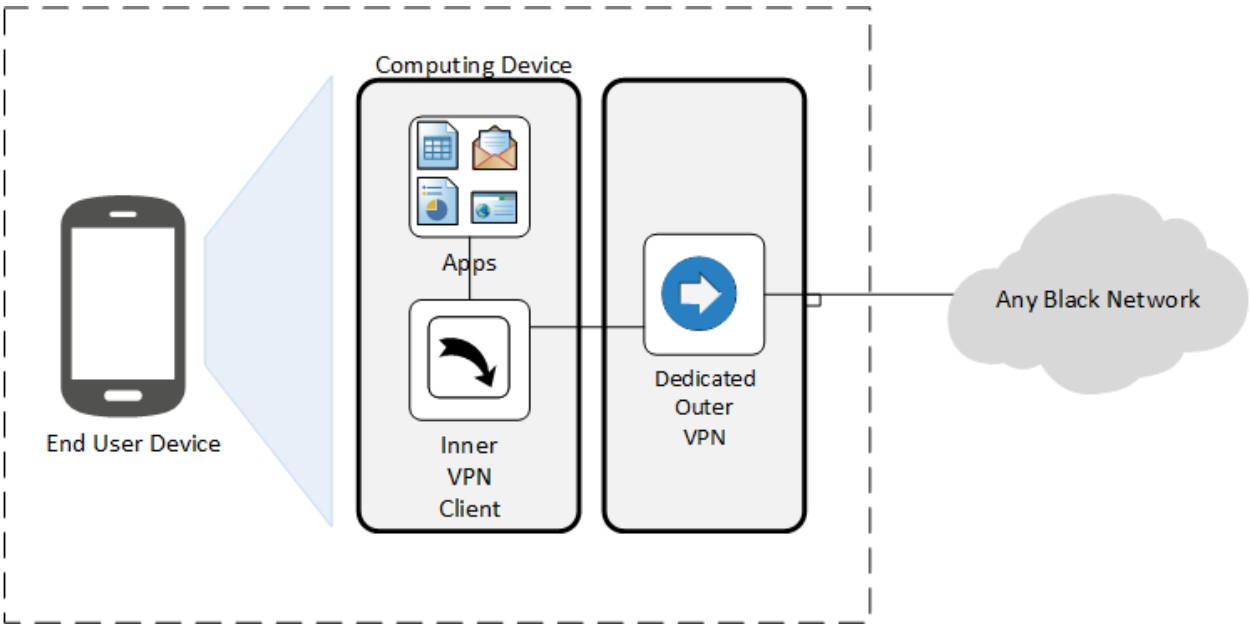

Figure 10. VPN EUD with Inner VPN Client and Separate Outer VPN Gateway

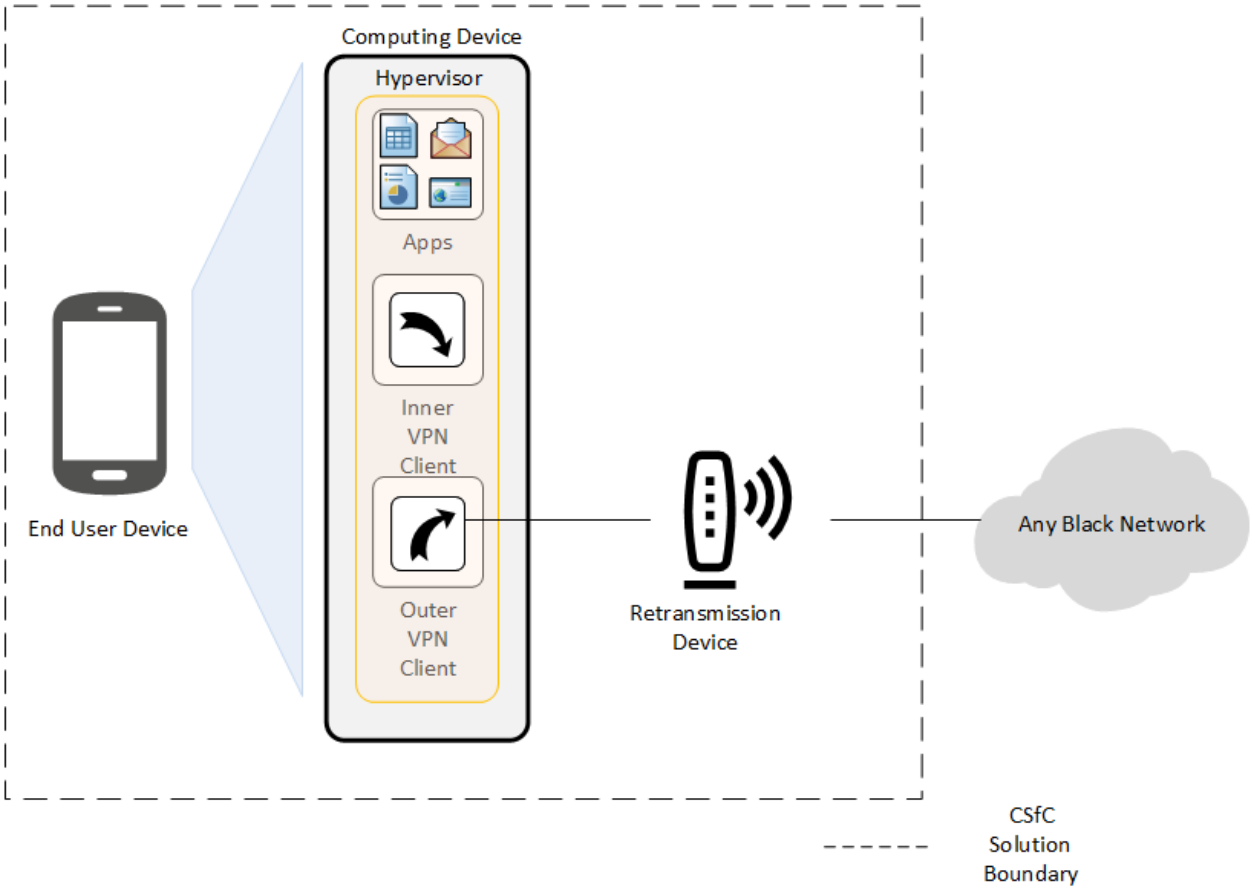

Figure 11. VPN EUD with Inner and Outer VPN Clients in Separate Virtual Machines with Retransmission Device

