National Security Agency/ Central Security Service

INFORMATION ASSURANCE CAPABILITIES

MULTI-SITE CONNECTIVITY CAPABILITY PACKAGE V1.1

This Commercial Solutions for Classified (CSfC) Capability Package describes how to protect classified data in transit across an untrusted network using multiple encrypted tunnels implemented with Internet Protocol Security (IPsec), Media Access Control Security (MACsec), or both encryption protocols.

Version 1.1
26 June 2018

Registration #

Solution Name:

Date Submitted

1. REQUIREMENTS FOR SELECTING COMPONENTS

CPs provide architecture and configuration information that allow customers to select COTS products from the CSfC Components List for their solution and then to properly configure those products to achieve a level of assurance sufficient for protecting classified data. The CSfC Components List consists of eligible COTS products identified by model/version numbers that have met appropriate Protection Profile requirements.

The products that are approved for use in this solution will be listed on the CSfC Components List. No single commercial product must be used to protect classified information. The only approved method for using COTS products to protect classified information in transit is through an approved CP.

Once the products for the solution are selected, each product 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 Supply Chain Risk Management (SCRM) for additional guidance).

In this section, a series of requirements are given for maximizing the independence between the components within the solution. The requirements in Table 3 will increase the level of effort required to compromise this solution.

Table 1. Product Selection (PS) Requirements

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
MSC-PS-1	The products used for any VPN Gateway must be chosen from the list of IPsec VPN Gateways on the CSfC Components List.	T=O	MSC-PS-1	
MSC-PS-2	The products used for any MACsec Device must be chosen from the list of MACsec Ethernet Encryptors on the CSfC Components List.	T=O		
MSC-PS-3	The products used for any Firewalls must be chosen from the list of Traffic Filtering Firewalls (TFFWs) on the CSfC Components List.	T=O		
MSC-PS-4	The products used for any 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.	T=O		

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
MSC-PS-5	Intrusion Prevention Systems (IPSs) must be chosen from the list of IPS on the CSfC Components List.	O	None	
MSC-PS-6	The Inner Encryption Component and the Outer Encryption Component 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.	T=O	MSC-PS-6	
MSC-PS-7	The Inner Encryption Component and the Outer Encryption Component must not use the same Operating System (OS). Differences between Service Packs and version numbers for a particular vendor's OS do not provide adequate diversity.	T=O		
MSC-PS-8	The cryptographic libraries used by the Inner Encryption Component and Outer Encryption Component must either: come from different manufacturers, where neither manufacturer is a subsidiary of the other; or be different libraries from the same manufacturer, where NSA has determined that the libraries meet the CSfC criteria for implementation independence.	O	None	

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
MSC-PS-9	If the solution contains an Inner CA and an Outer CA, the cryptographic libraries must either: come from different manufacturers, where neither manufacturer is a subsidiary of the other; or be different libraries from the same manufacturer, where NSA has determined that the libraries meet the CSfC criteria for implementation independence.	O	None	
MSC-PS-10	If Gray Firewalls are used, the Gray Firewalls and Inner Encryption Components must either: come from different manufacturers, where neither manufacturer is a subsidiary of the other; or be two different products from the same manufacturer, where NSA has determined that the two products meet the CSfC criteria for implementation independence.	T=O		
MSC-PS-11	The Inner Encryption Component and Outer Encryption Component must use physically separate components, such that no component is used for more than one function.	T=O		
MSC-PS-12	If an Outer Firewall and/or Gray Firewall is required, the Outer Firewall, Outer Encryption Component, Gray Firewall and Inner Encryption Component must use physically separate components, such that no component is used for more than one function.	T=O	MSC-PS-12	

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
MSC-PS-13	Black Network Enterprise PKI is prohibited from being used as the Outer or Inner tunnel CA.	T=O		
MSC-PS-14	If the solution contains an Inner CA and an Outer CA, the 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.	O	None	
MSC-PS-15	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).	T=O		
MSC-PS-16	MSC Solution Components must be configured to use the NIAP-certified evaluated configuration.	T=O		

1 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 on how to configure the components of the MSC Solution.

1.1 OVERALL SOLUTION REQUIREMENTS

Table 4 provides the overall solution requirements for this CP.

Table 2. Overall Solution Requirements (SR)

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
MSC-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 Outer Encryption Component and Red network for Inner Encryption Component).	T=O		
MSC-SR-2	Sites that need to communicate must ensure that each tunnel's Encryption Components selected by each site are interoperable.	T=O		
MSC-SR-3	The time of day on the Inner Encryption Component and Red Management Services must be synchronized to a time source located in the Red network.	T=O		
MSC-SR-4	The time of day on the Outer Encryption Component, Gray Management Services and Gray Firewall (if present) must be synchronized to a time source located in the Gray management network.	T=O		

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
MSC-SR-5	Default accounts, passwords, community strings, and other default access control mechanisms for all Solution Components must be changed or removed.	T=O		
MSC-SR-6	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.	T=O		
MSC-SR-7	All physical paths within a Gray network between Inner Encryption Components for Red networks of different security levels must include a Gray Firewall.	T=O		
MSC-SR-8	All physical paths within a Gray network between a CA, an Administration Workstation, or a CDP/OCSP Responder and an Inner Encryption Component for Red networks of different security levels must include a Gray Firewall.	T=O		
MSC-SR-9	Gray network components must be physically protected to the level of the highest classified network.	T=O		

