National Security Agency/
Central Security Service

INFORMATION ASSURANCE CAPABILITIES

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

Registration #

Solution Name

Date Submitted

1 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	Compliance (Explain how your solution meets the requirement)
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		
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		
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	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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	
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	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

2 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.

2.1 OVERALL SOLUTION REQUIREMENTS

Table 6. Overall Solution Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		
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		

[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.

2.2 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

2.3 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	Compliance (Explain how your solution meets the requirement)
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 .	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	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

2.4 INNER VPN COMPONENTS

Table 12. Inner VPN Components Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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	
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	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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	

2.5 OUTER VPN COMPONENTS

Table 13. Outer VPN Components Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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	

2.6 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	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		
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		

2.7 TLS-PROTECTED SERVER & SRTP ENDPOINT REQUIREMENTS

Table 15. TLS-Protected Server & SRTP Endpoint Requirements

Req #	Requirement Description	Capabilities	Threshold/Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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 that are approved to protect the highest classification level of the Red Network Data.	T	T=O		

Req #	Requirement Description	Capabilities	Threshold/Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

2.8 RETRANSMISSION DEVICE REQUIREMENTS

Table 16. Requirements for Retransmission Device

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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	
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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	
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	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

2.9 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	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		
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.	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		

2.10 END USER DEVICES REQUIREMENTS

Table 18. Requirements for End User Devices

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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	Compliance (Explain how your solution meets the requirement)
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	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		
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				

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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	
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		
MA-EU-67	EUDs must prohibit the use of removable media through configuration, policy, or physical modification.	VE, TE	T=O		

2.11 PORT FILTERING REQUIREMENTS FOR SOLUTION COMPONENTS

Table 19. Port Filtering Requirements for Solution Components

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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	
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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	
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		

2.12 CONFIGURATION CHANGE DETECTION REQUIREMENTS

Table 20. Configuration Change Detection Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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	

2.13 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	Compliance (Explain how your solution meets the requirement)
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	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
MA-DM-12	Devices must use Enrollment over Secure Transport (EST) as detailed in IETF RFC 7030 for certificate management.	All	O	Optional	
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	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

2.14 CONTINUOUS MONITORING REQUIREMENTS

Table 22. Continuous Monitoring Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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	Compliance (Explain how your solution meets the requirement)
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	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		
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	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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	

2.15 AUDITING REQUIREMENTS

Table 23. Auditing Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
MA-AU-22	Each log entry must record the user and, for role-based events, role identity, where applicable.	All	T=O		
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	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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	Compliance (Explain how your solution meets the requirement)
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		

2.16 KEY MANAGEMENT REQUIREMENTS

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

2.17 TWO FACTOR AUTHENTICATION

Table 24. Two Factor Authentication Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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	
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	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

3 REQUIREMENTS FOR SOLUTION OPERATION, MAINTENANCE, AND HANDLING

3.1 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	Compliance (Explain how your solution meets the requirement)
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		
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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.

3.2 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 2.14 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	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

Table 27. Role-Based Personnel Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		
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		

Table 28. Test Requirements

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
MA-TR-1	The organization implementing the CP must perform all tests listed in the MA CP Testing Annex.		T=O		

Table 29. Tactical Implementation Requirements Overlay

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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	

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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		

Req #	Requirement Description	Capabilities	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
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, TI	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		