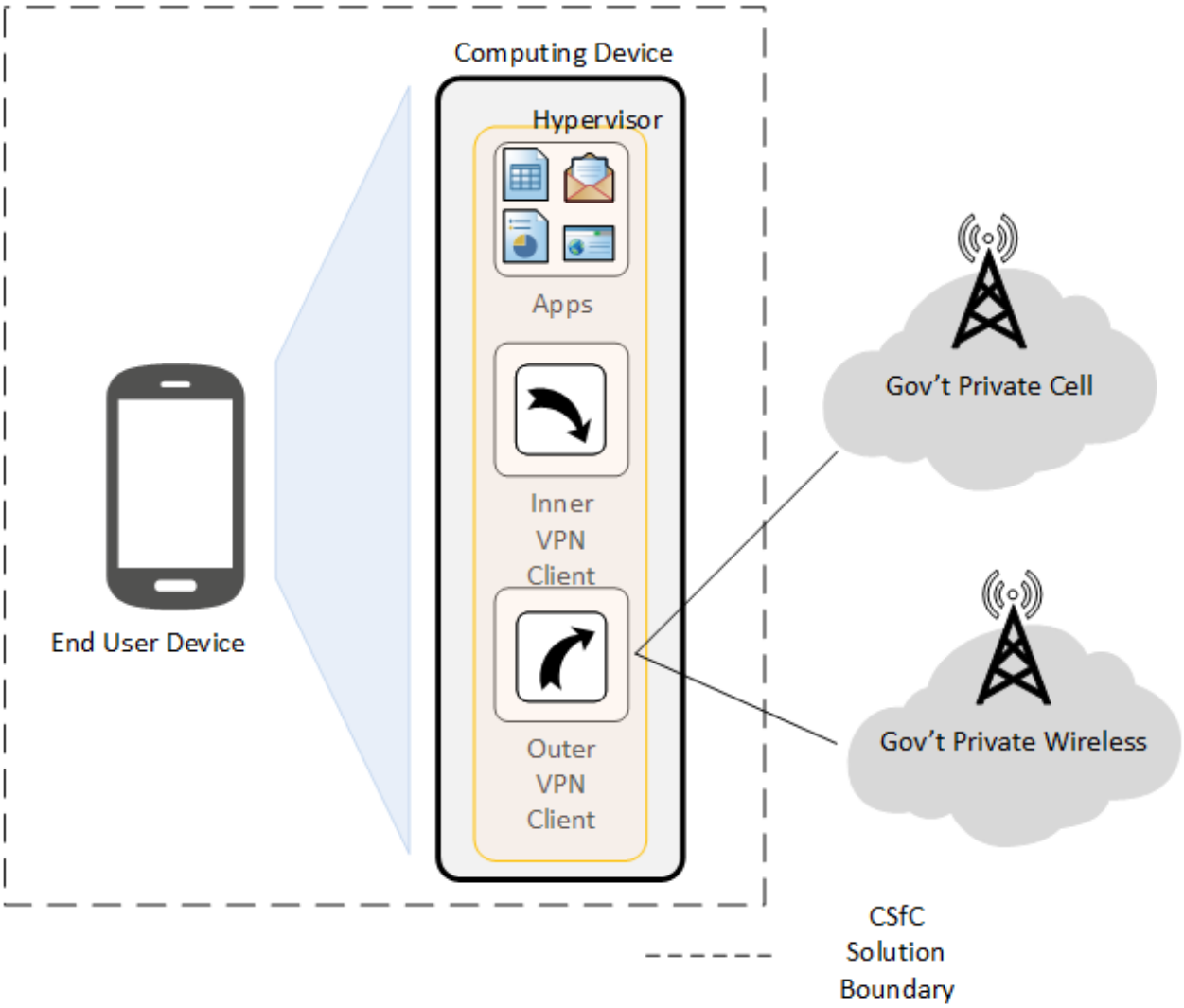

Figure 12. VPN EUD with Inner and Outer VPN Clients in Separate Virtual Machines without Retransmission Device

TLS End User Devices:

The TLS EUDs can be set up using up to two separate components. These components consist of the Computing Device and the VPN Component. The Computing Device sends and receives classified data. The Outer VPN Component is either a VPN Gateway or a VPN Client. Dedicated Outer VPN components are always physically separate from the Computing Device and are selected from the CSfC Components List (see Section 11). VPN Clients are selected from the IPsec VPN Client section of the CSfC Components List. The Inner layer of encryption is always provided by an application on the Computing Device which terminates either TLS and/or SRTP. Each application installed on the Computing Device must be selected

from the CSfC Components List. The CSfC Components List provides several sections for which customers can select the TLS Application including Web Browser, Email Client, and VoIP Application. Physical separation between encryption components provides a number of security advantages, but also is more difficult to implement due to the required hardware users require.

For TLS EUDs, each application installed on the Computing Device is responsible for terminating the Inner layer of encryption as shown in Figure 13. If a Dedicated Outer VPN component is used it must be connected to the Computing Device using Ethernet or wireless WPA2. When the Dedicated Outer VPN provides wireless connectivity to the Computing Device, the requirements in Section 12.9 must be followed.