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
MSC-SR-10	The Outer Encryption Component must use a unique physical internal interface for each Red network in the MSC Solution (e.g., VLAN trunking of multiple enclaves is not permitted).	T=O		
MSC-SR-11	A Gray Firewall is required if the MSC Solution is combined with another CSfC solution that requires a Gray Firewall.	T=O		
MSC-SR-12	If the MSC Solution uses the Public Internet for its Black transport network, an Outer Firewall must be located between the Black transport network and the Outer Encryption Component.	T=O		
MSC-SR-13	If the MSC Solution is combined with other CSfC data-in-transit solutions that include end user devices, an Inner Firewall is required. All firewall requirements for the other CSfC solution supersede firewall requirements for the MSC CP.	T=O		
MSC-SR-14	The only approved physical paths leaving the Red network must be through a MSC Solution in accordance with this CP or via an AO-approved solution for protecting data in transit[1].	T=O		

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

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets the requirement)
MSC-SR-15	Solution Components must receive virus signature updates as required by the local agency policy and the AO.	T=O		
MSC-SR-16	When multiple Inner Encryption Components share an Outer Encryption Component, they must be placed in parallel.	T=O		
MSC-SR-17	Inner Encryption Components must not perform switching or routing for other Encryption Components.	T=O		
MSC-SR-18	Solution Components must only be configured over an interface dedicated for management.	T=O		
MSC-SR-19	DNS lookup services on network devices must be disabled.	O	None	
MSC-SR-20	DNS server addresses on Solution Components must be specified or DNS services must be disabled.	T=O		
MSC-SR-21	Automatic remote boot-time configuration services must be disabled (e.g., automatic configuration via Trivial File Transfer Protocol (TFTP) on boot).	T=O		

1.2 VPN GATEWAY REQUIREMENTS

This section addresses requirements for VPN Gateways. Table 5 identifies the algorithms approved for IPsec encryption. Table 6 provides requirements for VPN Gateways.

Table 3. IPsec Encryption (Approved Algorithms for Classified)

Security Service	Algorithm Suite	Specifications
Confidentiality (Encryption)	Advanced Encryption Standard (AES)-256	FIPS PUB 197 IETF RFC 6379 IETF RFC 6380
Authentication (Digital Signature)	RSA 3072 or ECDSA over the curve P-384 with SHA-384	FIPS PUB 186-4 IETF RFC 4754 IETF RFC 6380 IETF RFC 7427
Key Exchange/ Establishment	ECDH over the curve P-384 (Diffie-Hellman (DH) Group 20) or DH 3072	NIST SP 800-56A IETF RFC 3526 IETF RFC 5903 IETF RFC 6379 IETF RFC 6380 IETF RFC 7296
Integrity (Hashing)	SHA-384	FIPS PUB 180-4 IETF RFC 6379 IETF RFC 6380

Table 4. VPN Gateway (VG) Requirements

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
MSC-VG-1	The proposals offered by VPN Gateways in the course of establishing the Internet Key Exchange (IKE) Security Association (SA) and the ESP SA for inner and outer tunnels must be configured to offer algorithm suite(s) containing only CNSA Suite algorithms (see Table 5).	T=O		

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
MSC-VG-2	Default, self-signed or proprietary device certificates, which are frequently preinstalled by the vendor, for any VPN Gateway must not be used for establishing SAs.	T	MSC-VG-3	
MSC-VG-3	Default, self-signed or proprietary device certificates, which are frequently preinstalled by the vendor, for any VPN Gateway must be removed.	O	MSC-VG-2	
MSC-VG-4	A unique device certificate must be loaded onto each VPN Gateway along with the corresponding CA certificate chain, to include the Trust Anchor CA certificate.	T=O		
MSC-VG-5	The private key stored on VPN Gateways must not be accessible through an interface.	T=O		
MSC-VG-6	A device certificate must be used for VPN Gateway authentication during IKE.	T=O		
MSC-VG-7	VPN Gateway authentication must include a check that the certificate is not revoked, which can include a CRL, OCSP Responder, whitelist, or other similar revocation reporting mechanism.	T=O		
MSC-VG-8	The VPN Gateway authentication must include a check that certificates are not expired.	T=O		

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
MSC-VG-9	All VPN Gateways must use IKEv2 (IETF RFC 7296) key exchange.	T=O		
MSC-VG-10	All VPN Gateways must use Cipher Block Chaining for IKE encryption.	T=O		
MSC-VG-11	All VPN Gateways must use Cipher Block Chaining for ESP encryption with a Host-based Message Authentication Code (HMAC) for integrity.	T	MSC-VG-12	
MSC-VG-12	All VPN Gateways must use Galois Counter Mode for ESP encryption.	O	MSC-VG-11	
MSC-VG-13	All VPN Gateways must set the IKE SA lifetime to at most 24 hours.	T=O		
MSC-VG-14	All VPN Gateways must set the ESP SA lifetime to at most 8 hours.	T=O		
MSC-VG-15	Inner VPN Gateways must only authenticate and establish an IPsec tunnel with one another if their Red networks operate at the same security level (as defined in this CP).	T=O		
MSC-VG-16	All VPN Gateways must re-authenticate the identity of the VPN Gateway at the other end of the established tunnel before rekeying the IKE SA.	T=O		

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
MSC-VG-17	The Mandatory Access Control policy must only allow the VPN Gateway to access the private key of the VPN Gateway.	O	None	

1.3 MACsec Device Requirements

This section addresses requirements for MACsec Devices. Table 7 identifies the algorithms approved for MACsec encryption. Table 8 provides requirements for MACsec Devices.

