NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

COMMERCIAL SOLUTIONS for CLASSIFIED (CSfC)

Multi-Site Connectivity (MSC) Capability Package 1.3.0

Version 1.3.0
27 March 2026

CHANGE HISTORY

Title	Version	Date	Change Summary
Commercial Solutions for Classified (CSfC) Multi-Site Connectivity (MSC) Capability Package (CP)	1.3.0	27 March 2026	• Added new CNSA 2.0 objective requirements: MSC-SR-24, MSC-VG-19, MSC-VG-20, and MSC-AA-4. • Added new Approved CNSA 2.0 Algorithms Tables 2, 7, and 11. • Updated Section 2 to include CNSS Policy 15 algorithms. • Added Section 5.11 -- CNSA 2.0 IPsec. • Provided language clarification in section 5.1 and 4.1.3 regarding Public Internet. • Updated MSC-GD-10, MSC-GD-11, MSC-GD-15, MSC-SR-21 language to add more clarity. • Changed Management Workstation to Administrative Workstation. • Updated MSC-PS-8, MSC-PS-14, MSC-DM-20, MSC-DM-21 to remove “Optional”. • Updated Table 7 and included SHA-512. • Various formatting and document cleanup.

Title	Version	Date	Change Summary
CSfC MSC Capability Package	1.2.0	2 March 2023	• Clarified Logging. • Expanded Management Workstation Options. • Improved Community of Interest Separation Requirements. • Eliminated Transport Mode IPsec as an Alternate to Tunnel Mode IPsec. • Clarified Filtering Requirements. • Added Objective Requirements for Transmission Security (TRANSEC). • Updated the CP to fully use the MKA feature set (Objective Requirements). • Ensured clarification across the entire CP and supporting documents. • Minor administrative changes made in editing and formatting.
CSfC MSC Capability Package	1.1	26 June 2018	• Relocated Key Management Requirements from the CP to a separate "*CSfC Key Management Requirements Annex*". • Updated requirements to use "must" instead of "shall." • Minor administrative changes were made in formatting. • Added bullet #6 to the "Security Administrator" definition.
CSfC MSC Capability Package	1.0	23 February 2017	• Official release of CSfC MSC guidance.
CSfC MSC Capability Package	0.8	4 May 2016	• Initial release of CSfC Multi-Site Connectivity guidance.

Table of Contents

Table of Figures

List of Tables

1 INTRODUCTION

The Commercial Solutions for Classified (CSfC) program within the National Security Agency's (NSA's) Cybersecurity Directorate (CSD) publishes Capability Packages (CPs) to provide configurations that allow customers to independently implement secure solutions using layered Commercial Off-the-Shelf (COTS) products. The CPs are vendor-agnostic and provide high-level security and configuration guidance for customers and/or Solution Integrators.

The NSA delivers the CSfC Multi-Site Connectivity (MSC) CP to meet the demand for data-in-transit solutions using approved cryptographic algorithms and National Information Assurance Partnership (NIAP) evaluated components. These algorithms, known as the Commercial National Security Algorithm (CNSA) Suite, are used to protect classified data using layers of COTS products.

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

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

2 PURPOSE AND USE

This CP provides high-level reference designs and corresponding configuration requirements that allow customers to select COTS products from the CSfC Components List, available on the CSfC web page (https://www.nsa.gov/resources/commercial-solutions-for-classified-program), for their MSC Solution and properly configure products to achieve a level of assurance sufficient to protect classified data while in transit. As described in Section 10, customers must ensure that the components selected from the CSfC Components List provide the necessary functionality for the selected capabilities. To successfully implement a solution based on this CP, all Threshold (T) Requirements, or the corresponding Objective (O) Requirements applicable to the selected capabilities, must be implemented, as described in Sections 9 & 11.

Customers who want to use this CP must register their solution with the NSA. Additional information about the CSfC process is available on the CSfC web page (https://www.nsa.gov/resources/commercial-solutions-for-classified-program).

This CP will be reviewed twice a year to ensure that the defined capabilities and other instructions still provide the security services and robustness required. Solutions designed according to this CP must be

registered with the NSA. Once successfully registered, a registration acknowledgement letter will be sent validating that the MSC solution is registered as a CSfC solution and is approved to protect classified information. Any solution designed according to this CP may be used for one year and then be revalidated against the most recently published version of this CP. Top Secret Solutions will be considered on a case-by-case basis. Customers are encouraged to engage their Client Advocate or the CSfC PMO team early in the process to ensure the solutions are properly scoped, vetted, and that the customers understand the risks and available mitigations.

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

CNSS Policy No. 15, *Use of Public Standards for Secure Information Sharing,* identifies additional public algorithms to protect information within NSS. Specifically, the following algorithms are required to protect all NSS up to Top Secret:

- Confidentiality
  - AES 256
- Digital Signatures and Authentication
  - RSA 3072 or ECDSA P-384 (Threshold)
  - ML-DSA 87 (Objective)
- Key Establishment
  - DH 3072 or ECDH P-384 (Threshold)
  - ML-KEM 1024 (Objective)
- Hashing and Integrity
  - SHA-384 or SHA-512
- Software and Firmware Signing
  - Leighton-Micali Signature (LMS), Xtended Merkle Signature Scheme (XMSS) or ML-DSA 87 (Objective)

3 LEGAL DISCLAIMER

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

The User of this CP agrees to hold harmless and indemnify the U.S. Government, its agents and employees from every claim or liability (whether in tort or in contract), including attorney's fees, court costs, and expenses, arising in direct consequence of Recipient's use of the item, including, but not

limited to, claims or liabilities made for injury to or death of personnel of User or third parties, damage to or destruction of property of User or third parties, and infringement or other violations of intellectual property or technical data rights.

Nothing in this CP is intended to constitute an endorsement, explicit or implied, by the U.S. Government of any particular manufacturer's product or service.

4 DESCRIPTION OF MSC SOLUTION

This CP describes a general MSC Solution to protect classified information as it travels across either an untrusted Network, or a different security level network. The solution supports interconnecting two or more networks operating at the same security level via encryption tunnels, where the security level encompasses the classification level, list of compartments, dissemination controls, and other such controls over information. The solution provides sufficient flexibility to be applicable to many use cases of MSC implementations.

The MSC Solution uses two nested, independent encryption tunnels to protect the confidentiality and integrity of data as it transits the untrusted network. The two encryption tunnels protecting a data flow can use either Internet Protocol Security (IPsec) generated by a Virtual Private Network (VPN) Gateway or Media Access Control Security (MACsec) generated by a MACsec Device. VPN Gateways and MACsec Devices are implemented as part of the network infrastructure.

Throughout this CP, the term "Encryption Component" refers generically to either a VPN Gateway or a MACsec Device. "Inner Encryption Component" refers to the component that terminates the Inner layer of encryption and "Outer Encryption Component" refers to the component that terminates the Outer layer of encryption.

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

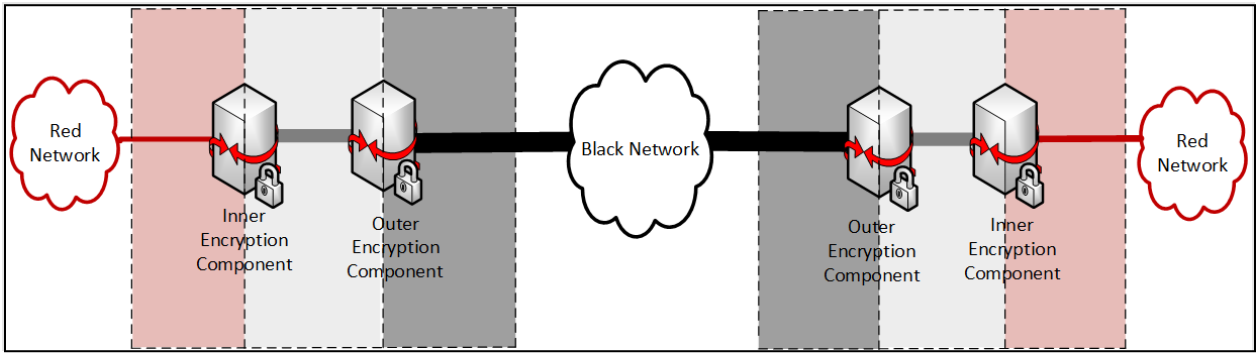

Figure 1. Two Encryption Tunnels Protect Data Across an Untrusted Network

The MSC CP instantiations are built using products from the CSfC Components List (see Section 9). Customers who are concerned that their desired products are not yet on the CSfC Components List are encouraged to contact the appropriate vendors to encourage them to sign a Memorandum of

Agreement with the NSA and commence evaluation against a NIAP-approved Protection Profile using the CSfC mandated selections that will enable them to be listed on the CSfC Components List. NIAP Certification alone does not guarantee inclusion on the CSfC Components List. Products listed on the CSfC Components List are not guaranteed to be interoperable with all other products on the CSfC Components List. Customers and Integrators should perform interoperability testing to ensure the components selected for their MSC Solution are interoperable. If you need assistance obtaining vendor Point of Contact (POC) information, please email csfc_components@nsa.gov.

4.1 NETWORKS

This CP uses the following terminology to describe the various networks in an MSC Solution and the types of traffic present on each. The terms Red, Gray, and Black refer to the level of protection applied to the data as described below.

4.1.1 RED NETWORK

Red data consists of unencrypted classified data. The Red Network is logically located behind an Inner Encryption Component. The networks connected to one another through the MSC Solution are Red Networks. Red Networks may only communicate with one another through the MSC Solution if the networks operate at the same security level. Red Networks are under the control of the Solution Owner or a trusted third party using a Red Administrative Workstation (AW). The Red AWs maintain, monitor, and control all security functions for the Inner Encryption Components, Inner Firewall, and all Red Management Service Components. The Red AWs are not permitted to maintain, monitor, or control Outer Encryption Components or Gray Management Services.

4.1.2 GRAY NETWORK

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

The Gray Network is physically treated as a classified network even though all classified data is singly encrypted. If a Solution Owner's classification authority determines that the data on a Gray Network is classified, perhaps by determining the Internet Protocol (IP) addresses used on the Gray Network interfaces are classified at some level, then the MSC Solution described in this CP cannot be implemented. The MSC Solutions are not designed to ensure that such information will be afforded two layers of protection.

Gray Network components consist of the Outer Encryption Component, Gray Firewall, and Gray Management Services. All Gray Network components are physically protected at the same level as the Red Network components of the MSC Solution. Gray Management Services are physically connected to the Gray Firewall and include, at a minimum, a AW that can be a physical workstation or Virtual Machine (VM). The Gray Management Services may also include a Security Information and Event Management (SIEM) unless the SIEM is implemented in the Red Network in conjunction with a cross domain solution (CDS) (see *CSfC Continuous Monitoring Annex*). This CP requires the management of Gray Network components through a Gray AW. As a result, neither Red nor Black AWs are permitted to manage the Outer Encryption Component, Gray Firewall, or Gray Management Services. Additionally, the Gray AWs

are prohibited from managing Inner Encryption Components. Inner Encryption Components must be managed from a Red AW.

4.1.3 BLACK NETWORK

Black data is classified data that has been encrypted twice. The network connecting the Outer Encryption Components together is a Black Network. Black Networks may be referred to as Black transport networks. Black Networks are not necessarily (and often will not be) under the control of the Solution Owner, and may be operated by an untrusted third party. As shown in Figure 2, if the Black Network is an untrusted network such as the Public Internet, an Outer Firewall is required between the Black Network and the Outer Encryption Component.

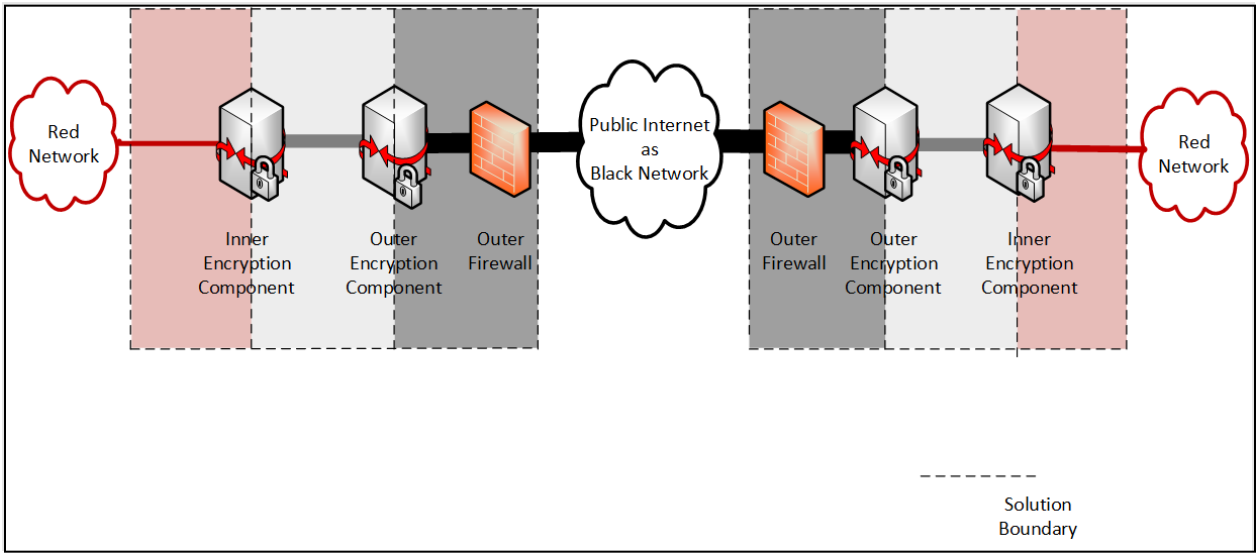

Figure 2. MSC Solution Using the Public Internet as the Black Transport Network

4.1.4 DATA, MANAGEMENT AND CONTROL PLANE TRAFFIC

Data plane traffic is classified information, encrypted or unencrypted, that passes through the MSC Solution. The MSC Solution exists to encrypt and decrypt data plane traffic. All data plane traffic within the Gray and Black Networks is encapsulated within the IPsec's Encapsulating Security Payload (ESP) and/or MACsec protocols.