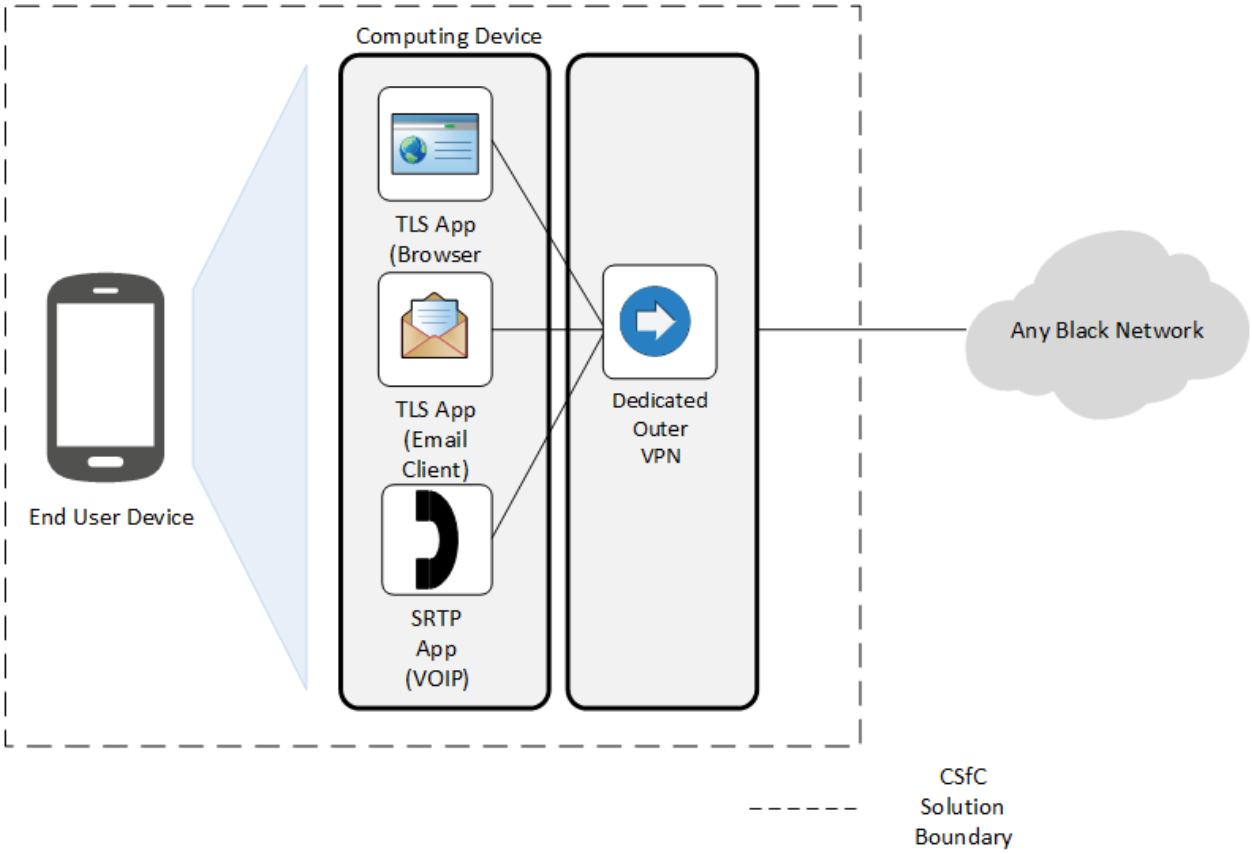

Figure 13. TLS EUD with Separate Outer VPN Gateway

An Outer VPN Client can be installed within the same Computing Device as the TLS Applications which provide the inner layer of encryption as shown in Figure 14. A RD will also be required in this case, unless, as noted in Section 4.1.3, the connection is to a Government Private Wireless Network or a Government Private Cellular Network as shown in Figure 15.