Table 5. MACsec Encryption (Approved Algorithms for Classified)

Security Service	Algorithm Suite	Specifications
Confidentiality (Encryption)	Galois Counter Mode (GCM)-AES-256 GCM-AES-XPN-256	FIPS PUB 197 IEEE 802.1AEbn-2011 IEEE 802.1AEbw-2013
Key Wrap	AES Key Wrap	IETF RFC 3394

Table 6. MACsec Device (MD) Requirements

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
MSC-MD-1	MACsec Devices must use AES Key Wrap for key distribution with a cryptographic key size of 256 bits.	T=O		
MSC-MD-2	MACsec Devices must use AES GCM for MACsec with a cryptographic key size of 256 bits.	T=O		
MSC-MD-3	MACsec Devices must authenticate using Pre-Shared Keys (PSKs), known as Connectivity Association Keys (CAKs).	T=O		

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
MSC-MD-4	Requirement has been relocated to the Key Management Requirements Annex.	T=O		
MSC-MD-5	MACsec Devices must have the length of the CKN set to a minimum of 16 bytes (128 bits) and generate the CKN using an NSA-approved KGS.	T=O		
MSC-MD-6	For each pair of MACsec Devices establishing an encryption tunnel, one of the two must be configured to be the Key Server by setting its Key Server value to 0 (zero). The other MACsec Device must have its Key Server value set to 1. If a Central Management Site is part of the MSC Solution, it must be the Key Server.	T=O		
MSC-MD-7	MACsec Devices must enable data delay protection for MACsec Key Agreement (MKA).	T=O		
MSC-MD-8	MACsec Devices must have an MKA Lifetime Timeout limit set to 6.0 seconds and Hello Timeout limit set to 2.0 seconds.	T=O		
MSC-MD-9	MACsec Devices must have the replay window set to 2 or as low as possible given the nature of the Black network being traversed.	T=O	MSC-MD-9	
MSC-MD-10	MACsec Devices must require all data traffic on an external facing port to be encrypted (e.g., must-secure).	T=O	MSC-MD-10	

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
MSC-MD-11	MACsec Device configuration files, whether printed or electronically copied, must be physically protected to the highest classification of the MACsec Device's CAK.	T=O	MSC-MD-11	
MSC-MD-12	MACsec Devices must have the Confidentiality Offset set to 0 (zero).	T=O	MSC-MD-12	
MSC-MD-13	If a standalone device is required to provide encapsulation of MACsec traffic between an Inner MACsec Device and an Outer Encryption Component, the standalone device must be considered a Solution Component when satisfying requirements in Section 11.1.	T=O	MSC-MD-13	

1.4 Additional Requirements for Inner Encryption Components

Additional requirements for Inner Encryption Components are identified in Table 9.

Table 7. Additional Requirements for Inner Encryption Components (IR)

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
MSC-IR-1	The Inner VPN Gateway must use ESP Tunnel mode IPsec, or ESP Transport mode IPsec using an associated IP tunneling protocol (e.g., Transport Mode IPsec with GRE).	T=O		
MSC-IR-2	Sizes for packets or frames leaving the external interface of the Inner Encryption Component must be configured to reduce	O	None	

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
	fragmentation and impact performance. This requires proper configuration of the Maximum Transmission Unit (MTU) (for IPv4 or MACsec) or Path MTU (PMTU) (for IPv6) and should consider Black network and Outer Encryption Component MTU/PMTU values to achieve this.			
MSC-IR-3	The Inner Encryption Component 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.	T	MSC-IR-4	
MSC-IR-4	The Inner Encryption Component must use Mandatory Access Control 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.	O	MSC-IR-3	
MSC-IR-5	The Inner Encryption 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.	T	MSC-IR-6	

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
MSC-IR-6	The Inner Encryption Component must use Mandatory Access Control 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.	O	MSC-IR-5	
MSC-IR-7	The Inner Encryption Component must not permit split-tunneling.	T=O		

1.5 ADDITIONAL REQUIREMENTS FOR OUTER ENCRYPTION COMPONENTS

Additional requirements for Outer Encryption Components are identified Table 10.

Table 8. Additional Requirements for Outer Encryption Components (OR)

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-OR-1	Outer VPN Gateways must use ESP Tunnel mode IPsec.	T=O		
MSC-OR-2	Outer Encryption Components 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.	T	MSC-OR-3	
MSC-OR-3	Outer Encryption Components must use Mandatory Access Control policy to not allow any packets received on an interface	O	MSC-OR-2	

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets requirement)
	connected to a Gray network to bypass encryption and be forwarded out through an interface connected to a Black network.			
MSC-OR-4	All traffic received by Outer Encryption Components on an interface connected to a Gray network, with the exception of control plane traffic, must have already been encrypted once.	T=O		
MSC-OR-5	Outer Encryption Components must not allow any packets received on an interface connected to a Black network to bypass decryption.	T	MSC-OR-6	
MSC-OR-6	Outer Encryption Components must use Mandatory Access Control policy to not allow any packets received on an interface connected to a Black network to bypass decryption.	O	MSC-OR-5	
MSC-OR-7	The Outer Encryption Components must not permit split-tunneling.	T=O		
MSC-OR-8	Outer Encryption Components must not use routing protocols (e.g., OSPF, BGP).	T=O		

1.6 Port Filtering Requirements for Solution Components

Requirements for port filtering for Solution Components are identified in Table 11.