Management plane traffic is used to configure and monitor Solution Components. It includes the communications between a system administrator and a component, as well as the logs and other status information forwarded from a Solution Component to a SIEM, or similar repository. Management plane traffic on Red and Gray Networks is encapsulated within the Secure Shell version 2 (SSHv2), IPsec, MACsec, or Transport Layer Security (TLS) 1.2 or later protocols.

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

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

In general, this CP does not impose detailed requirements on control plane traffic, although control plane protocols may be used to implement certain requirements. For example, requirements MSC-SR-3 and MSC-SR-4 (see Section 10.1) require that time synchronization be performed but does not require the use of any particular time synchronization protocol or technique. Notable exceptions are for IPsec session establishment and for certain certificate status distribution scenarios where, given their impact on the security of the solution, this CP does provide detailed requirements. Restrictions are also placed on control plane traffic for the Outer Encryption Component. The Outer Encryption Component is prohibited from implementing routing protocols on external and internal interfaces. The Outer Encryption Component may not perform routing functionality. If an Outer Firewall is present, the Outer Firewall can perform routing functions.

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

Data plane and management plane traffic must be physically and cryptographically separated from one another. Use of a Virtual Local Area Network (VLAN) alone is not sufficient to separate data plane and management plane traffic. As a result, a solution may have a Gray Data Network and a Gray Management Network that are separate from one another, where the components on the Gray Management Network are used to manage the components on the Gray Data Network. Unless otherwise specified given that some control plane traffic is necessary for a network to function, there is no general requirement that control plane traffic be similarly separated.

4.2 HIGH LEVEL DESIGN

Depending on the needs of the customer implementing the solution, the MSC Solution is adaptable to support capabilities for multiple sites and/or multiple security levels. If a customer does not have a need to support multiple sites or multiple security levels, then those elements need not be included as part of the implementation. As explained in Section 8, any implementation of the MSC Solution must satisfy all of the applicable requirements specified in this CP.

4.2.1 MULTIPLE SITES

Sites in the solution may be managed independently of one another or may be remotely managed from a central site.

Figure 3 shows two Red Networks at different sites that operate at the same security level and connected to one another through the MSC Solution. Here, each Red Network has two Encryption Components associated with it; an Inner Encryption Component connected to the Red Network, and an Outer Encryption Component between the Inner Encryption Component and the Black Network.

There are two layers of encryption tunnels between any pair of sites communicating directly with one another; one encryption tunnel between their Outer Encryption Components, and a second encryption tunnel between their Inner Encryption Components. Each set of Inner or Outer Encryption Components can provide encryption using either IPsec or MACsec.

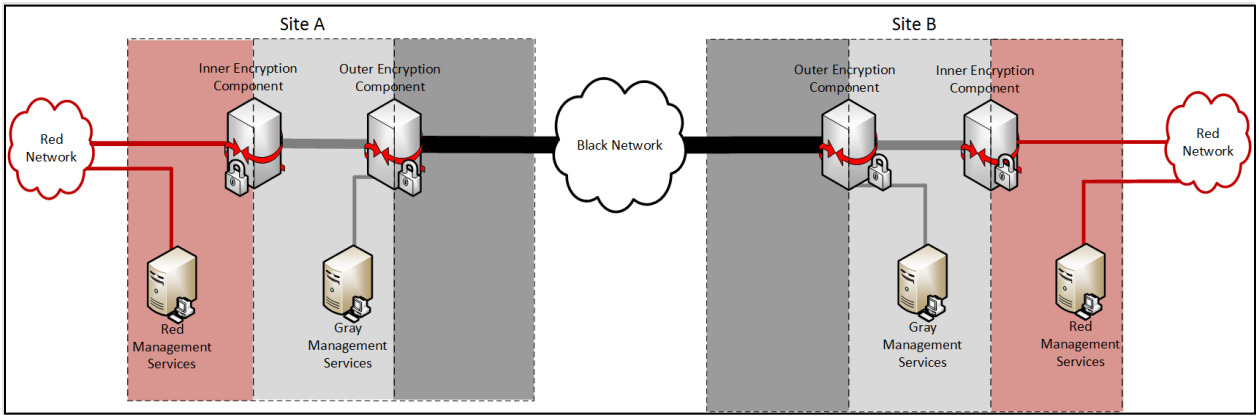

Figure 3. MSC Solution Connecting Two Independently Managed Sites

There is no limit to the number of sites that may be incorporated into a single MSC Solution.

4.2.1.1 Independently Managed Sites

For independently managed sites, each site performs the administration of its own Encryption Components. If Certification Authorities (CAs) are part of the MSC Solution, each site has the option to use either locally run CAs that they manage and control or, where available, enterprise CAs that are not necessarily managed by the Solution Owner. Each site needs to ensure that the Encryption Components selected interoperate with those at the other sites.

When using independent managed sites, management traffic will not cross the Black Network, encrypted or unencrypted. In the MSC Solution, Encryption Components at each site using public key certificates need to have the signing certificates and revocation information for the corresponding CAs used by the other sites. This high-level design requires cooperation between the various sites in the solution to ensure that all CAs used by each site are trusted at all the other sites. Similarly, MACsec Devices using a Connectivity Association Key (CAK) need to have the same CAK used by the other site in the MSC Solution. If MACsec Devices are authenticating using certificates, the authentication server (AS) must not connect to both Gray and/or Red Networks.

This model has the advantage of allowing communication between larger organizations that have a need to share information while maintaining independence.

Note that while Figure 3 shows only two sites, this solution can scale to include numerous sites, with each additional site having the same design as that in Figure 3.

4.2.1.2 Centrally Managed Sites

As shown in Figure 4, if remote management is used, personnel at a single geographic site administer and perform keying and device management for all the sites included in the solution. In this case, because the administration is done by one group of Security Administrators, CA Administrators, and Key Generation Solution Administrators (see Section 12), they ensure the interoperability of each site as new sites are added. At least two CAs are needed; one for all the Inner Encryption Components and one for all the Outer Encryption Components. If available, enterprise CAs should be used. If MACsec Devices are used on either or both layers and EAP-TLS is used for authentication, then CAs and an AS located at the Central site are required, otherwise, PSKs may be used for authentication for one of the layers of the solution and that layer would not require a CA.

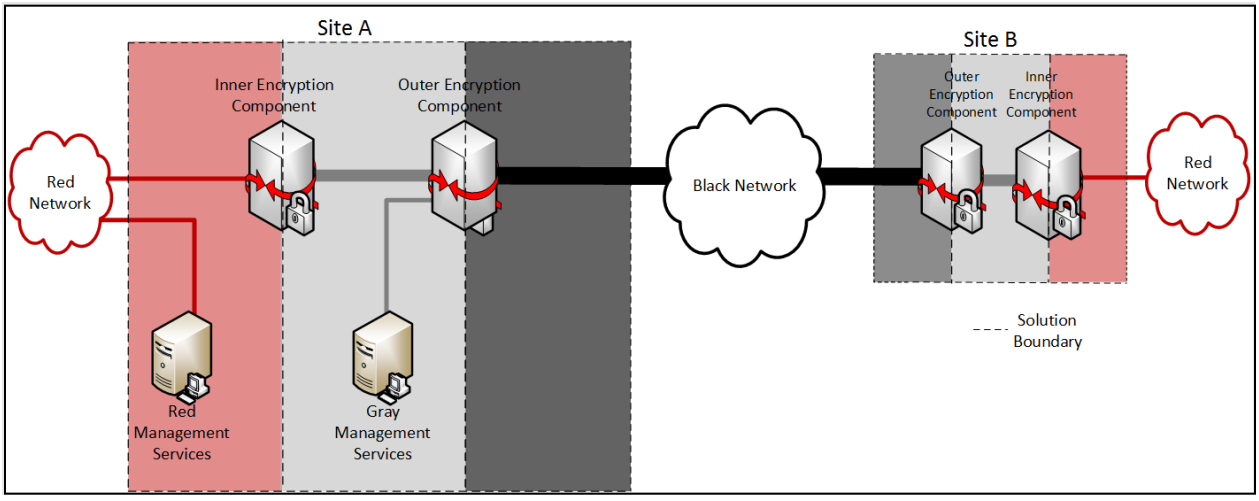

Figure 4. MSC Solution Connecting a Central Management Site and a Remote Site

Because the central management site manages the Encryption Components at the other sites over the network, encryption is used to logically separate data and management traffic as it passes between sites. Central Management of the Gray Network must be done in accordance with the *CSfC Enterprise Gray Implementation Requirements Annex*. Red management traffic is encrypted before being routed through the Inner and Outer Encryption Components to another site. As a result, all management traffic between sites is encrypted at least twice before traversing the Black Network. See the *CSfC Enterprise Gray Implementation Requirements Annex* for additional details and requirements.

While Figure 4 shows only two sites, this solution can scale to include numerous sites, with each additional site having the same high-level design as the remotely managed site.

4.2.2 Multiple Security Levels

A single implementation of the MSC Solution may support Red Networks of different security levels. The MSC Solution provides secure connectivity between the Red Networks within each security level while preventing Red Networks of different security levels from communicating with one another. This enables a customer to use the same physical infrastructure to carry traffic from multiple networks. Although each Red Network requires its own Inner Encryption Component, a site may use a single Outer Encryption Component to encrypt and transport traffic that has been encrypted by Inner Encryption Components of varying security levels.

There is no limit to the number of different security levels that an MSC Solution may support. An unclassified network can also be included behind the Outer Encryption Component but must be behind its own Inner Encryption Component and meet the requirements in this CP as if it was a Red Network.

MSC Solutions supporting multiple security levels may include independently managed sites (see Section 4.2.1.1) or centrally managed sites (see Section 4.2.1.2). Given both cases, separate CAs, CAKs, and management devices are needed to manage the Inner Encryption Components at each security level. For example, Figure 5 shows a Central Management Site (Site A) and a Remote Site (Site B), but network 1 and network 2 each has its own Red Management Services, which prevents the Inner Encryption Components of the two networks from being able to authenticate with one another.

4.2.2.1 Networks Operating at the Same Security Level

When Red Networks that operate at the same security level are implemented, the cryptographic separation provided by the Inner Encryption Components is sufficient to protect against unintended data flows between the two networks. Two Inner Encryption Components for networks of different security levels will be unable to mutually authenticate with each other because they trust different CAs that do not have a trust relationship with one another or they use different CAKs that will not provide authentication. This difference prevents the establishment of an encryption tunnel between the two components.

Figure 5 shows an MSC Solution between two sites that carries traffic between two Red Networks; a Secret U.S.-only Network (Network 1), and a Secret U.S.-only Network (Network 2). Because Network 1 and Network 2 both operate at the same security level, their singly-encrypted traffic can be carried over the Gray Network without any additional security controls in place.

Although not required by this CP, a Solution Owner may choose to implement the additional security described in Section 4.2.2.2 to provide additional protection against unintended data flows between Red Networks at the same security level.