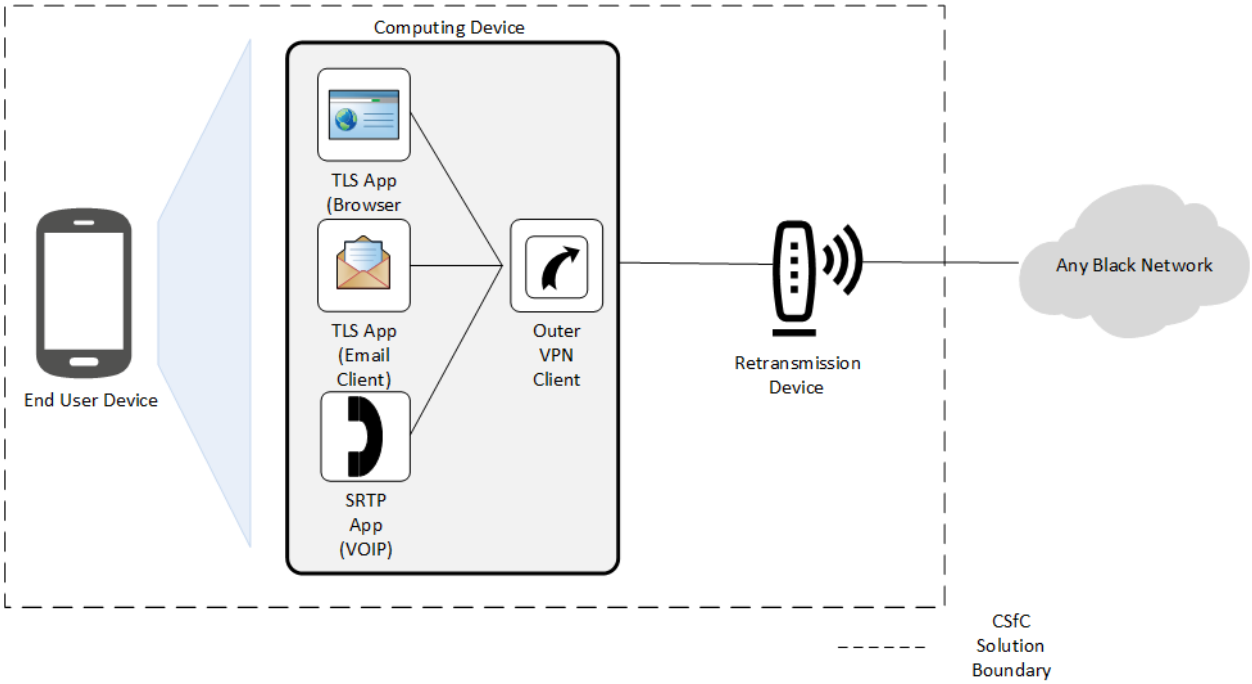

Figure 14. TLS EUD with Integrated Outer VPN Client with Retransmission Device

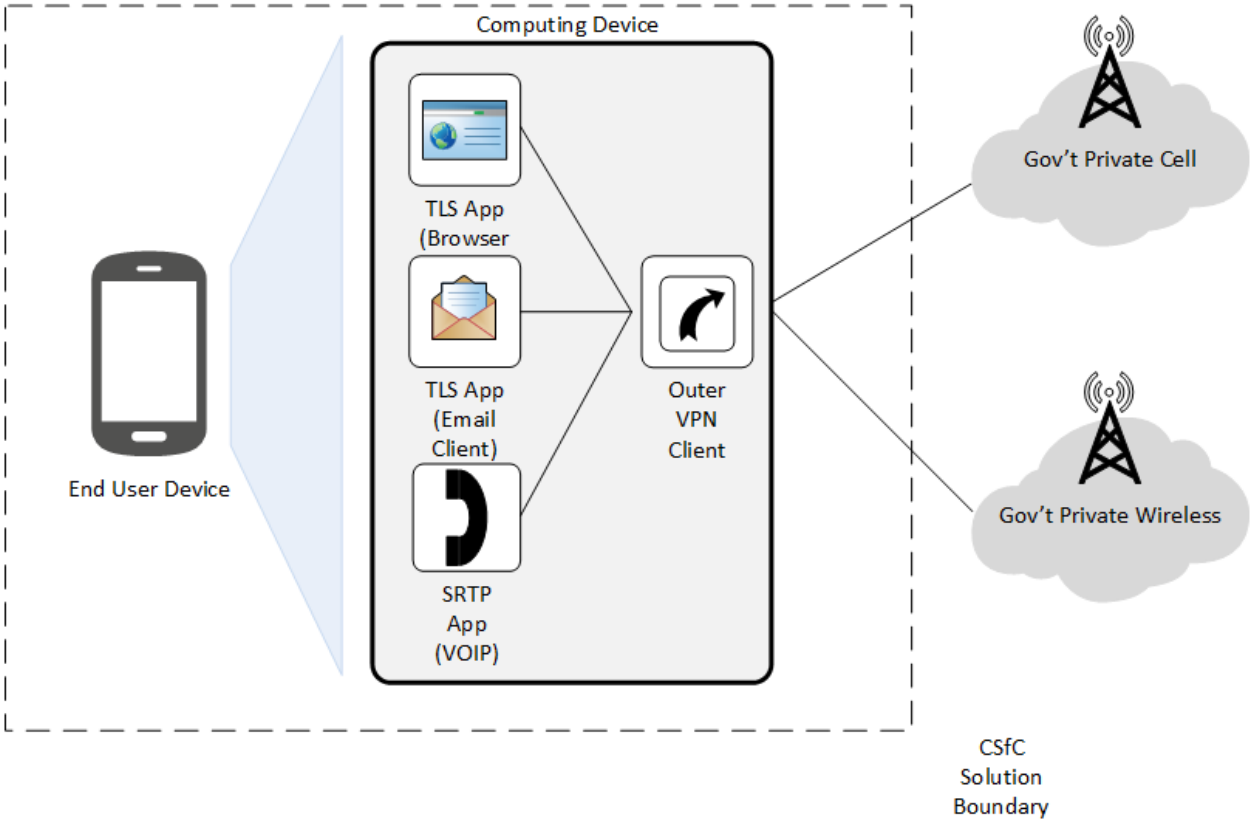

Figure 15. TLS EUD with Integrated Outer VPN Client with Retransmission Device

Retransmission Devices:

A Government-owned RD includes Wi-Fi Hotspots and Mobile Routers. On the external side, the RD can be connected to any type of medium (e.g., Cellular, Wi-Fi, SATCOM, Ethernet) to gain access to the Wide Area Network. On the internal side the RD is connected to EUDs either through an Ethernet cable or Wi-Fi as shown in Figure 16.