Table 9. Port Filtering (PF) Requirements for Solution Components

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-PF-1	All Solution Components must have all network interfaces restricted to the smallest address ranges, ports, and protocols possible.	T=O		
MSC-PF-2	All Solution Components must have all unused network interfaces disabled.	T=O		
MSC-PF-3	For all Outer VPN Gateway interfaces 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.	T=O		
MSC-PF-4	For all Outer MACsec Device interfaces connected to a Black network, traffic filtering rules must be applied to both inbound and outbound traffic, such that only MACsec Protocol Data Units (MPDUs) and control plane protocols (as defined in this CP) approved by organization-defined policy are allowed.	T=O		
MSC-PF-5	For all Inner Encryption Component interfaces connected to a Gray network, traffic filtering rules must be applied to both inbound and outbound traffic, such that only IKE, IPsec, MKA, MACsec, and	T=O		

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets requirement)
	control plane protocols (as defined in this CP) approved by organization-defined policy are allowed.			
MSC-PF-6	Any service or feature that allows an Outer Encryption Component to contact a third party server (such as one maintained by the manufacturer) must be blocked.	T	MSC-PF-7	
MSC-PF-7	Any service or feature that allows an Outer Encryption Component to contact a third party server (such as one maintained by the manufacturer) must be disabled.	O	MSC-PF-6	
MSC-PF-8	Management plane traffic must only be initiated from the Gray Administration Workstation with the exception of logging or authentication traffic that may be initiated from Outer Encryption Components.	T=O		
MSC-PF-9	Multicast messages received on external interfaces of Outer Encryption Components must be dropped.	T=O		
MSC-PF-10	For solutions using IPv4, Outer VPN Gateways using IPsec must drop all packets that use IP options.	O		

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-PF-11	For solutions using IPv4, each VPN Gateway must only accept packets with Transmission Control Protocol (TCP), User Datagram Protocol (UDP), ESP, or ICMP in the IPv4 Protocol field and drop all other packets.	T=O		
MSC-PF-12	For solutions using IPv6, each VPN Gateway must only accept packets with ESP, TCP, UDP, or ICMPv6 in the IPv6 Next Header field and drop all other packets.	T=O		
MSC-PF-13	The Gray network interfaces of Outer Encryption Components must allow IKE and IPsec, or MKA and MACsec traffic, as appropriate, that is between two Inner Encryption Components protecting networks of the same security level or that is being used for management of the Gray network.	T=O		
MSC-PF-14	The Gray network interfaces of Outer VPN Gateways must allow HTTP traffic between Inner VPN Gateways and Inner CDPs/OCSP Responders.	T	MSC-PF-15 and MSC-PF-16	

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-PF-15	The Gray network interfaces of Outer VPN Gateways must allow HTTP GET and OCSP requests from Inner VPN Gateways to Inner CDPs and OCSP Responders, respectively, for the Uniform Resource Locator (URL) of the CRL or OCSP response needed by the Inner VPN Gateway, and block all other HTTP requests.	O	MSC-PF-14	
MSC-PF-16	The Gray network interfaces of Outer VPN Gateways must allow HTTP responses from Inner CDPs/OCSP Responders to Inner VPN Gateways that contain a well-formed CRL per IETF RFC 5280 or a well-formed OCSP response per IETF RFC 6960, and block all other HTTP responses.	O	MSC-PF-14	
MSC-PF-17	The Gray network interfaces of Outer Encryption Components must only permit packets whose source and destination IP addresses match the external interfaces of Inner Encryption Components that support Red networks of the same security level.	T=O		
MSC-PF-18	The Gray network interfaces of Outer Encryption Components must block all packets whose source address does not match a list of addresses or address ranges known to be reachable from the interface where the packet was received.	T=O		

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-PF-19	The Gray network interfaces of Outer Encryption Components must allow management and control plane protocols (as defined in this CP) that have been approved by policy.	T=O		
MSC-PF-20	The Gray network interfaces of Outer Encryption Components must deny all traffic that is not explicitly allowed by requirements MSC-PF-8, MSC-PF- 13, MSC-PF-14, MSC-PF-15, MSC-PF-16, or MSC-PF-19.	T=O		
MSC-PF-21	CDPs/OCSP Responders must only allow inbound and outbound HTTP traffic per requirements MSC-PF-14, MSC-PF-15, and MSC-PF-16.	T=O		
MSC-PF-22	If an Outer Firewall is required, for all Outer Firewall interfaces, traffic filtering rules must be applied to both inbound and outbound traffic, such that only IKE, ESP, MKA, MACsec and control plane protocols (as defined in this CP) approved by organization-defined policy are allowed.	T=O		

Registration #

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-PF-23	If a Gray Firewall is required, the Gray Firewall must permit IKE, IPsec, MKA and MACsec traffic between two Inner Encryption Components protecting networks of the same security level.	T=O		
MSC-PF-24	If a Gray Firewall is required, the Gray Firewall must allow HTTP traffic between Inner VPN Gateways and Inner CDP/OCSP Responder.	T	MSC-PF-25 and MSC-PF-26	
MSC-PF-25	If a Gray Firewall is required, the Gray Firewall must allow HTTP GET and OCSP requests from Inner VPN Gateways to Inner CDPs/OCSP Responders for the URL of the CRL or OCSP response needed by the Inner VPN Gateway, and block all other HTTP requests.	O	MSC-PF-24	
MSC-PF-26	If a Gray Firewall is required, the Gray Firewalls must allow HTTP responses from Inner CDPs/OCSP Responders to Inner VPN Gateways that contain a well-formed CRL per IETF RFC 5280 or well-formed OCSP response per IETF RFC 6960, and block all other HTTP responses.	O	MSC-PF-24	
MSC-PF-27	If a Gray Firewall is required, the Gray Firewall must only accept management traffic on the physical ports connected to the Gray management network.	T=O		

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-PF-28	If a Gray Firewall is required, the Gray Firewall must only permit packets whose source and destination IP addresses match the external interfaces of Inner Encryption Components that support Red networks of the same security level.	T=O		
MSC-PF-29	If a Gray Firewall is required, the Gray Firewall must block all packets whose source address does not match a list of addresses or address ranges known to be reachable from the interface where the packet was received.	T=O		
MSC-PF-30	If a Gray Firewall is required, the Gray Firewall must allow control plane traffic (e.g., NTP, DHCP, and DNS).	T=O		
MSC-PF-31	If a Gray Firewall is required, the Gray Firewall must deny all traffic that is not explicitly allowed by requirements MSC-PF-23, MSC-PF- 24, MSC-PF-25, MSC-PF-26, MSC-PF-27 or MSC-PF-30.	T=O		

1.7 Configuration Change Detection Requirements

Table 12 defines the requirements for Configuration Change Detection.