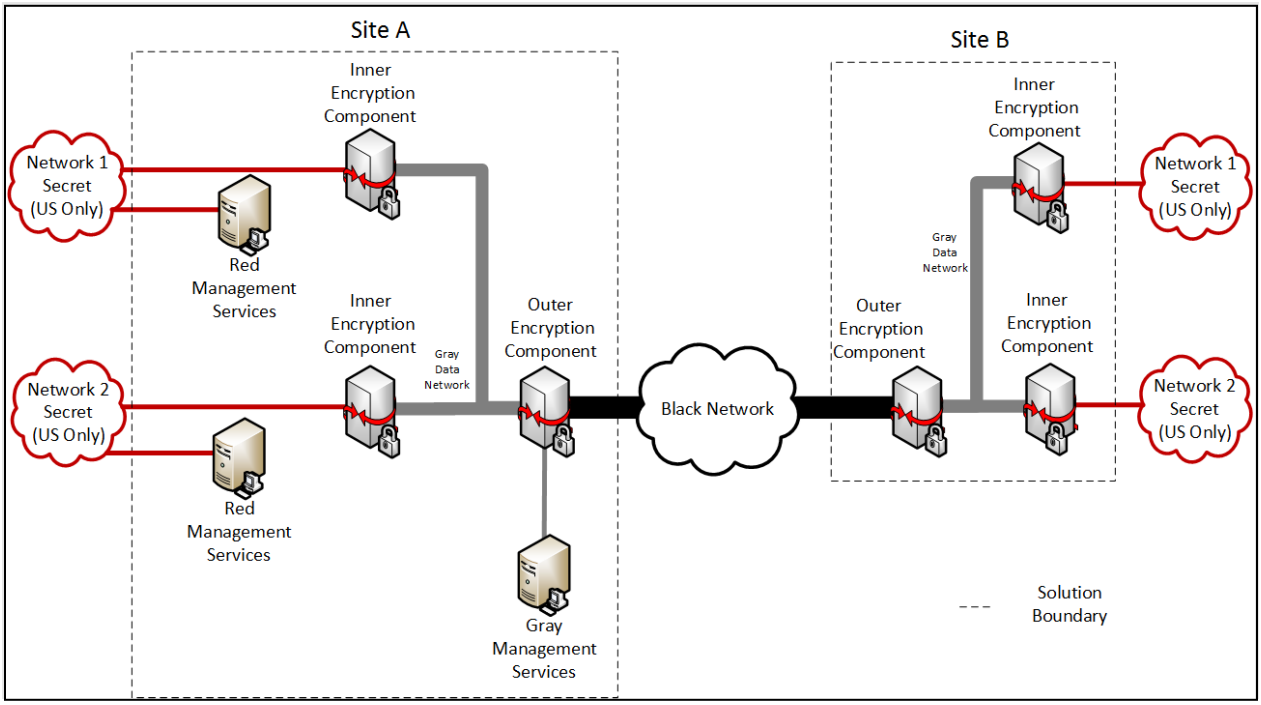

Figure 5. MSC Solution for Two Networks at the Same Security Level

4.2.2.2 Networks Operating at Different Security Levels

A single implementation of the MSC Solution may support Red Networks of different security levels, to include unclassified networks. The MSC Solution provides secure connectivity between the Red Networks within each security level while preventing Red Networks of different security levels from communicating with one another. This enables a customer to use the same infrastructure to carry traffic from multiple networks.

For Red Networks of different security levels, the cryptographic separation of their traffic on a Gray Network, as described in Section 4.2.2.1, is still present. However, because the consequences of an unintended data flow between different security levels are more severe than of one with a single security level, an additional mechanism is necessary to prevent such a flow from occurring.

This CP uses packet filtering within Gray Networks as an additional mechanism to prevent data flows between networks of different security levels. Any physical path through a Gray Network between multiple Inner Encryption Components supporting Red Networks of different security levels must include at least one filtering component. This filtering component restricts the traffic flow based primarily on the Gray Network source and destination addresses, and only allows a packet through if the source and destination components intend to communicate with one another and drops the packet if they are not.

When multiple security levels are used, it is critical to enforce proper IP address assignment and firewall rule sets. The IP address assigned must be unique to that security level such that each network's Inner Encryption Component is only able to send and receive traffic to its respective Inner Encryption Component at the other site.

Additionally, filtering components are included between the components used for management of the Gray Networks themselves (namely, AWs and locally run CAs) and Inner Encryption Components that support Red Networks of a lower security level than the Red Network with the highest security level supported by the solution. In other words, AWs and locally run CAs on Gray Networks are treated as, and grouped with, the Inner Encryption Component for the Red Network with the highest security level.

One or more Gray Firewalls must be included in the Gray Network to perform filtering. Standalone Gray Firewalls have been placed at each site between the Inner Encryption Components and the Outer Encryption Component; these Gray Firewalls are responsible for dropping packets between Inner Encryption Components of different security levels.

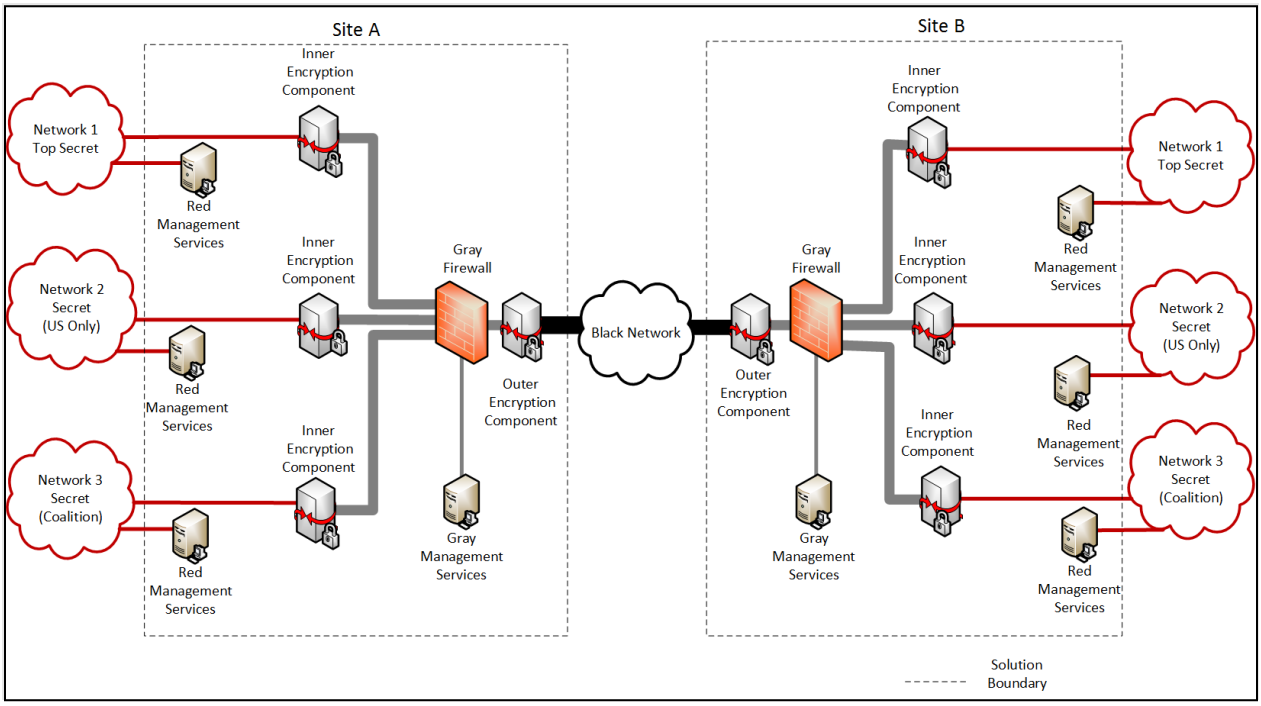

Figure 6. MSC Solution for Networks at Different Security Levels

Figure 6 also shows an example placement of Gray Firewalls, as long as any path between Inner Encryption Components for networks of different security levels includes a Gray Firewall.

Including one or more standalone Gray Firewalls in a solution does not remove the requirement to perform the filtering on the Outer Encryption Component as well. Outer Encryption Components are uniquely positioned to block traffic between Inner Encryption Components supporting Red Networks of different security levels when one of those Inner Encryption Components is located at a different site.

4.2.3 Layering Options

Each layer of the MSC Solution can use either an IPsec tunnel or MACsec tunnel. An IPsec tunnel is established between VPN Gateways. A MACsec tunnel is established between MACsec Devices. Table 1 identifies four different layering options provided by this CP. For configurations 2 and 4 which use an outer MACsec tunnel these solutions would only be point to point solutions instead of a multi-site solution.

Table 1. Layering Options

Configuration	Inner	Outer Tunnel
1	IPsec	IPsec
2	IPsec	MACsec
3	MACsec	IPsec
4	MACsec	MACsec

MACsec was designed to provide hop-to-hop security within a Local Area Network (LAN). As MACsec-encrypted traffic arrives at an interface, it is typically decrypted, examined, and re-encrypted after determining its destination.

The MACsec-encrypted traffic needs to be encapsulated if the MACsec Device is the first layer of encryption in the MSC Solution or if the MACsec-encrypted traffic needs to traverse an IP-based network. Encapsulation creates a new packet by adding a new header, and sometimes trailer, to the MACsec-encrypted traffic. Encapsulation ensures the MACsec-encrypted traffic is not decrypted prior to reaching its destination and ensures the second layer of encryption can be applied.

In some commercial MACsec Devices, encapsulation can be applied on the internal interface by creating a pseudowire (see Figure 7), which emulates a point-to-point connection. If this feature is not supported, a standalone device is needed to encapsulate the MACsec-encrypted data (see Figure 8). If using a standalone device, the internal interface will be connected to the Inner MACsec Device and the external interface will be connected to the Outer Encryption Component. Since this device resides in the Gray Network, all requirements for Solution Components must be implemented.

This CP does not mandate the use of a specific protocol for encapsulation. Options include, but are not limited to, Layer 2 Tunneling Protocol version 3, and Ethernet over Multiprotocol Label Switching.

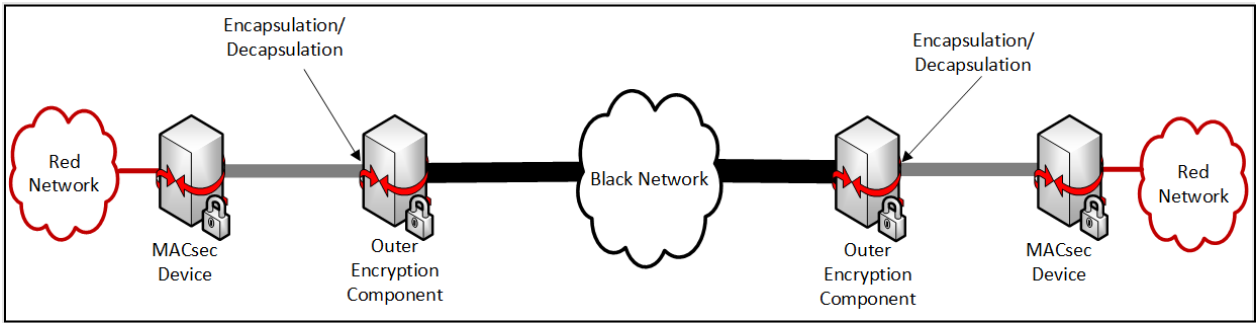

Figure 7. Encapsulating MACsec on an Internal Interface

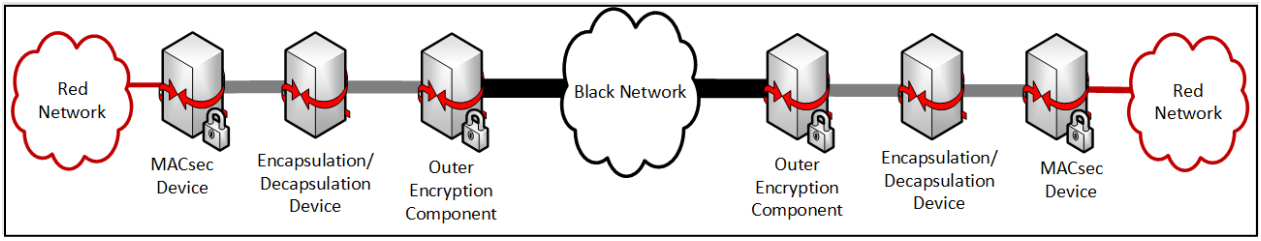

Figure 8. Encapsulating MACsec with a Separate Device

When the Inner Encryption Component is a MACsec Device the traffic requires additional encapsulation before it is passed through the Outer Encryption Component to the Black Network. This additional step falls outside the boundary of the MSC Solution. However, it is highly recommended to apply the general device management (DM) and port filtering requirements for Solution Components.

In the current MACsec standard, the entire frame is encrypted with the exception of the source and destination addresses. Institute of Electrical and Electronics Engineers (IEEE) 802.1AE-2018 provides the option of moving the Virtual Local Area Network (VLAN) identification (ID) tag out of the encrypted payload and into the clear in the header. The benefits of moving the VLAN ID tag into the clear include service multiplexing (i.e., multiple point-to-point or multipoint services existing on a single physical interface) and providing quality of service across a Service Provider's network. If supported in the MACsec Device, this CP allows VLAN ID tags to be used in the clear.

At high speeds (100 GB/s or higher), some MACsec Devices may be configured to use an extended Packet Number (XPN), as described in IEEE 802.1AE-2018. Without XPN, the unique packet numbers may be exhausted quickly at high speeds and re-keying at high speeds may interrupt traffic flow. If supported in the MACsec Device, this CP allows the XPN feature to be used.

4.2.4 AUTHENTICATION

The MSC Solution provides mutual device authentication between Outer Encryption Components and between Inner Encryption Components. The method of authentication is different for VPN Gateways and MACsec Devices.

VPN Gateways authenticate via public key certificates. VPN Gateways may also implement Internet Engineering Task Force (IETF) Request for Comments (RFC) 8784-compliant IKEv2 and use Pre-Shared Key (PSK) in addition to public key certificates to provide quantum resistant confidentiality.

MACsec Devices authenticate using a PSK called a CAK or using EAP-TLS over 802.1X to pass public key device certificates for mutual authentication between devices. The EAP-TLS mechanism is used to mutually authenticate and get the Master Session Key (MSK) from which the Connectivity Association Key (CAK) is derived for the MACsec Key Agreement (MKA) protocol. For each MACsec tunnel, a Key Server is identified. The Key Server authenticates the other MACsec Device and issues a Secure Association Key to provide confidentiality and integrity for the MACsec tunnel.