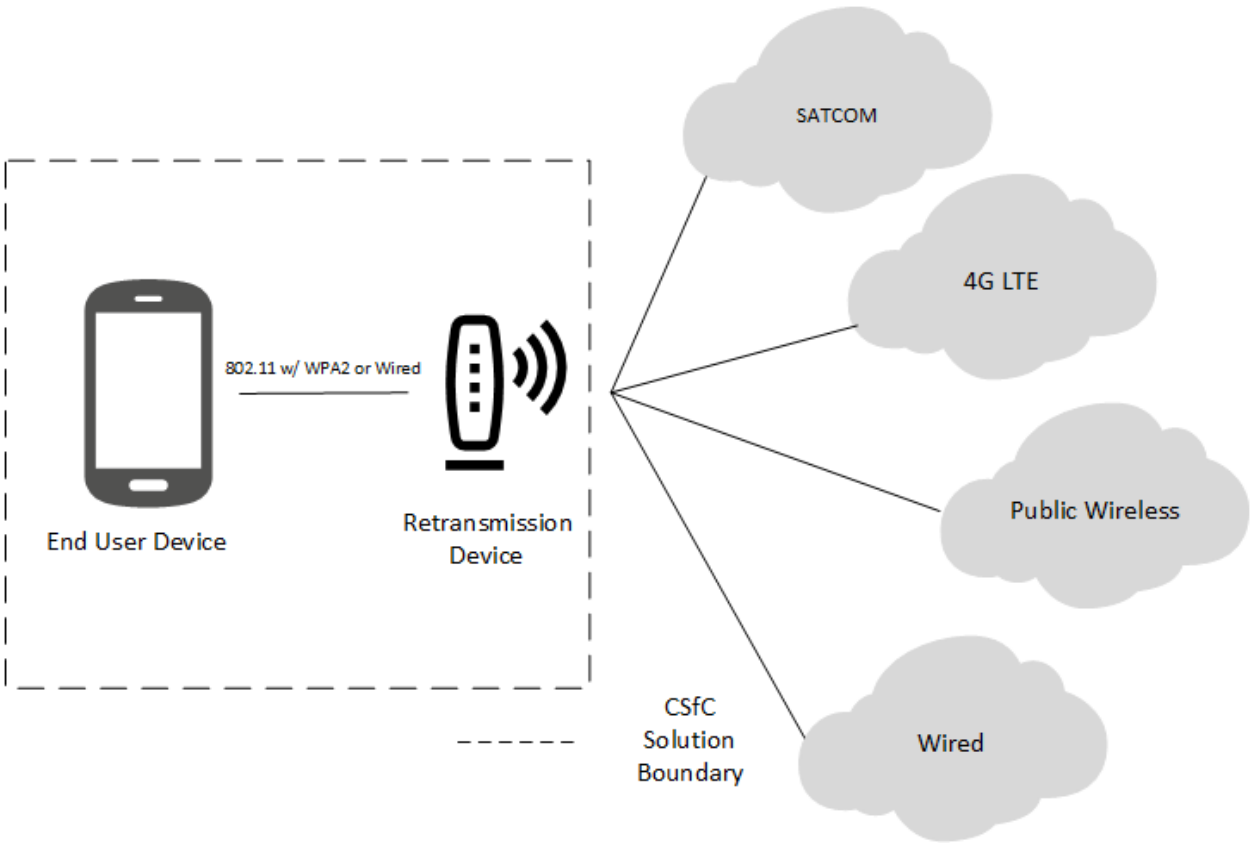

Figure 16. Retransmission Device Connectivity

Solution Infrastructure supporting VPN and TLS EUDs:

When supporting both VPN EUDs and TLS EUDs, the solution infrastructure will always include an Inner VPN Gateway between the Gray Firewall and Inner Firewall (data flow 1 in Figure 17). Additionally, the solution infrastructure will include one or more TLS-Protected Servers. The TLS-Protected Servers are