Table 10. Configuration Change Detection (CM) Requirements

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-CM-1	A baseline configuration for all components must be maintained by the Security Administrator and be available to the Auditor.	T=O		
MSC-CM-2	An automated process must ensure that configuration changes are logged.	T=O		
MSC-CM-3	Log messages generated for configuration changes must include the specific changes made to the configuration.	T=O		
MSC-CM-4	All Solution Components must be configured with a monitoring service that detects all changes to configuration.	O	None	

1.8 DEVICE MANAGEMENT REQUIREMENTS

Table 13 defines the requirements for Device Management.

Table 11. Device Management (DM) Requirements

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-DM-1	Administration Workstations must be dedicated for the purposes given in this CP and must be physically separated from workstations used to manage non-CSfC solutions.	T=O		
MSC-DM-2	Administration Workstations must physically reside within a protected facility where CSfC solution(s) are managed.	T=O		

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-DM-3	Administration Workstations must connect from an internal port. Specifically, the Inner Encryption Component must be managed from the Red network, and the Outer Encryption Component and Gray Firewall, if present, must be managed from the Gray network.	T=O		
MSC-DM-4	A separate LAN or VLAN on the Red network must be used exclusively for all management of Inner Encryption Components and Solution Components within the Red network.	T=O		
MSC-DM-5	A separate LAN or VLAN on the Gray network must be used exclusively for all management of the Outer Encryption Component, Gray Firewall, if present, and Solution Components within the Gray network.	T=O		
MSC-DM-6	The Gray management network must not be directly connected to the Non-secure Internet Protocol Router Network (NIPRNet) or any other Unclassified network not dedicated to the administration of CSfC solutions.	T=O		

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-DM-7	All components must be configured to restrict the IP address range for the network administration device to the smallest range possible. Note that locally managing Solution Components is also acceptable.	T=O		
MSC-DM-8	All administration of Solution Components must be performed from an Administration Workstation remotely using an NSA-approved solution (e.g., CP or Type 1 encryptor), or by managing the Solution Components locally.	T=O		
MSC-DM-9	Security Administrators must authenticate to Solution Components before performing administrative functions.	T	MSC-DM-10	
MSC-DM-10	Security Administrators must authenticate to Solution Components with CNSA Suite compliant certificates before performing administrative functions remotely.	O	MSC-DM-9	
MSC-DM-11	The MSC Solution Owner must identify the authorized Security Administrators to initiate certificate requests.	T=O		
MSC-DM-12	Authorized Security Administrators must initiate certificate signing requests for Solution Components as part of their initial keying within the solution.	T=O		

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-DM-13	Authentication of Security Administrators must be enforced by either procedural or technical means.	O	None	
MSC-DM-14	Administration Workstations that interact with the Certificate Authority for the Outer VPN Gateways must be located on the Gray network.	T=O		
MSC-DM-15	Requirement has been relocated to the Key Management Requirements Annex.			
MSC-DM-16	Requirement has been relocated to the Key Management Requirements Annex.			
MSC-DM-17	The same Administration Workstation must not be used to manage Inner Encryption Components and Outer Encryption Components.	T=O		
MSC-DM-18	If SIEMs are used in the solution, Outer Encryption Components 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 event’s occurrence.	T=O		

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-DM-19	If SIEMS are used in the solution, 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 event's occurrence.	T=O		
MSC-DM-20	If SIEMS are used in the solution, all logs forwarded to a SIEM on the Gray management network must be encrypted using SSHv2, IPsec, MACsec, or TLS 1.2 or later.	O	None	
MSC-DM-21	If SIEMS are used in the solution, all logs forwarded to a SIEM on a Red management network must be encrypted using SSHv2, IPsec, MACsec, or TLS 1.2 or later.	O	None	
MSC-DM-22	Outer Encryption Components must only be managed by Security Administrators cleared to at least the highest level of classification of each Red network supported by the Outer Encryption Component at the physical site the Outer Encryption Component is located.	T=O		

1.9 Continuous Monitoring Requirements

Continuous monitoring requirements are identified in Table 14.

Table 12. Requirements for Continuous Monitoring (MR)

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-MR-1	Traffic from the Black, Gray, or Red networks must be monitored from an IDS.	T	MSC-MR-2	
MSC-MR-2	Traffic from the Black, Gray, or Red networks must be monitored from an IPS.	O	MSC-MR-1	
MSC-MR-3	If the Black transport network is the Public Internet, an IDS must be deployed in at least two of the following locations: • Between the Outer Firewall and the Outer Encryption Component (M1). • Between the Outer Encryption Component and Gray Firewall, if present, or the Inner Encryption Component (M2). • Between the Inner Encryption Component and Inner Firewall, if present, or the Red network (M3).	T	MSC-MR-4 MSC-MR-5 MSC-MR-6	