This CP requires all authentication certificates issued to VPN Gateways and MACsec Devices to be Non-Person Entity certificates. This CP also requires all CAKs and their associated Connectivity Key Names (CKNs) to be generated using an NSA-approved Key Generation Solution (KGS). Guidance and requirements for using PSKs, including RFC 8784 compliance, can be found in the *CSfC Symmetric Key*

Management Requirements Annex, and guidance and requirements for using public key certificates can be found in the *CSfC Key Management Requirements Annex*.

4.3 OTHER PROTOCOLS

Throughout this CP, when IP traffic is discussed, it may refer to either Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) traffic, unless otherwise specified, as the MSC Solution is agnostic to most named data handling protocols. In addition, Red, Gray and Black Networks can run either IPv4 or IPv6, and each network can independently make that decision. In the remainder of the CP, if no protocols or standards are specified then any appropriate protocols may be used to achieve the objective.

Public standards conformant Layer 2 control protocols, such as ARP, are allowed as necessary to ensure the operational usability of the network. Public standards conformant Layer 3 control protocols, such as Internet Control Message Protocol (ICMP), may be allowed based on local Authorizing Official (AO) policy, but the default configuration of this solution is for all Layer 3 control protocols to be disabled. Red and Gray Network multicast messages and Internet Group Management Protocol or Multicast Listener Discovery may also be allowed depending on local AO policy. Multicast messages received on external interfaces of the Outer Encryption Component must be dropped.

The MSC Solution can be implemented to take advantage of standards-based routing protocols that are already used in the Black and/or Red Network. For example, networks that currently use Generic Routing Encapsulation (GRE), Multiprotocol Label Switching or OSPF protocols can continue to use these in conjunction with this solution to provide routing as long as the AO approves their use.

4.4 AVAILABILITY

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

Figure 9 shows an MSC Solution between two sites where each site has a redundant Outer Encryption Component (Management components are omitted from the figure for clarity). There are two outer encryption tunnels that transit the Black Network: one between the upper pair of Outer Encryption Components, and one between the lower pair of Outer Encryption Components. Each site's Gray Network contains an ordinary router between the Inner and Outer Encryption Components that selects which Outer Encryption Component to route outbound packets. This router is part of the solution only in the sense that it is part of the network infrastructure of the Gray Network; this CP does not levy any security requirements on the router/switch. The MSC Solution can maintain connectivity between the two sites even if one of the Outer Encryption Components fails because traffic will be routed through the tunnel that has not failed.

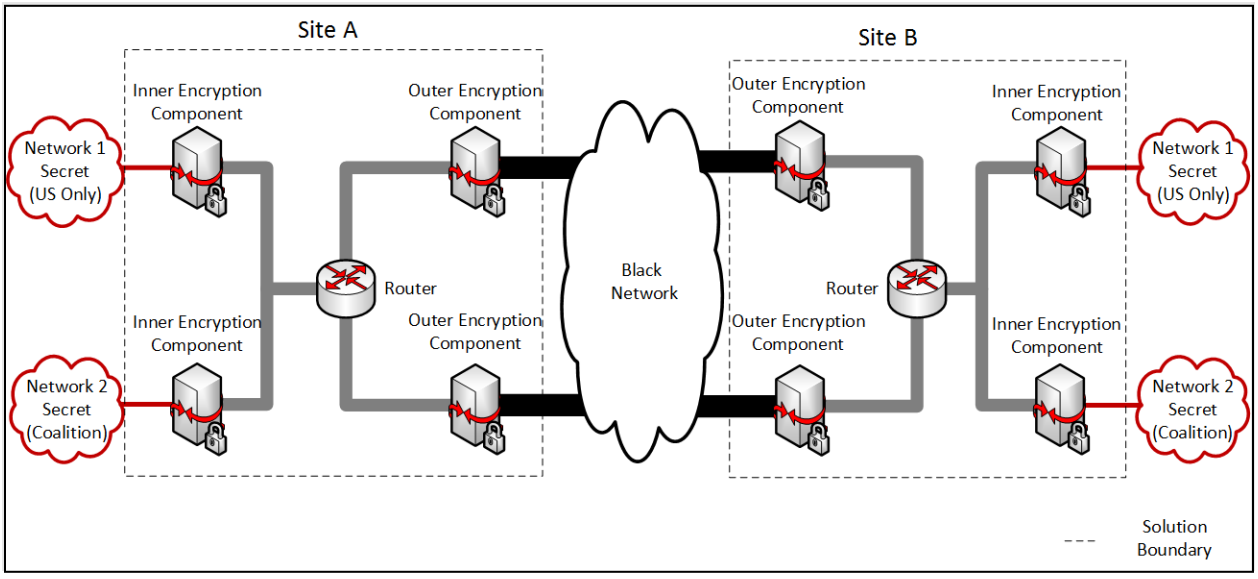

Figure 9. MSC Solution with Redundant Outer Encryption Components

Figure 9 shows a simple example of how redundancy could be added, if needed, for an MSC Solution. Implementing standby or failover Encryption Components, performing load balancing between Encryption Components, or other techniques to improve the availability or throughput of the solution are outside the scope of this CP and are not discussed further.

5 SOLUTION COMPONENTS

In the high-level designs discussed in Section 4.2, all communications flowing across a Black Network are protected by at least two layers of encryption, implemented using IPsec tunnels generated by VPN Gateways or MACsec tunnels generated by MACsec Devices. Mandatory aspects of the solution also include AWs, CAs for key management using Public Key Infrastructure (PKI), a KGS for generating pre-shared CAKs, and Gray Firewalls when networks of different security levels share the same Outer Encryption Component.

Each Solution Component is described in more detail below. The descriptions include information about the security provided by the components as evidence for why they are deemed necessary for the solution. Components are selected from the CSfC Components List in accordance with the Product Selection requirements of this CP (see Section 9).

All the individual components within the solution must be physically protected to the level of the connected network with the highest classification/protection level. The only exception to this requirement would be the Outer Firewall if one is present in the solution.

Additional components, discussed in the *CSfC Key Management Requirements Annex* and *CSfC Symmetric Key Management Requirements Annex* can be added to the solution to help reduce the overall risk. However, these are not considered mandatory components for the security of the solution; therefore, this CP does not place configuration or security requirements on those components.

5.1 OUTER FIREWALL

An MSC Solution that uses an untrusted network such as the Public Internet as its Black Network must include an Outer Firewall (see Section 4.1.3). The Outer Firewall is located at the edge of the MSC Solution and is connected to the Black Network.

The external interface of the Outer Firewall only permits IPsec or MACsec traffic with a destination address of the Outer Encryption Component.

The internal interface of the Outer Firewall only permits IPsec or MACsec traffic with a source address of the Outer Encryption Component and any necessary control plane traffic. The minimum requirements for port filtering on the Outer Firewall can be found in Section 10.6.

As shown in Figure 2, the Outer Firewall, selected from the CSfC Components List, must be physically separate from the Outer Encryption Component.

5.2 OUTER ENCRYPTION COMPONENT

The Outer Encryption Component can be either a VPN Gateway or a MACsec Device. The Outer Encryption Component establishes an encrypted tunnel using IPsec or MACsec with peer Outer Encryption Components, which provides device authentication, confidentiality, and integrity of information traversing Black Networks.

If the Black Network is the Public Internet, the external interface of the Outer Encryption Component is connected to the internal interface of the Outer Firewall. Otherwise, the external interface of the Outer Encryption Component is connected to the Black Network. The internal interface of the Outer Encryption Component is connected to Gray Firewalls, if required, or Inner Encryption Components. If the Black Network is the Public Internet, Transmission Security (TRANSEC) must be enabled to provide additional security.

The Outer Encryption Component may be a perimeter device (if the Outer Firewall is not present) and more exposed to external attacks. The Outer Encryption Component may use internal filtering to help protect the network from unauthenticated traffic. This allows specification of rules that prohibit unauthorized data flows, which helps mitigate Denial of Service attacks and resource exhaustion. This CP does not require that the Outer Encryption Component terminate all tunnels on a single physical interface; however, all such external interfaces must conform to the port filtering requirements in Section 10.6. The Outer Encryption Component is implemented identically for all the high-level designs covered in this CP.

Outer Encryption Components are also responsible for filtering traffic on its Gray Network interfaces to prevent Inner Encryption Components for networks of the same security level from being able to send packets to one another. Since this filtering is primarily based on the source and destination addresses in the packet on a Gray Network, the Gray Network itself must use an addressing scheme that supports the necessary filtering (such as using separate address ranges for the Gray interfaces of Inner Encryption Components supporting each Red Network).

The Outer Encryption Component is prohibited from implementing routing protocols on external and internal interfaces and must rely on an Outer Firewall or Gray Firewall to provide dynamic routing

functionality. The Outer Encryption Component, selected from the CSfC Components List, must be physically separate from the Outer Firewall and Gray Firewall.

The Outer Encryption Component cannot route packets between Gray and Black Networks; any packets received on a Gray Network interface and sent out on a Black Network interface must be transmitted within an IPsec or MACsec tunnel configured according to this CP. As described in this CP, Management traffic on a Gray Network, which originates from the AW, must include two layers of encryption.

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

5.3 GRAY FIREWALL

The Gray Firewall is located between the Outer Encryption Component and Inner Encryption Component(s). As described in Section 4.2.2.2, an MSC Solution that supports multiple Red Networks of different security levels must include one or more Gray Firewalls. The Gray Firewall blocks any packets sent between Inner Encryption Components for Red Networks of different security levels. A Gray Firewall also blocks any packets sent between management components on the Gray Network and Inner Encryption Components for Red Networks that operate at a security level other than the highest security level of data protected by the solution. Gray Firewalls are physically protected as classified devices.

As shown in Figure 6, a standalone Gray Firewall, selected from the CSfC Components List, must be physically separate from the Outer Encryption Component and Inner Encryption Component. A Gray Firewall would typically only be used in solutions where the physical design of the Gray Network includes paths between Inner Encryption Components for Red Networks of different security levels that do not pass through the Outer Encryption Components. Effectively, each Gray Firewall is another instance of the Gray Network filtering performed by the Outer Encryption Component. For load balancing or other performance reasons, multiple Gray Firewalls that comply with the requirements of this CP are acceptable.

5.4 GRAY MANAGEMENT SERVICES

Secure administration of components in the Gray Network and continuous monitoring of the Gray Network are essential roles provided by the Gray Management Services. Gray Management Services are composed of multiple components that provide distinct security to the solution. This CP allows flexibility in the placement of some Gray Management Services as described below. The Gray Management Services are physically protected as classified devices.

5.4.1 GRAY ADMINISTRATIVE WORKSTATION (AW)

The Gray AW maintains, monitors, and controls all security functionality for the Outer Encryption Component, Gray Firewall, and all Gray Management Service components. The Gray AW is not permitted to maintain, monitor, or control Inner Encryption Components or Red Management Services. All MSC Solutions must have at least one Gray AW.

5.4.2 GRAY SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

The Gray SIEM collects and analyzes log data from the Outer Encryption Component, Gray Firewall, and other Gray Management Service components. Log data should be encrypted between the originating component and the Gray SIEM with SSHv2, TLS 1.2 or later, IPsec, or MACsec to maintain confidentiality

and integrity of the log data. The SIEM is configured to provide alerts for specific events including if the Outer Encryption Component or Gray Firewall receives and drops any unexpected traffic that could indicate a compromise. These functions can also be performed on a Red SIEM using an approved CDS, as described in the *CSfC Continuous Monitoring Annex.* A Gray SIEM is not a mandatory component of the MSC Solution.

5.5 Inner Encryption Components

Inner Encryption Components can either be VPN Gateways or MACsec Devices. For load balance or other performance reasons, multiple Inner Encryption Components that comply with the requirements of this CP are acceptable.

Similar to an Outer Encryption Component, an Inner Encryption Component provides authentication of peer VPN Gateways or MACsec Devices, cryptographic protection of data in transit, and configuration and enforcement of network packet handling rules.

Similar to the Outer Encryption Component, the external interface of the Inner Encryption Component only permits egress of IPsec/MACsec traffic and AO-approved control plane traffic. The internal interface of the Inner Encryption Component is configured to only permit traffic with an IP address and port associated with Red Network services.

The Inner Encryption Component must not route packets between Red and Gray Networks; any packets received on a Red Network interface and sent to a Gray Network interface must be transmitted within an IPsec or MACsec tunnel configured according to this CP. The Inner Encryption Component, selected from the CSfC Components List, must be physically separate from the Gray Firewall and Inner Firewall, if either are required by this CP.

When an Inner MACsec Device is used, the MACsec traffic needs to be encapsulated prior to being processed by the Outer Encryption Component, regardless of whether it is a VPN Gateway or a MACsec Device. Some VPN Gateways and MACsec Devices allow this encapsulation to occur on the incoming interface, prior to encrypting traffic for the outer tunnel. If the selected VPN Gateway or MACsec Device does not have this feature, a separate standalone router or switch is necessary to provide encapsulation and all requirements for Solution Components in this CP must apply to it. Any AO-approved encapsulation protocol may be used.