also placed between the Gray Firewall and Inner Firewall (data flow 2 in Figure 17). Each Inner Encryption Component is independent and parallel to other Inner Encryption Components.

Figure 17 below shows a MA Solution which supports both TLS EUDs and VPN EUDs.

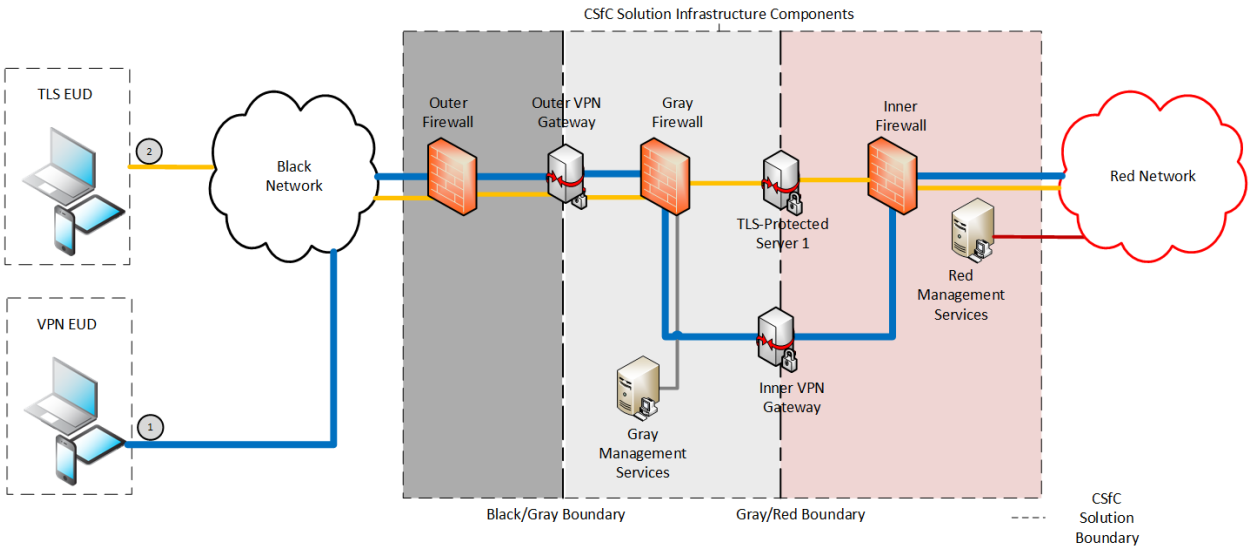

Figure 17. Mobile Access Solution Infrastructure Supporting VPN and TLS EUDs

The following text describes each of the data flows shown above.