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-MR-4	If the Black transport network is the Public Internet, an IDS must be deployed in all of the following locations: • Between the Outer Firewall and the Outer Encryption Component (M1). • Between the Outer Encryption Component and Gray Firewall, if present, or the Inner Encryption Component (M2). • Between the Inner Encryption Component and Inner Firewall, if present, or the Red network (M3).	O	MSC-MR-3 MSC-MR-5 MSC-MR-6	
MSC-MR-5	If the Black transport network is the Public Internet, an IPS must be deployed in at least two of the following locations: • Between the Outer Firewall and the Outer Encryption Component (M1). • Between the Outer Encryption Component and Gray Firewall, if present, or the Inner Encryption Component (M2). • Between the Inner Encryption Component and Inner Firewall, if present, or the Red network (M3).	O	MSC-MR-3 MSC-MR-4 MSC-MR-6	

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-MR-6	If the Black transport network is the Public Internet, an IPS must be deployed in all of the following locations: • Between the Outer Firewall and the Outer Encryption Component (M1). • Between the Outer Encryption Component and Gray Firewall, if present, or the Inner Encryption Component (M2). • Between the Inner Encryption Component and Inner Firewall, if present, or the Red network (M3).	O	MSC-MR-3 MSC-MR-4 MSC-MR-5	
MSC-MR-7	If IDSs are part of the solution, each IDS must be configured to provide a dashboard or send alerts to the Security Administrator.	T	MSC-MR-8	
MSC-MR-8	If IPSs are part of the solution, each IPS must be configured to block malicious traffic flows and alert the Security Administrator.	O	MSC-MR-7	
MSC-MR-9	If IDSs are part of the solution, each IDS must be configured with rules that generate alerts upon detection of any unauthorized destination IP addresses.	T	MSC-MR-10	

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-MR-10	If IPSs are part of the solution, each IPS must be configured with rules that block and generate alerts upon detection of any unauthorized destination IP addresses.	O	MSC-MR-9	
MSC-MR-11	If IDSs are part of the solution, each IDS must be configured with rules that generate alerts upon detection of any unauthorized source IP addresses.	T	MSC-MR-12	
MSC-MR-12	If IPSs are part of the solution, each IPS must be configured with rules that block and generate alerts upon detection of any unauthorized source IP addresses.	O	MSC-MR-11	
MSC-MR-13	If SIEMs are part of the solution, 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.	T=O		
MSC-MR-14	If SIEMs are part of the solution, the SIEM must be configured to send alerts to the Security Administrator when anomalous behavior is detected (e.g., blocked packets from the Outer Encryption Component or Gray Firewall).	T=O		

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-MR-15	If a Gray SIEM is part of the solution, the Gray SIEM must collect logs from the Outer Encryption Component, Gray Firewall, and any components located within the Gray Management Services.	T=O		
MSC-MR-16	If a Gray SIEM is part of the solution, the Gray SIEM must maintain an up-to-date table of Certificate Common Name and assigned IP address used for the Outer VPN Gateway.	T=O		
MSC-MR-17	If a Gray SIEM is part of the solution, the Gray SIEM must provide a dashboard or alert for sites attempting to establish a connection with the Outer Encryption Component using misconfigured settings.	T=O		
MSC-MR-18	If a Gray SIEM is part of the solution, the Gray SIEM must provide an alert or dashboard for three or more invalid login attempts in a 24-hour period to the Outer Encryption Component and Gray Firewall, if present.	T=O		
MSC-MR-19	If a Gray SIEM is part of the solution, the Gray SIEM must provide an alert or dashboard of privilege escalations on the Outer Encryption Component and Gray Firewall, if present.	T=O		

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-MR-20	If a Gray SIEM is part of the solution, the Gray SIEM must provide an alert or dashboard of configuration changes to the Outer Encryption Component and Gray Firewall, if present.	T=O		
MSC-MR-21	If a Gray SIEM is part of the solution, the Gray SIEM must provide an alert or dashboard of new accounts created on the Outer Encryption Component and Gray Firewall, if present.	T=O		
MSC-MR-22	If a Gray SIEM is part of the solution, the Gray SIEM must provide an alert or dashboard for attempted connections to the Outer Encryption Component that use invalid certificates or keys.	T=O		
MSC-MR-23	If a Gray SIEM is part of the solution, the Gray SIEM must provide an alert, graph or table of blocked traffic at the Gray Firewall (if present) grouped by Common Name.	T=O		
MSC-MR-24	If a Gray SIEM is part of the solution, the Gray SIEM must provide a dashboard or alert for DNS queries other than expected values for IP addresses and domains.	O	None	
MSC-MR-25	Network flow data must be enabled on all routers and switches in the Red network.	T=O		

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-MR-26	A network flow data collector (e.g., SILK, IPFlow, and NetFlow Collector) must be installed in the Red network.	T=O		
MSC-MR-27	A baseline for network flow data must be established.	O	None	
MSC-MR-28	A baseline for network flow data must be updated regularly at an interval determined by the AO.	O	None	
MSC-MR-29	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.	O	None	
MSC-MR-30	Network flow data must be reviewed for systems generating an excessive number of short packets (e.g., over 60% of packets containing 150 bytes or less).	O	None	
MSC-MR-31	Network flow data must be reviewed for excessive numbers of ICMP messages.	O	None	

1.10 Auditing Requirements

Auditing requirements for the MSC Solution are identified in Table 15.