5.6 Inner Firewall

An Inner Firewall is located between the Inner Encryption Component and the Red Network. In this CP, an Inner Firewall is not required. If the MSC Solution is deployed with solutions from other CSfC CPs then those CPs will specify the Inner Firewall requirements.

5.7 Red Management Services

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

5.7.1 RED ADMINISTRATION MANAGEMENT COMPONENTS

The Red AWs maintain, monitor, and control all security functions for the Inner Encryption Components, Inner Firewall, and all Red Management Service components. The Red AWs are not permitted to maintain, monitor, or control Outer Encryption Components or Gray Management Services. All MSC Solutions will have at least one Red AW.

5.7.2 RED SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Red SIEMs collect and analyze log data and flow data from the Inner Encryption Components, the Inner Firewall and other Red Management Service components. Log data should be encrypted between the originating component and the Red SIEM with SSHv2, TLS 1.2 or later, IPsec, or MACsec to ensure confidentiality and integrity. The SIEM is configured to provide alerts for specific events.

5.8 MSC AUTHENTICATION SERVER (AS)

The MSC AS is responsible for mutual authentication between MACsec Devices. Authentication must be established between the MACsec device and the AS, where each MACsec device must perform the functions of a supplicant and authenticator. This communication is used throughout the EAP-TLS negotiation to mutually authenticate two MACsec Devices to pass MACsec traffic. Objectively, the MSC Authentication Server should use CNSA 2.0-compliant algorithms as part of the EAP-TLS negotiation to mutually authenticate the MACsec Devices with ML-KEM 1024 for key establishment and ML-DSA 87 for digital signatures as vendors enable support for these algorithms.

5.9 KEY AND CERTIFICATE MANAGEMENT COMPONENTS

Key Management Requirements have been relocated to a separate *CSfC Key Management Requirements Annex* and the *CSfC Symmetric Key Management Requirements Annex.*

5.10 OTHER CONTROLS

There are additional controls that could be used within this solution to potentially reduce the overall risk. A screening router can be used to filter packets from Black Networks before they arrive at Outer Encryption Components. The screening router could be part of an existing Black Network (e.g., Customer Edge Router), or could be added between Outer Encryption Components and existing Black Network components. However, since the screening router would become part of a Black Network, it is not considered to be part of the MSC Solution itself.

Additionally, if an Integrator is used for implementation of this solution, the customer can require separation of roles between individuals working on Red and Gray components. The separation of roles ensures that during the development of the solution no single individual can compromise Red and Gray components simultaneously.

5.11 CNSA 2.0 IPSEC

As part of the CNSA 2.0 migration, the VPN Gateways will have to implement CNSA 2.0-compliant key establishment and digital signatures. As of now, this is an objective design feature but will be required in the future for the use of IPsec in MSC. The CNSA Suite 2.0 is relevant to the choice of cryptography employed in IPsec and especially affects the Internet Key Exchange Protocol Version 2 (IKEv2) key establishment construction, requiring support for several new RFCs. NSA has worked with industry to develop an implementation profile, CNSA Suite 2.0 Profile for IPsec (*draft-guthrie-cnsa2-ipsec-profile*).

The draft profile (*draft-guthrie-cnsa2-ipsec-profile*) specifies the use of the CNSA 2.0-compliant algorithms ML-KEM-1024 [FIPS203] for key establishment and ML-DSA-87 [FIPS204] for digital signatures within IPsec. It describes the use of RFCs that are required in order to support the large ML-KEM-1024 public key and ciphertext sizes, including:

- RFC 7383 IKEv2 Message Fragmentation
- RFC 9242 Intermediate Key Exchanges in IKEv2
- RFC 9370 Multiple Key Exchanges in IKEv2
- draft-ietf-ipsecme-ikev2-pqc-auth Signature Authentication in the IKEv2 using PQC
- RFC 9881 Internet X.509 Public Key Infrastructure - Algorithm Identifiers for the Module-Lattice-Based Digital Signature Algorithm (ML-DSA)
- draft-ietf-ipsecme-ikev2-mlkem Post-quantum Key Exchange with ML-KEM in the IKEv2

These additional RFCs facilitate the use of ML-KEM-1024 without causing IP-level fragmentation, which can create operational challenges and prevent the establishment of a connection. In particular, if ML-KEM-1024 were used in the initial IKEv2 Security Association (SA) key exchange (IKE_SA_INIT), the sizes of its public key and ciphertext would cause the initiator and responder messages to exceed the typical path Maximum Transmission Unit (MTU) and necessitate IP-level fragmentation. In order to prevent this issue, the solution leveraged first performs a CNSA 1.0-compliant key establishment that does not exceed PMTU and subsequently performs an additional key establishment using a newly-defined exchange called Intermediate Exchange (IKE_INTERMEDIATE). IKE_INTERMEDIATE exchanges can circumvent IP-level fragmentation by using IKEv2-level fragmentation, which does not incur the same operational issues. The specifications of which this solution is comprised work as follows:

RFC 7383 IKEv2 Fragmentation: Describes a way to prevent IP fragmentation of large encrypted IKEv2 messages by fragmenting at the IKEv2 layer. This allows IKEv2 messages to traverse network devices that do not allow IP fragments to pass through.

RFC 9242 Intermediate Key Exchanges: Specifies a new exchange type called IKE_INTERMEDIATE. IKE_INTERMEDIATE exchanges can be used for transferring large amounts of data in the process of establishing an IKEv2 Security Association. It is sent after IKE_SA_INIT and before IKE_AUTH.

RFC 9370 Multiple Key Exchanges: Leverages the IKE_INTERMEDIATE exchange specified in RFC 9242 in order to perform multiple key establishments. In particular, this document enables the use of a quantum resistant key establishment algorithm whose public key and ciphertexts would exceed MTU and cause IP fragmentation of the IKE_SA_INIT messages. The document resolves this issue by specifying how to perform such large key establishments in IKE_INTERMEDIATE which can benefit from the IKEv2 fragmentation mechanism specified in RFC 7383. An initial key establishment that does not cause IP fragmentation is first performed in IKE_SA_INIT, followed by additional key establishment(s) using IKE_INTERMEDIATE message(s).

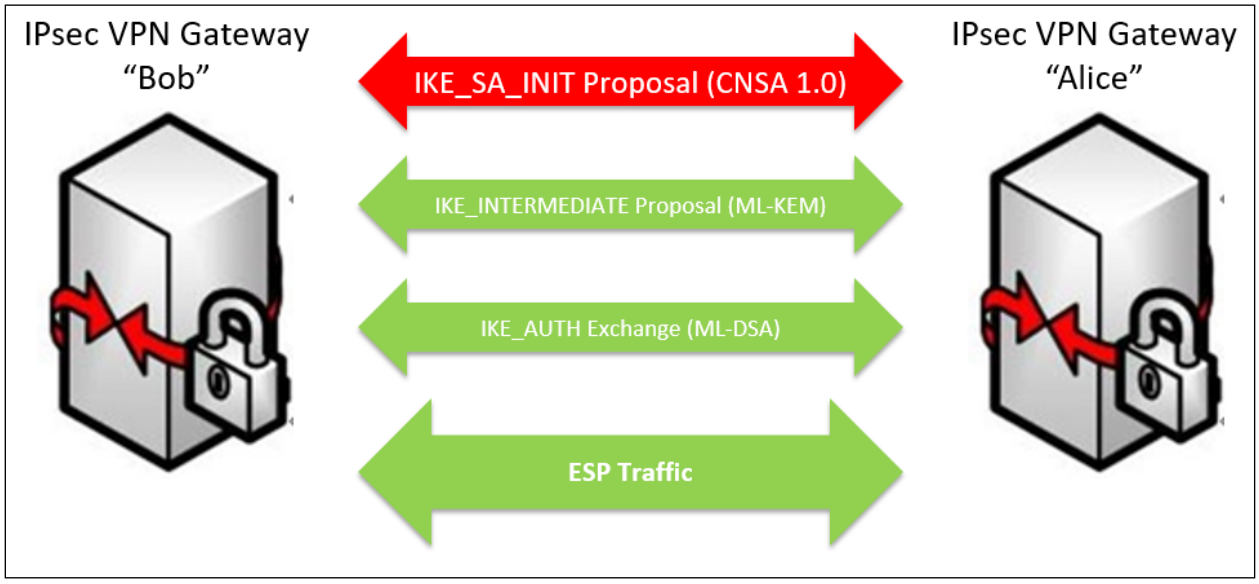

Figure 10. CNSA 2.0 IKEv2 Exchanges

As detailed in Figure 10, RFC 9370 enables peers to perform multiple key exchanges. The key-establishment algorithm used in the Initial IKE SA (IKE_SA_INIT) exchange must be constrained enough in size as to not induce IP fragmentation. The ML-KEM-1024 public key and ciphertext sizes are too large for this initial exchange and thus the IKE_SA_INIT exchange must use a CNSA 1.0-compliant key establishment algorithm. A subsequent Intermediate IKE (IKE_INTERMEDIATE) exchange (as specified in RFC 9242) is then used to perform an ML-KEM key establishment. This second exchange, encrypted using keys established by IKE_SA_INIT, can leverage the IKEv2-level fragmentation mechanism specified in RFC 7383.

5.12 CNSA 2.0 MACsec

As part of the CNSA 2.0 migration, MACsec Devices will have to implement CNSA 2.0-compliant key establishment and digital signatures when utilizing EAP-TLS for mutual authentication. As of now, this is an objective design feature but will be required in the future for the use of MACsec in MSC. The EAP-TLS negotiation to mutually authenticate MACsec Devices will need to use ML-KEM 1024 for key establishment and ML-DSA 87 for digital signatures. For implementations of EAP-TLS to use CNSA 2.0-compliant algorithms, TLS 1.3 will be required per RFC 9190 *EAP-TLS 1.3 Using the Extensible Authentication Protocol with TLS 1.3* and CNSA 2.0 Suite Profile for TLS 1.3 *(draft-becker-cnsa2-tls-profile)*.

5.13 Software and Firmware Signing

As part of the requirement laid out in NSM-10, the CSfC Program has added Software and Firmware Signing requirements for all components listed on the CSfC Components list. As of now this is an objective security feature but the implementation timeline for these requirements will be the same as the CNSA 2.0 timeline in CSfC. These timelines are subject to change depending on market acceptance, vendor and customer feedback for these new requirements.

There are three acceptable algorithms for software and firmware digital signatures, which are all included as part of the CNSA 2.0 cipher suites. These algorithms are enumerated within Table 2 and only one of the algorithms will be required to meet this requirement.

Table 2. CNSA 2.0 Algorithms for Software and Firmware Signing

Algorithm	Function	Specification	Parameters
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels. SHA-256/192 recommended.
Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels.
ML-DSA	Asymmetric algorithm for digital signatures	FIPS 204	Category 5 parameter, ML-DSA-87.

6 CONFIGURATION AND MANAGEMENT

This CP includes design details for the provisioning and management of Solution Components. The MSC Solution Owner must identify authorized Security Administrators to perform configuration and management tasks. The following sections describe the design in detail and Section 10.8 states specific configuration requirements that must be met to comply with this CP.

6.1 COMPONENT PROVISIONING

Provisioning is an out-of-band process performed in a physically secured area (e.g., the Red Network location) where MSC Solution Components are configured and initialized before their first use. During the provisioning process, the Security Administrator configures the Outer Firewall, Outer Encryption Component, Gray Firewall, Gray Management Services, Inner Encryption Component, Red Management Services and Inner Firewall in accordance with the requirements of this CP.

For provisioning IPsec Outer VPN Gateways and Inner VPN Gateways generate a public/private key pair and output the public key in a Certificate Signing Request (CSR). The Security Administrator delivers the Outer VPN Gateway's CSR to the Outer CA and the Inner VPN Gateway's CSR to the Inner CA. The appropriate CA processes the CSR for each encryption component and returns a signed X.509 certificate. The Security Administrator then installs the unique signed certificate and the certificate chain, which consists of the signing CA's certificate and the Trust Anchor certificate (e.g., Root CA certificate). The Security Administrator may also install an initial CRL.

For provisioning MACsec PSK Encryption Components, the Security Administrator obtains a Symmetric Key from an NSA-approved KGS and applies them to each Encryption Component.

For provisioning Certificate-based MACsec, Outer Encryption Components and/or Inner Encryption Components generate a public/private key pair and output the public key in a CSR. The Security

Administrator delivers the Outer Encryption's CSR to the Outer CA and the Inner VPN Gateway's CSR to the Inner CA. The appropriate CA processes the CSR for each encryption component and returns a signed X.509 certificate. The Security Administrator then installs the unique signed certificate and the certificate chain, which consists of the signing CA's certificate and the Trust Anchor certificate (e.g., Root CA certificate). The Security Administrator may also install an initial CRL.

6.2 ADMINISTRATION OF COMPONENTS

Each component in the solution has one or more AWs that maintain, monitor, and control all security functions for that component. It should be noted that all of the required administrative functionality does not need to be present in each individual management component, but the entire set of AWs must collectively meet administrative functionality requirements. Implementations may employ a SIEM in the Gray Management Services for log management of Gray infrastructure components except where AOs use a CDS to move Gray Network log data to a Red SIEM.