1. The Inner VPN Gateway terminates the Inner layer of IPsec traffic for all VPN EUDs, and authenticates the EUD VPN client based on device certificates. There is a physical connection between the Gray Firewall and the Inner VPN Gateway and between the Inner VPN Gateway and the Inner Firewall.
2. The TLS-Protected Server is placed between Gray Firewall and Inner Firewall. The TLS-Protected Server terminates the Inner layer of TLS traffic for one or more of the services available to TLS EUDs. The TLS-Protected Server could also be a Session Border Controller which terminates SRTP traffic and relays it to the appropriate destination in the Red Network. The TLS-Protected Server authenticates the EUD's TLS client based on user or device certificates. There is a physical connection between the Gray Firewall and the TLS-Protected Server and between the TLS-Protected Server and the Inner Firewall. This connection is in parallel with the VPN Gateway such that the TLS-Protected server is not dependent on the Inner-VPN Gateway to reach the Gray Firewall or the Inner Firewall.

APPENDIX E. TACTICAL SOLUTION IMPLEMENTATIONS

Although the majority of customers instantiating solutions based on the MA CP will be used for Strategic or Operational Environments, some organizations may deploy the MA CP in Tactical Environments. These Tactical Environments include a specific set of Size, Weight, and Power (SWaP) constraints not found in traditional environments.

Organizations intending to deploy a MA CP Solution for Tactical Environments may use this Appendix, which accommodates the SWaP constraints unique to their environment. This Appendix may only be used to protect Tactical Data classified as SECRET or below. The CP follows CNSSI 4009, which defines Tactical Data as "Information that requires protection from disclosure and modification for a limited duration as determined by the originator or information owner." In addition to protecting Tactical Data, organizations that register their solution using this Appendix must be deployed at the Tactical Edge. The CP also follows CNSSI 4009, which defines the Tactical Edge as, "The platforms, sites, and personnel (U. S. military, allied, coalition partners, first responders) operating at lethal risk in a battle space or crisis environment characterized by 1) a dependence on information systems and connectivity for survival and mission success, 2) high threats to the operational readiness of both information systems and connectivity, and 3) users are fully engaged, highly stressed, and dependent on the availability, integrity, and transparency of their information systems."

If an organization's planned solution meets the three above criteria then their solution may be registered utilizing the requirement accommodations in this Appendix. The MA CP Registration form must explicitly state that the solution is being used in Tactical Environments and provide justification on how the above criteria are met. In general, customers registering with this Appendix will be deployed in support of Battalion and below (or equivalent) unit structure. Typically, these Tactical Environments are located in austere environments where communication infrastructure is generally limited. Due to the lack of existing communication infrastructure, the Tactical Environments are also generally characterized by the use of Government owned Black Infrastructure (Government Private Wireless Networks and/or Government Private Cellular Networks).

The below table may be used by customers meeting the above criteria when configuring, testing, registering, and operating their MA Solution. All other requirements stand as written in the body of the CP above. Any questions on the use of this Appendix should be directed to mobile_access@nsa.gov and csfc@nsa.gov.

Table 29. Tactical Implementation Requirements Overlay

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative
MA-PS-17	The Outer Firewall, Outer VPN Gateway, Gray Firewall, Inner Encryption Component, and Inner Firewall must use physically separate components, such that no component is used for more than one function (see Figure 1).	VI, TI	O	MA-TO-1
MA-TO-1	The Outer VPN Gateway must be physically separate from the Inner Encryption Components	VI, TI	T	MA-PS-17
MA-EU-12	Users of EUDs must successfully authenticate themselves to the services they access on the Red Network using an AO approved method.	All	O	
MA-EU-13	Red Network services must not transmit any classified data to EUDs until user authentication succeeds.	VI, TI	O	
MA-MR-5	Each IDS in the solution must be configured to send alerts to the Security Administrator.	VI, TI	O	
MA-MR-7	The organization must create IDS rules that generate alerts upon detection of any unauthorized destination IP addresses.	VI, TI	O	
MA-DM-14	The Outer VPN Gateway and solution components within the Gray Network must forward log entries to a SIEM on the Gray Management network (or SIEM in the Red Network if using an AO approved one-way tap) within 10 minutes.	VI, TI	O	
MA-EU-47	USB mass storage mode must be disabled on the EUDs.	VE, TE	O	
MA-EU-8	Rekeying of an EUD's certificates and associated private keys must be done through re-provisioning prior to expiration of keys.	VE, TE	O	