Table 13. Auditing (AU) Requirements

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-AU-1	Encryption Components must log establishment of an encryption tunnel.	T=O		
MSC-AU-2	Encryption Components must log termination of an encryption tunnel.	T=O		
MSC-AU-3	Solution Components must log all actions performed on the audit log (e.g., off-loading, deletion).	T=O		
MSC-AU-4	Solution Components must log all actions involving identification and authentication.	T=O		
MSC-AU-5	Solution Components must log attempts to perform an unauthorized action (e.g., read, write, execute, delete) on an object.	T=O		
MSC-AU-6	Solution Components must log all actions performed by a user with super-user or administrator privileges.	T=O		
MSC-AU-7	Solution Components must log escalation of user privileges.	T=O		
MSC-AU-8	Solution Components must log generation, loading, and revocation of certificates.	T=O		
MSC-AU-9	Solution Components must log changes to time.	T=O		

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-AU-10	Solution Components must log when packets received on Gray network interfaces are dropped or blocked.	T=O		
MSC-AU-11	Solution Components must log the results of built-in self-tests.	T=O		
MSC-AU-12	MACsec Devices must log the installation of a CAK into the MACsec Device, including all subsequent installations of new CAKs (i.e., CAK rekey).	T=O		
MSC-AU-13	MACsec Devices must log creation and updates of SAKs.	T=O		
MSC-AU-14	MACsec Devices must log administrator lockout due to excessive authentication failures.	T=O		
MSC-AU-15	MACsec Devices must log detected replay attempts.	T=O		
MSC-AU-16	Each log entry must record the date and time of the event.	T=O		
MSC-AU-17	Each log entry must include the identifier of the event.	T=O		

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-AU-18	Each log entry must record the type of event.	T=O		
MSC-AU-19	Each log entry must record the success or failure of the event to include failure code, when available.	T=O		
MSC-AU-20	Each log entry must record the subject identity.	T=O		
MSC-AU-21	Each log entry must record the source address for network-based events.	T=O		
MSC-AU-22	Each log entry must record the user and, for role-based events, role identity, where applicable.	T=O		
MSC-AU-23	VPN Gateways must log the failure to download the CRL from a CDP.	T=O		
MSC-AU-24	VPN Gateways must log if the version of the CRL downloaded from a CDP is older than the current cached CRL.	T=O		
MSC-AU-25	VPN Gateways must log if signature validation of the CRL downloaded from a CDP fails.	T=O		

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-AU-26	Auditors must compare and analyze collected network flow data against the established baseline on at least a daily basis.	T=O		
MSC-AU-27	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.	T=O		
MSC-AU-28	Locally-run CAs must comply with periodic audit and assessment requirements defined in IETF RFC 3647 Section 4.8.	T=O		
MSC-AU-29	Audits and assessments for a CA must be performed by personnel who are knowledgeable in the CA’s operations, as well as the CA’s Certificate Policy and CPS requirements and processes, respectively.	T=O		
MSC-AU-30	KGSs that deliver CAK Management Services for MSC Solutions are to comply with audit and assessment requirements defined by the customer's operational security doctrine and enterprise KGS (if applicable).	T=O		

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-AU-31	Audits and assessments for a KGS are to be performed by personnel who are knowledgeable in the KGS's operations, as well as the KGS’s audit requirements and processes, respectively.	T=O		

1.11 Key Management Requirements

Key Management Requirements are found in the Key Management Requirements Annex.

2 REQUIREMENTS FOR SOLUTION OPERATIONS, MAINTENANCE, AND HANDLING

2.1 Requirements for the Use and Handling of Solutions

The requirements in Table 16 must be followed regarding the use and handling of the solution.

Table 14. Requirements for the Use and Handling of Solutions

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-GD-1	All Solution Components, with the exception of the Outer Firewall (if present), must be physically protected as classified devices, classified at the level of the network with the highest classification in the solution or in any other MSC Solutions with which it is interconnected.	T=O		

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-GD-2	Only authorized and appropriately cleared (or escorted) administrators and security personnel must have physical access to the Solution Components.	T=O		
MSC-GD-3	All components of the solution must be disposed of as classified devices, unless declassified using AO-approved procedures.	T=O		
MSC-GD-4	Acquisition and procurement documentation must not include information concerning the purpose of the equipment, to include that it will be used to protect classified information.	T=O		
MSC-GD-5	The Solution Owner must allow, and fully cooperate with, NSA or its authorized agent to perform an Information Assurance (IA) compliance audit (including, but not limited to, inspection, testing, observation, and interviewing) of the solution implementation to ensure it meets the latest version of this CP.	T=O		
MSC-GD-6	The AO will ensure that a compliance audit must be conducted every year against the latest version of this CP as part of the annual solution re-registration process.	T=O		

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-GD-7	Results of the compliance audit must be provided to and reviewed by the AO.	T=O		
MSC-GD-8	Customers interested in registering their solution against this CP must register with NSA and receive approval prior to operating the solution.	T=O		
MSC-GD-9	The implementing organization must complete and submit an MSC CP requirements compliance matrix to their respective AO.	T=O		
MSC-GD-10	Registration and re-registration against this CP must include submission of CP registration forms and compliance matrix to NSA.	T=O		
MSC-GD-11	When a new approved version of the MSC CP is published by NSA, the AO must ensure compliance against this new CP within 6 months.	T=O		
MSC-GD-12	Solution implementation information that was provided to NSA during solution registration must be updated annually (in accordance with Section 14.3) as part of the annual re-registration process.	T=O		
MSC-GD-13	Audit log data must be maintained for a minimum of 1 year.	T=O		

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-GD-14	The amount of storage remaining for audit events must be assessed by the Security Administrator quarterly to ensure that adequate memory space is available to continue recording new audit events.	T=O		
MSC-GD-15	Audit data must be off-loaded to a backup storage medium at least once a week.	T=O		
MSC-GD-16	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.	T=O		
MSC-GD-17	The implementing organization must develop a continuity of operations plan for auditing capability that includes a mechanism or method for determining when the audit log is reaching its maximum storage capacity.	T=O		