AWs may be virtual machines (VMs) on a physical host/server that is dedicated to hosting AWs VMs. A physical host/server that hosts AWs VMs must not host VMs that are used for enrollment or provisioning servers, certificate registrations, or SIEMs. A physical host/server that hosts AWs VMs may not host VMs used for non-CSfC purposes. If an AW is a physical workstation, then that workstation cannot also be used for provisioning, enrollment, certificate registrations, SIEM services, or for any non-CSfC functions. AWs (physical or virtual) must be configured, patched, and operated in accordance to the organizational or local policy. AWs must also be powered off when not in use.

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

The Gray AWs along with all Gray Management Services, are physically connected to the Gray Firewall, if required, or the Outer Encryption Component. The Gray Firewall maintains separate Access Control Lists (ACLs) to permit management traffic to/from the Gray Management Services but prohibits such traffic from all other components. These ACLs ensure that approved management traffic is only capable of flowing in the intended direction. This architecture provides the separation necessary for two independent layers of protection.

Management traffic for all MSC Solution Components is always encrypted to protect confidentially and integrity, except in the case where components are locally managed through a direct physical connection (i.e., serial cable from a Gray AW to the Outer Encryption Component). Management traffic must be encrypted with SSHv2, TLS 1.2 or later, IPsec or MACsec. When components are managed over the Black Network, a CSfC Solution must be implemented to provide two layers of approved encryption. This requirement is not applicable if the MSC Solution Components are managed from the same LAN or VLAN. For example, a Gray AW residing within the Gray Management Services at the same site as the Outer Encryption Component need not use CNSA Suite algorithms since this traffic does not traverse an untrusted network.

7 SUPPORTING DOCUMENTS

7.1 CONTINUOUS MONITORING

Continuous monitoring (CM) allows customers to detect, react to, and report any attacks against their solution. CM also enables the detection of any configuration errors within Solution Components Continuous Monitoring (CM) Requirements have been relocated to a separate *CSfC Continuous Monitoring Annex.*

7.2 KEY MANAGEMENT

Key Management (KM) Requirements have been relocated to a separate *CSfC Key Management Requirements Annex* and the *CSfC Symmetric Key Management Requirements Annex.*

8 REQUIREMENTS OVERVIEW

Sections 9 through Section 13, and the *CSfC Key Management Requirements Annex*, specify requirements for implementations of MSC Solutions compliant with this CP. KM Requirements have been relocated to a separate *CSfC Key Management Requirements Annex*.

8.1 THRESHOLD AND OBJECTIVE REQUIREMENTS

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

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

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

In most cases there is no distinction between the Threshold and Objective versions of a requirement. In these cases, the "Threshold/Objective" column indicates that the Threshold equals the Objective (T=O).

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

8.2 REQUIREMENTS DESIGNATORS

Each requirement defined in this CP has a unique identifier consisting of the prefix "MSC," a digraph that groups related requirements together (e.g., "PS"), and a sequence number (e.g., 11). Table 3 lists the digraphs used to group together related requirements and identifies the sections where those requirement groups can be found.

Table 3. Requirement Digraphs

Digraph	Description	Section	Table
PS	Product Selection Requirements	Section 9	Table 4
SR	Overall Solution Requirements	Section 10.1	Table 5
VG	VPN Gateway Requirements	Section 10.2	Table 8
MD	MACsec Device Requirements	Section 10.3	Table 12
AA	Certificate-based MACsec Authentication and Authorization Requirements	Section 10.3	Table 13
IR	Additional Requirements for Inner Encryption Components	Section 10.4	Table 14
OR	Additional Requirements for Outer Encryption Components	Section 10.5	Table 15
PF	Port Filtering Requirements for Solution Components	Section 10.6	Table 16
CM	Configuration Change Detection Requirements (see *CSfC Continuous Monitoring Annex*)		
DM	Device Management Requirements	Section 10.8	Table 17
MR	Continuous Monitoring Requirements (see *CSfC Continuous Monitoring Annex*)		
AU	Auditing Requirements (see *CSfC Continuous Monitoring Annex*)		
GD	Use and Handling of Solutions Requirements	Section 11.1	Table 18
RP	Incident Reporting Requirements	Section 11.2	Table 19
RB	Role-Based Personnel Requirements	Section 12	Table 20
TR	Testing Requirement	Section 13.1	Table 21
KM	Key Management Requirements (See *CSfC Key Management Requirements Annex*)		

9 REQUIREMENTS FOR SELECTING COMPONENTS

CPs provide architecture and configuration information that allows 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 CSfC Components List, contains the approved products for use in this solution. 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 to maximize the independence between the components within the solution. The requirements in Table 4 will increase the level of effort required to compromise this solution.

Table 4. Product Selection (PS) Requirements

Req. #	Requirement Description	Threshold/ Objective	Alternative
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-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 on the CSfC Components List.	T=O	
MSC-PS-4	Requirement has been relocated to the *CSfC Key Management Requirements Annex.*		
MSC-PS-5	Intrusion Prevention Systems (IPSs) must be chosen from the list of IPSs on the CSfC Components List.	O	Optional
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-7	The Inner Encryption Component and the Outer Encryption Component must not use the same Operating System. 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.	T=O	
MSC-PS-9	Requirement has been relocated to the *CSfC Key Management Requirements Annex.*		
MSC-PS-10	If Gray Firewalls are used, the Gray Firewalls and Inner Encryption Components must either; come	T=O	

Req. #	Requirement Description	Threshold/ Objective	Alternative
	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.		
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-13	Requirement has been relocated to the *CSfC Key Management Requirements Annex.*		
MSC-PS-14	Requirement has been relocated to the *Key Management Requirements Annex.*		
MSC-PS-15	Each component 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	
MSC-PS-17	Products used for the AS must be chosen from the list of ASs on the CSfC Components List.	T=O	

10 CONFIGURATION REQUIREMENTS

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

10.1 OVERALL SOLUTION REQUIREMENTS

Table 5 defines the overall solution requirements for this CP.

Table 5. Overall Solution Requirements (SR)

Req. #	Requirement Description	Threshold/ Objective	Alternative
MSC-SR-1	Network services provided by control plane protocols (such as 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 Encryption Components selected by each site for each tunnel 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 trusted 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 trusted time source located in the Gray Management Network.	T=O	
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, a AW, or a CRL Distribution Point (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	
MSC-SR-10	The Outer Encryption Component must use a unique physical internal interface for each Red Network in the MSC Solution (i.e., VLAN trunking of multiple enclaves is not permitted).	T=O	
MSC-SR-11	A Gray Firewall must be implemented if the MSC Solution is combined with another CSfC solution that requires a Gray Firewall.	T=O	

Req. #	Requirement Description	Threshold/ Objective	Alternative
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, the Inner Firewall requirements from that CP must be followed.	T=O	
MSC-SR-14	The only approved physical paths leaving the Red Network must be through an MSC Solution in accordance with this CP or via an AO-approved solution for protecting data in transit[1].	T=O	
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	Optional
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 on all solution components (i.e., automatic configuration via Trivial File Transfer Protocol on boot).	T=O	
MSC-SR-22	If a CDS is being leveraged within the solution, then it must adhere with DoDI 8540.01, the DISN Connection Process Guide, and the CDS must be on the National Cross Domain Strategy Management Office CDS Baseline.	T=O	
MSC-SR-23	The packet size for packets leaving the external interface of the Gray Firewall/Encryption Component must be configured to keep the packets	T=O	

[1] In some cases, the customer will need to communicate with other sites that have NSA-certified Government-off-the-Shelf 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
	from being fragmented and impacting performance. This requires proper configuration of the Maximum Transmission Unit (MTU) for IPv4 or Path MTU (PMTU) for IPv6 and should consider the Outer VPN Gateway MTU/PMTU values for achievement.		
MSC-SR-24	All solution components (Firewalls, VPN Gateways, Authentication Servers, etc) must use software and firmware signing algorithms in Table 2.	O	Optional

10.2 VPN GATEWAY REQUIREMENTS

This section addresses requirements for VPN Gateways. Table 6 identifies the CNSA 1.0 algorithms approved for IPsec encryption. Table 7 identifies the CNSA 2.0 algorithms approved for IPsec encryption. Table 8 defines requirements for VPN Gateways.

Table 6. Approved CNSA 1.0 Algorithms for IPsec

Security Service	Algorithm Suite	Specifications
Confidentiality (Encryption)	Advanced Encryption Standard (AES)-256	FIPS PUB 197 IETF RFC 7296 IETF RFC 9206
Authentication (Digital Signature)	Rivest Shamir Adelman (RSA) 3072 or Elliptic Curve Digital Signature Algorithm over the curve P-384 with SHA-384	FIPS PUB 186-5 IETF RFC 4754 IETF RFC 7427 IETF RFC 7296 IETF RFC 9206
Key Exchange/ Establishment	Elliptic Curve Diffie-Hellman over the curve P-384 (Diffie-Hellman (DH) Group 20) or DH with prime modulus of 3072 bits (group 15) or 4096 bits (group 16)	NIST SP 800-56A IETF RFC 3526 IETF RFC 5903 IETF RFC 7296 IETF RFC 9206
Integrity (Hashing)	SHA-384 or SHA-512	FIPS PUB 180-4 IETF RFC 6234 IETF RFC 9206

Table 7. Approved CNSA 2.0 Algorithms for IPsec

Security Service	Algorithm Suite	Specifications
Confidentiality (Encryption)	AES-256-GCM	FIPS PUB 197
Authentication (Digital Signature)	ML-DSA-87	FIPS 204

Security Service	Algorithm Suite	Specifications
Key Establishment	ML-KEM-1024	FIPS 203
Integrity (Hashing)	SHA-384 or SHA-512	FIPS PUB 180-4 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460

Table 8. VPN Gateway (VG) Requirements

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-VG-1	The proposals offered by VPN Gateways in the course of establishing the Internet Key Exchange (IKE) Security Association and the Encapsulating Security Payload (ESP) SA for inner and outer tunnels must be configured to offer algorithm suite(s) containing only CNSA 1.0 algorithms as detailed in Table 6.	T	MSC-VG-19, MSC-VG-20, and MSC-VG-21
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	When using certificate-based authentication, 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, 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	
MSC-VG-9	All VPN Gateways must use IKEv2 (IETF RFC 7296) key exchange.	T=O	

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-VG-10	All VPN Gateways must use Cipher Block Chaining for IKE encryption.	T	MSC-VG-18
MSC-VG-11	All VPN Gateways must use Cipher Block Chaining for ESP encryption with a Host-based Message Authentication Code 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 no more than 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	
MSC-VG-17	The Mandatory Access Control policy must only allow the VPN Gateway to access the private key of the VPN Gateway.	O	Optional
MSC-VG-18	All VPN Gateways must use Galois Counter Mode (GCM) for IKE encryption.	O	MSC-VG-10
MSC-VG-19	All IPsec connections must use multiple key exchanges with an initial IKEv2 SA key exchange and an intermediate IKEv2 key exchange: • IKE_SA_INIT: The IKEv2 SA key exchange performed in IKE_SA_INIT must use a CNSA 1.0 key establishment algorithm (as specified in Table 6). • IKE_INTERMEDIATE: The IKEv2 SA key establishment performed in the IKE_INTERMEDIATE exchange must use ML-KEM-1024 (as specified in Table 7).	O	MSC-VG-1
MSC-VG-20	All IPsec connections must use IETF standards compliant with IKE implementations as specified in Commercial National Security Algorithm (CNSA) Suite 2.0 Profile for IPsec (draft-guthrie-cnsa2-ipsec-profile) including RFC 9370, RFC 9242, and RFC 7383.	O	MSC-VG-1
MSC-VG-21	The VPN Components must use algorithms from the algorithm suite in Table 7 for all IPsec VPN	O	MSC-VG-1

Req. #	Requirement Description	Threshold / Objective	Alternative
	tunnels, with the exception of the IKE_SA_INIT exchange.		

10.3 MACSEC DEVICE REQUIREMENTS

This section addresses requirements for MACsec Devices. Table 9 identifies the approved algorithms for MACsec encryption. Table 10 identifies the approved CNSA 1.0 algorithms for MACsec EAP-TLS. Table 11 identifies the approved CNSA 2.0 algorithms for MACsec EAP-TLS. Table 12 defines MACsec Device requirements. Table 13 defines certificate based MACsec authentication and authorization requirements.