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-GD-18	The implementing organization must develop a continuity of operations plan for auditing capability that includes a mechanism or method for off-loading audit log data for long-term storage.	T=O		
MSC-GD-19	The implementing organization must develop a continuity of operations plan for auditing capability that includes a mechanism or method for responding to an overflow of audit log data within a product.	T=O		
MSC-GD-20	The implementing organization must develop a continuity of operations plan for auditing capability that includes a mechanism or method for ensuring the audit log can be maintained during power events.	T=O		
MSC-GD-21	Strong passwords must be used that comply with the requirements of the AO.	T=O		
MSC-GD-10	Registration and re-registration against this CP must include submission of CP registration forms and compliance matrix to NSA.	T=O		

Req. #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-GD-22	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.	T=O		
MSC-GD-23	Local policy must dictate how the Security Administrator will install patches to Solution Components.	T=O		
MSC-GD-24	Solution Components must comply with local TEMPEST policy.	T=O		
MSC-GD-25	All hardware components must be tracked through an AO-approved inventory management process that identifies each component as part of a CSfC solution.	T=O		

2.2 REQUIREMENTS FOR INCIDENT REPORTING

Table 17 lists requirements for reporting security incidents to NSA to be followed in the event that a Solution Owner identifies a security incident that 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 Security Administrators, Certification Authority Administrators (CAAs), KGSAs, 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.

Table 17 only provides requirements directly related to the incident reporting process. See Section 11.9 for requirements supporting the detection of events that may reveal that a reportable incident has occurred.

Table 15. Incident Reporting Requirements

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-RP-1	Solution Owners must report confirmed incidents meeting the criteria in MSC-RP-3 through MSC-RP-14 within 24 hours of detection via the Joint Incident Management System (JIMS) or contacting NSA as specified in the CSfC Registration Letter issued for the solution.	T=O		
MSC-RP-2	At a minimum, the organization must provide the following information when reporting security incidents: • CSfC Registration Number • Primary POC name, phone, email • Alternate POC name, phone, email • Security 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)	T=O		

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-RP-3	Solution Owners must report a security failure in any of the CSfC Solution Components.	T=O		
MSC-RP-4	Solution Owners must report any evidence of a compromise or spillage of classified data caused by a failure of the CSfC solution.	T=O		
MSC-RP-5	For Gray network interfaces, Solution Owners must report any malicious inbound and outbound traffic.	T=O		
MSC-RP-6	Solution Owners must report any evidence of an unauthorized device/user gaining access to the classified network via the solution.	T=O		
MSC-RP-7	Solution Owners must report if a Solution Component sends traffic with an unauthorized destination address.	T=O		
MSC-RP-8	Solution Owners must report any malicious configuration changes to the components.	T=O		
MSC-RP-9	Solution Owners must report any unauthorized escalation of privileges to any of the CSfC Solution Components.	T=O		

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-RP-10	Solution Owners must report if two or more simultaneous VPN connections from different IP addresses are established using the same device certificate.	T=O		
MSC-RP-11	Solution Owners must report any evidence of malicious physical tampering with Solution Components.	T=O		
MSC-RP-12	Solution Owners must report any evidence that one or both layers of the solution failed to protect the data.	T=O		
MSC-RP-13	Solution Owners must report any significant degradation of services provided by the solution excluding connectivity issues associated with the Black network.	T=O		
MSC-RP-14	Solution Owners must report malicious discrepancies in the number of connections established by the Outer Encryption Component.	T=O		
MSC-RP-15	Solution Owners must report malicious discrepancies in the number of connections established by the Inner Encryption Component.	T=O		

Table 16. Role-Based Personnel Requirements

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-RB-1	The Security Administrators, CAAs, KGSAs, Auditors, and Integrators must be cleared to the highest level of data protected by the MSC Solution. When an Enterprise CA/KGS is used in the solution, the CAA/KGSA already in place may also support this solution, provided they meet this requirement. Black network Administrators may be cleared at the Black network security level.	T=O		
MSC-RB-2	The Security Administrator, CAA, KGSA, and Auditor roles must be performed by different people.	T=O		
MSC-RB-3	All Security Administrators, CAAs, KGSAs, and Auditors must meet local IA training requirements.	T=O		
MSC-RB-4	The CAA(s) for the inner tunnel must be different individuals from the CAA(s) for the outer tunnel.	T=O		
MSC-RB-5	The Security Administrator(s) for the Inner Encryption Components and supporting components on the Red network must be different individuals from the Security Administrator(s) for the Outer Encryption Components and supporting components on the Gray network.	T=O		

Req. #	Requirement Description	Threshold/ Objective	Alternative	Compliance (Explain how your solution meets requirement)
MSC-RB-6	Administrators must periodically inspect the physical attributes of infrastructure hardware for signs of tampering or other unauthorized changes.	T=O		
MSC-RB-7	The Auditor must review all logs specified in this CP at least once a day.	T=O		
MSC-RB-8	Security Administrators must initiate the certificate revocation/CAK destruction process prior to disposal of any Solution Component.	T=O		
MSC-RB-9	Auditing of the Outer and Inner CA operations must be performed by individuals who were not involved in the development of the Certificate Policy and CPS, or integration of the MSC Solution.	T=O		
MSC-RB-10	Auditing of the KGS operations must be performed by individuals who were not involved in the development of the KMP, or integration of the MSC Solution.	T=O		
MSC-RB-11	Mandatory Access Control policy must specify roles for Security Administrator, CAA, KGSA, and Auditor using role-based access controls.	O	None	

Table 17. Test (TR) Requirements

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