Table 9. Approved Algorithms for MACsec Encryption

Security Service	Algorithm Suite	Specifications
Confidentiality (Encryption)	Galois Counter Mode (GCM)-AES-256 GCM-AES-XPN-256	FIPS PUB 197 IEEE 802.1AE-2018
Key Wrap	AES Key Wrap	IETF RFC 3394

Table 10. Approved CNSA 1.0 Algorithms for MACsec EAP-TLS

Security Service	Algorithm Suite	Specifications
Confidentiality (Encryption)	AES-256-GCM	FIPS PUB 197
Authentication (Digital Signature)	RSA 3072 or ECDSA over the curve P-384 with SHA-384	FIPS PUB 186-5 IETF RFC 5216 IETF RFC 6460
Key Exchange/ Establishment	ECDH over the curve P-384 (DH group 20) or DH with prime modulus of 3072 bits (group 15) or 4096 bits (group 16)	NIST SP 800-56A IETF RFC 5216 IETF RFC 6460
Integrity (Hashing)	SHA-384 or SHA-512	FIPS PUB 180-4 IETF RFC 5216 IETF RFC 6234 IETF RFC 6460

Table 11. Approved CNSA 2.0 Algorithms for MACsec EAP-TLS

Security Service	Algorithm Suite	Specifications
Confidentiality (Encryption)	AES-256-GCM	FIPS PUB 197
Authentication (Digital Signature)	ML-DSA-87	FIPS 204

Security Service	Algorithm Suite	Specifications
Key Establishment	ML-KEM-1024	FIPS 203
Integrity (Hashing)	SHA-384 or SHA-512	FIPS PUB 180-4 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460

Table 12. MACsec Device (MD) Requirements

Req. #	Requirement Description	Threshold / Objective	Alternative
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	MSC-MD-14
MSC-MD-4	Requirement has been relocated to the *CSfC Key Management Requirements Annex*.		
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-10	MACsec Devices must require all data traffic on an external facing port to be encrypted (e.g., must-secure).	T=O	
MSC-MD-11	MACsec Device configuration files, whether printed or electronically copied, must be physically	T=O	

Req. #	Requirement Description	Threshold / Objective	Alternative
	protected to the highest classification of the MACsec Device's CAK.		
MSC-MD-12	MACsec Devices must have the Confidentiality Offset set to 0 (zero).	T=O	
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-14	MACsec Devices must authenticate using EAP-TLS (certificate based).	T	MSC-MD-3
MSC-MD-15	Must disable Fallback (rollover) CAKs.	T=O	
MSC-MD-16	MACsec Devices must be configured to "must-secure".	T=O	

Table 13. Certificate-based MACsec Authentication and Authorization (AA) Requirements

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-AA-1	The AS must be used to provide mutual authentication using EAP-TLS with device certificates between MACsec Devices.	T=O	
MSC-AA-2	The AS must only connect to one site's network when a MACsec device is an Outer or Inner Encryption Component.	T=O	
MSC-AA-3	The MACsec Devices and the AS must use the CNSA 1.0 EAP-TLS Ciphersuite in Table 10.	T	MSC-AA-4
MSC-AA-4	The MACsec Devices and the AS must use the CNSA 2.0 EAP-TLS Ciphersuite in Table 11.	O	MSC-AA-3

10.4 Additional Inner Encryption Component Requirements

Table 14 defines additional Inner Encryption Component Requirements.

Table 14. Additional Inner Encryption Component (IR) Requirements

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-IR-1	The Inner VPN Gateway must use ESP Tunnel mode IPsec, with an associated IP tunneling protocol.	T=O	
MSC-IR-2	Packet sizes, or frames leaving the external interface of the Inner Encryption Component must be configured to reduce fragmentation and lessen the impact on performance. This requires proper	O	Optional

Req. #	Requirement Description	Threshold / Objective	Alternative
	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 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 a Mandatory Access Control policy to not allow 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 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
MSC-IR-6	The Inner Encryption Component must use Mandatory Access Control policy to not allow 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	

10.5 Additional Requirements for Outer Encryption Components

Table 15 defines additional Outer Encryption Components Requirements.

Table 15. Additional Outer Encryption Components (OR) Requirements

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-OR-1	Outer VPN Gateways must use ESP Tunnel mode IPsec.	T=O	
MSC-OR-2	Outer Encryption Components must not allow 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 packets received on an interface connected to a Gray Network to	O	MSC-OR-2

Req. #	Requirement Description	Threshold / Objective	Alternative
	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	
MSC-OR-9	Outer Encryption must enable TRANSEC when external interface is MACsec enabled and connected to the Outer Firewall.	O	
MSC-OR-10	Packets leaving the external interface of the Outer Encryption Component must only make connections with the remote Outer Encryption Component or the other intended device.	T=O	

10.6 Port Filtering Solution Components Requirements

Table 16 defines Port Filtering Solution Components Requirements.

Table 16. Port Filtering (PF) Solution Components Requirements

Req. #	Requirement Description	Threshold/ Objective	Alternative
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	T=O	

Req. #	Requirement Description	Threshold/ Objective	Alternative
	applied to both inbound and outbound traffic, such that only MACsec Protocol Data Units and control plane protocols (as defined in this CP) approved by organization-defined policy are allowed.		
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 control plane protocols (as defined in this CP) approved by organization-defined policy are allowed.	T=O	
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 a Gray AW 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	
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, 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	*Withdrawn*		
MSC-PF-15	If the CDP/OCSP is on the gray data plane, the Gray Network interfaces of Outer VPN Gateways must	T=O	

Req. #	Requirement Description	Threshold/ Objective	Alternative
	allow HTTP traffic that is necessary to perform revocation checking for the Inner encryption layer (i.e., requests/replies between the Inner VPN Gateways and the CDPs/OCSP Responders) and block all other HTTP traffic. Refer to IETF RFC 5280 and IETF RFC 6960 for further details on this type of traffic.		
MSC-PF-16	*Withdrawn*		
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	
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-15, or MSC-PF-19.	T=O	
MSC-PF-21	*Withdrawn*		
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	
MSC-PF-23	If a Gray Firewall is required (i.e., networks of multiple protection levels are included in the solution) the Gray Firewall must allow appropriate traffic (IKE, IPsec, MKA and MACsec) between Red Networks operating at the same security level.	T=O	
MSC-PF-24	*Withdrawn*		
MSC-PF-25	If a Gray Firewall is required, the Gray Firewall must allow HTTP traffic that is necessary to perform revocation checking for the Inner encryption layer (i.e., requests/replies between the Inner VPN Gateways and CDPs/OCSP Responders) and block all	T=O	

Req. #	Requirement Description	Threshold/ Objective	Alternative
	other HTTP traffic. Refer to IETF RFC 5280 and IETF RFC 6960 for further details on this type of traffic.		
MSC-PF-26	*Withdrawn*		
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	
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 and DHCP).	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-25, MSC-PF-27 or MSC-PF-30.	T=O	
MSC-PF-32	The Gray Firewall must block all traffic routed to and between two or more Inner VPN Gateways of different classification levels.	T=O	

10.7 Configuration Change Detection Requirements

Configuration Change Detection Requirements have been moved to the *CSfC Continuous Monitoring Annex.*

10.8 Device Management Requirements

Table 17 defines device management requirements.

Table 17. Device Management (DM) Requirements

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-DM-1	If using physical AWs, they 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	AWs (or hosts/servers hosting VMs serving as AWs) must physically reside within a protected facility where CSfC solution(s) are managed.	T=O	

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-DM-3	AWs 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	The Red Management Network must be used exclusively for all management of Inner Encryption Components and Solution Components within the Red Network.	T=O	
MSC-DM-5	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	
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 securely be performed from an AW remotely using an NSA-approved solution (e.g., CP or High Assurance 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.	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	
MSC-DM-13	Security Administrators must use authentication methods in accordance with NIST SP 800-63.	O	Optional

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-DM-14	AWs 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 *CSfC Key Management Requirements Annex*.		
MSC-DM-16	Requirement has been relocated to the *CSfC Key Management Requirements Annex*.		
MSC-DM-17	The same AW must not be used to manage Inner Encryption Components and Outer Encryption Components.	T=O	
MSC-DM-18	Requirement has been relocated to the *CSfC Continuous Monitoring Annex.*		
MSC-DM-19	Requirement has been relocated to the *CSfC Continuous Monitoring Annex.*		
MSC-DM-20	Requirement has been relocated to the *CSfC Continuous Monitoring Annex.*		
MSC-DM-21	Requirement has been relocated to the *CSfC Continuous Monitoring Annex.*		
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	
MSC-DM-23	Hosts/servers for management VMs may not host VMs that perform non-CSfC functions.	T=O	
MSC-DM-24	VMs that perform management services must not also perform other functions within the solution (i.e., provisioning, enrollment, CA registration, SIEM, etc. must be performed by separate workstations or VMs).	T=O	
MSC-DM-25	The Gray Management and Gray Data Networks must be at minimum logically separated by the Gray Firewall using ACL.	T=O	
MSC-DM-26	AWs (physical or virtual) must be configured, patched, and operated in accordance with applicable Operating System vendor hardening guide and the organizational or local policy.	T=O	
MSC-DM-27	AWs (physical or virtual) must be powered off when not in use.	T=O	
MSC-DM-28	The AW must not also be used for provisioning, certificate registrations, and SIEM services.	T=O	
MSC-DM-29	Each AW admin must have a unique login credential. Group accounts are prohibited.	T=O	

10.9 CONTINUOUS MONITORING REQUIREMENTS

Continuous Monitoring Requirements have been moved to the *CSfC Continuous Monitoring Annex.*

10.10 AUDITING REQUIREMENTS

Auditing Requirements have been moved to the *CSfC Continuous Monitoring Annex.*

10.11 KEY MANAGEMENT REQUIREMENTS

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

11 SOLUTION OPERATIONS, MAINTENANCE, AND HANDLING REQUIREMENTS

11.1 USE AND HANDLING OF SOLUTIONS REQUIREMENTS

Table 18 defines the use and handling of the solution requirements.

Table 18. Use and Handling of Solutions (GD) Requirements

Req. #	Requirement Description	Threshold / Objective	Alternative
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	
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, the 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	As part of the annual solution re-registration process, the AO will ensure that a compliance audit must be conducted every year against the latest version of this CP.	T=O	

Req. #	Requirement Description	Threshold / Objective	Alternative
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 the 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 a complete CSfC solution registration package to the NSA.	T=O	
MSC-GD-11	The AO must ensure that when the NSA publishes a new approved MSC CP that their organization must be in compliance upon the next registration renewal.	T=O	
MSC-GD-12	Solution implementation information that was provided to the NSA during solution registration must be updated annually (in accordance with Section 13.3) 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	
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 frequently off-loaded to a backup storage medium.	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	
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	T=O	

Req. #	Requirement Description	Threshold / Objective	Alternative
	includes a mechanism or method for ensuring the audit log can be maintained during power events.		
MSC-GD-21	All infrastructure components must implement a password of at least 112 random bits. Passwords should be generated using an approved password generator. See *CSfC Key Management Requirements Annex, Appendix A* for more information.	T	MSC-GD-27
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 installs 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	
MSC-GD-26	A baseline configuration for all components must be maintained by the Security Administrator and be available to the Auditor.	T=O	
MSC-GD-27	All infrastructure components must use an authentication service on their respective network/domain in order to access the Infrastructure component of the respective network/domain.	O	MSC-GD-21

11.2 INCIDENT REPORTING REQUIREMENTS

Table 19 lists incident reporting requirements for reporting security incidents to the NSA. These requirements must 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 incident reporting procedures already in use within the Solution Owner's organization. It is critical that Security Administrators and Auditors are familiar with maintaining the solution in accordance with this CP. Familiarity with the known-good configuration of the solution will better equip personnel responsible for the operations and maintenance of the solution 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 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 19 only provides requirements directly related to the incident reporting process. See the *CSfC Continuous Monitoring Annex* for requirements supporting the detection of events that may reveal that a reportable incident has occurred.

Table 19. Incident Reporting (RP) Requirements

Req. #	Requirement Description	Threshold/ Objective	Alternative
MSC-RP-1	Solution Owners must report confirmed incidents meeting the criteria in MSC-RP-3 through MSC-RP-15 within 24-hours of detection via the Joint Incident Management System or contacting the NSA as specified in the CSfC Acknowledgement 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 the NSA requested? (Yes/No)	T=O	
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	
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	

Req. #	Requirement Description	Threshold/ Objective	Alternative
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	

12 ROLE-BASED PERSONNEL REQUIREMENTS

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

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

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

2) Document and report security-related incidents to the appropriate authorities.

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

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

5) Ensure that the implemented MSC Solution remains compliant with the latest version of this CP, as specified by MSC-GD-11.

Auditor – The Auditor must review the actions performed by the Security Administrator and events recorded in the audit logs to ensure that no action or event represents a compromise to the security of the MSC Solution. The Auditor will only be authorized access to Outer and Inner administration components. Auditor duties include, but are not limited to:

1) Review, manage, control, and maintain security audit log data.

2) Document and report security-related incidents to the appropriate authorities.

3) Develop, maintain and report a System Audit Capability Survey.

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

1) Acquire the products that compose the solution.

2) Configure the MSC Solution in accordance with this CP.

3) Document, test, and maintain the solution.

4) Respond to incidents affecting the solution.

Table 20 identifies additional personnel requirements that must be performed in an MSC Solution.

Table 20. Role-Based (RB) Personnel Requirements

Req. #	Requirement Description	Threshold/ Objective	Alternative
MSC-RB-1	The Security Administrators, Auditors, and Integrators must be cleared to the highest level of data protected by the MSC Solution. Black Network Administrators may be cleared at the Black Network security level.	T=O	
MSC-RB-2	The Security Administrator and Auditor roles must be performed by different people.	T=O	
MSC-RB-3	All Security Administrators and Auditors must meet local IA training requirements.	T=O	
MSC-RB-4	Requirement has been relocated to the *CSfC Key Management Requirements Annex.*		
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	
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	Requirement has been relocated to the *CSfC Continuous Monitoring Annex.*		
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	Requirement has been relocated to the *CSfC Key Management Requirements Annex.*		
MSC-RB-10	Requirement has been relocated to the *CSfC Symmetric Key Management Requirements Annex.*		
MSC-RB-11	Mandatory Access Control policy must specify roles for Security Administrator and Auditor using role-based access controls.	O	Optional

13 INFORMATION TO SUPPORT AO

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

- The customer, possibly with support from an Integrator, instantiates a solution implementation that follows the NSA-approved CP.
- The customer's testing team develops a test plan and performs testing of the MSC Solution (see Section 13.1).
- The customer has the security control assessment and system authorization performed using the risk assessment information referenced in Section 13.2.
- The customer provides the results from the security control assessment and system authorization to the AO for use in making an approval decision. The AO is ultimately responsible to ensure all requirements from this CP have been properly implemented in accordance with this CP.
- The customer registers the solution with the NSA and re-registers yearly to validate its continued use as detailed in Section 13.3.
- Customers who want to use a variant of the solution detailed in this CP will contact their NSA External Engagement Representative to determine ways to obtain NSA approval.
- The AO ensures that a compliance audit must be conducted every year against the latest version of the MSC CP, and the results must be provided to the AO.
- In case of a compromise, the AO ensures that certificate and CAK revocation information is updated on all the Solution Components in the MSC Solution.
- The AO ensures that any Layer 2 or Layer 3 control plane protocols that are used in the solution are necessary for the operation of the network and that local policy supports their use.
- The AO reports incidents affecting the solution in accordance with Section 11.2.

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

13.1 SOLUTION TESTING

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

The security features and operational capabilities associated with the use of the solution must be tested. The following is a general high-level methodology for developing the T&E plan and procedures and for

the execution of those procedures to validate the implementation and functionality of the MSC Solution. The entire solution, to include each component described in Section 5, is addressed by this test plan, including the following:

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

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

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

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

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

The test requirement in Table 21 was developed to ensure that the MSC Solution functions properly and meets the configuration requirements in Section 10. Testing of these requirements should be used as a minimum framework for the development of the detailed T&E plan and procedures.

Table 21. Test (TR) Requirement

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-TR-1	The organization implementing the CP must perform all tests listed in the *CSfC MSC CP Testing Annex* and maintain artifacts of the testing results.	T=O	

13.2 Risk Assessment

The Risk Assessment of the MSC Solution presented in this CP focuses on the types of attacks that are feasible against this solution and the mitigations that can be employed. Customers should contact their NSA External Engagement Representative to request this document, or visit the CSfC Secret Internet Protocol Router Network (SIPRNet) site for information. The process to obtain the Risk Assessment can be obtained via the CSfC PMO. The AO must be provided a copy of the NSA Risk Assessment for their consideration in approving the use of the solution.

13.3 Registration of Solutions

All customers using CSfC solutions to protect information on National Security Systems must register their solution with the NSA prior to operational use. This registration allows the NSA to track where MSC Solutions are instantiated and to provide the AOs at those sites with appropriate information, including any significant vulnerabilities that may be discovered in components or high-level designs approved for these solutions. The CSfC solution registration process is available on the CSfC web page

under the “Solution Registration” tab (https://www.nsa.gov/resources/commercial-solutions-for-classified-program/solution-registration).

Solution registrations are valid for one year from the date the solution registration is approved, at which time customers are required to re-register their solution to continue using it. Approved CPs will be reviewed twice a year, or as events warrant. Registered users of this CP will be notified when a new version is published. When a new version of this NSA-approved CP is published, customers have six months from the date they are notified, to bring their solutions into compliance with the new version of this CP and re-register their solution (see requirement MSC-GD-11). Customers are also required to update their registrations whenever the information provided on the registration form changes.

APPENDIX A. GLOSSARY OF TERMS

Assurance –The grounds for confidence that the set of intended security controls in an information system are effective in their application. (CNSSI 4009)

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

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

Authorizing Official – A senior (Federal) official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use of a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation. (NIST SP 800-37)

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

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

Black Network – A network that contains classified data that has been encrypted twice.

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

Central Management Site – A site within a MSC Solution that is responsible for remotely managing the Solution Components located at other sites.

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

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

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

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

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

Encapsulation – Packaging a packet/frame into a new packet/frame by adding a header and sometimes a trailer.

Encryption Component – Either a VPN Gateway or a MACsec Device.

External Interface – The interface on an Encryption Component that connects to the outer network (i.e., the Gray Network on the Inner Encryption Component or the Black Network on the Outer Encryption Component).

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

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

Gray Network – A network that contains classified data that has been encrypted once.

Gray Firewall – A traffic filtering firewall placed on the Gray Network to provide additional separation between flows of singly-encrypted data of different security levels.

Independently Managed Site – A site within a MSC Solution where Solution Components are locally managed and that does not remotely manage other sites' Solution Components.

Integrity – Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. (NIST SP 800-37)

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

Key Server – The MACsec Device designated as the one responsible for distribution Secure Association Keys to the other MACsec Device.

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

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

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

Pseudowire – Emulation of a point-to-point connection.

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

Red Network – A network that contains unencrypted classified data.

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

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

Remote Site – A site within a MSC Solution where Solution Components are remotely managed by a Central Management Site.

Security Control Assessment – The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization. (NIST SP 800-37)

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

Split-tunneling – Allows network traffic to egress through a path other than the established encryption tunnel (either on the same interface or another network interface. Split-tunneling is explicitly prohibited in MSC CP compliant configurations.

Transmission Security (TRANSEC) – Measures (security controls) applied to transmissions in order to prevent interception, disruption of reception, communications deception, and/ or derivation of intelligence by analysis of transmission characteristics such as signal parameters or message externals. (CNSSI 4009)

APPENDIX B. ACRONYMS

Acronym	Meaning
ACL	Access Control List
AES	Advanced Encryption Standard
AO	Authorizing Official
ARP	Address Resolution Protocol
AS	Authentication Server
AW	Administrative Workstation
BGP	Border Gateway Protocol
CA	Certification Authority
CAK	Connectivity Association Key
CEK	CAK Encryption Key
CDP	CRL Distribution Point
CDS	Cross Domain Solution
CKN	Connectivity Association Key Name
CNSA	Commercial National Security Algorithm [Suite]
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COTS	Commercial Off-the-Shelf
CP	Capability Package
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSD	Cybersecurity Directorate
CSfC	Commercial Solutions for Classified
CSR	Certificate Signing Request
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DM	Device Management
DNS	Domain Name System
ECDSA	Elliptic Curve Digital Signature Algorithm
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standards
GCM	Galois Counter Mode
GRE	Generic Routing Encapsulation
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IA	Information Assurance
IAD	Information Assurance Directorate
ICMP	Internet Control Message Protocol
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6

Acronym	Meaning
KGS	Key Generation Solution
KM	Key Management
LAN	Local Area Network
MACsec	Media Access Control Security
MKA	MACsec Key Agreement
MSC	Multi-Site Connectivity
MSK	Master Session Key
MTU	Maximum Transmission Unit
MW	Management Workstation
NDP	Neighbor Discovery Protocol
NIAP	National Information Assurance Partnership
NIPRNet	Non-secure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSS	National Security Systems
NTP	Network Time Protocol
(O)	Objective
OCSP	Online Certificate Status Protocol
OSPF	Open Shortest Path First
PKI	Public Key Infrastructure
PMTU	Path Maximum Transmission Unit
PSK	Pre-Shared Key
RA	Registration Authority
RFC	Request for Comments
RSA	Rivest Shamir Adelman
SCRM	Supply Chain Risk Management
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SIPRNet	Secret Internet Protocol Router Network
SP	Special Publication
SSH	Secure Shell
SSHv2	Secure Shell Version 2
(T)	Threshold
T&E	Test and Evaluation
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
XPN	extended Packet Number

APPENDIX C. REFERENCES

CNSSD 505	*CNSS Directive (CNSSD) Number 505, Supply Chain Risk Management (SCRM)*	November 2021
CNSSI 1253	*CNSS Instruction (CNSSI) 1253, Security Categorization and Control Selection for National Security Systems*	March 2014
CNSSI 4009	*CNSS Instruction (CNSSI) 4009, Committee on National Security Systems (CNSS) Glossary*	April 2015
CNSSP 7	*CNSS Policy (CNSSP) Number 7, National Policy on the Use of Commercial Solutions to Protect National Security Systems*	December 2015
CNSSP 11	*CNSS Policy (CNSSP) Number 11, National Policy Governing the Acquisition of Information Technology Products*	February 2025
CNSSP 15	*CNSS Policy (CNSSP) Number 15, Use of Public Standards for the Secure Information Sharing*	October 2016
CNSSP 15	*CNSS Policy (CNSSP) Number 15, National Policy on the Use of Public Standards for Secure Information Sharing (CNSA 2.0)*	February 2025
FIPS 140-3	*Federal Information Processing Standard 140, Security Requirements For Cryptographic Modules.* National Institute for Standards and Technology (NIST).	March 2019
FIPS 180-4	*Federal Information Processing Standard 180-4, Secure Hash Standard (SHS).* NIST.	August 2015
FIPS 186-5	*Federal Information Processing Standard 186-5, Digital Signature Standard (DSS).* NIST.	February 2023
FIPS 197	*Federal Information Processing Standard 197, Advanced Encryption Standard (AES).* NIST.	May 2023
IEEE 802.1AE-2018	*IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security*	December 2018
IEEE 802.1X-2020	*IEEE Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control*	January 2020
RFC 3647	*IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.* S. Chokhani, et. al.	November 2003
RFC 4252	*IETF RFC 4252 The Secure Shell (SSH) Authentication Protocol*. T. Ylonen and C. Lonvick.	January 2006
RFC 4253	*IETF RFC 4253 The Secure Shell (SSH) Transport Layer Protocol*. T. Ylonen and C. Lonvick.	January 2006
RFC 4254	*IETF RFC 4254 The Secure Shell (SSH) Connection Protocol*. T. Ylonen and C. Lonvick.	January 2006
RFC 4256	*IETF RFC 4256 Generic Message Exchange Authentication for the Secure Shell Protocol (SSH)*. F. Cusack and M. Forssen.	January 2006
RFC 4302	*IETF RFC 4302 IP Authentication Header*. S. Kent.	December 2005
RFC 4303	*IETF RFC 4303 IP Encapsulating Security Payload*. S. Kent.	December 2005

RFC 4308	*IETF RFC 4308 Cryptographic Suites for IPsec*. P. Hoffman.	December 2005
RFC 4754	*IETF RFC 4754 IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)*. D. Fu and J. Solinas.	January 2007
RFC 5246	*IETF RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2*. T. Dierks and E. Rescorla.	August 2008
RFC 5280	*IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. D. Cooper, et. al.	May 2008
RFC 5746	*IETF RFC 5746 Transport Layer Security (TLS) Renegotiation Indication Extension.* E. Rescorla, et. al.	February 2010
RFC 5878	*IETF RFC 5878 Transport Layer Security (TLS) Authorization Extensions.* M. Brown and R. Housley.	May 2010
RFC 5903	*IETF RFC 5903 Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2.* D. Fu and J. Solinas.	June 2010
RFC 6176	*IETF RFC 6176 Prohibiting Secure Sockets Layer (SSL) Version 2.0.* S. Turner and T. Polk.	March 2011
RFC 6234	*IETF RFC 6234 US Secure Hash Algorithms* T. Hansen and D. Eastlake 3rd.	May 2011
RFC 6668	*IETF RFC 6668 SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol.* D. Bider and M. Baushke.	July 2012
RFC 6960	*IETF RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.* S. Santerson, et. al.	June 2013
RFC 7030	*IETF RFC 7030 Enrollment over Secure Transport*. M. Pritikin, P. Yee, and D. Harkins.	October 2013
RFC 7296	*IETF RFC 7296 Internet Key Exchange Protocol Version 2 (IKEv2).* C. Kaufman, et. al.	October 2014
RFC 7383	*IKEv2 Message Fragmentation.* V. Smyslov.	November 2014
RFC 7427	*IETF RFC 7427 Signature Authentication in the Internet Key Exchange version 2 (IKEv2).* T. Kivinen and J. Snyder.	January 2015
RFC 7465	*IETF RFC 7465 Prohibiting RC4 Cipher Suites.* A. Popov.	February 2015
RFC 7507	*IETF RFC 7507 TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks.* B. Moeller and A. Langley.	April 2015
RFC 7568	*IETF RFC 7568 Deprecating Secure Sockets Layer Version 3.0.* R. Barnes, et. al.	June 2015
RFC 7627	*IETF RFC 7627 Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension.* K. Bhargavan, et. al.	September 2015
RFC 7670	*IETF RFC 7670 Generic Raw Public-Key Support for IKEv2.* T. Kivinen, P. Wouters, and H. Tschofenig.	January 2016
RFC 7685	*IETF RFC 7685 A Transport Layer Security (TLS) ClientHello Padding Extension.* A. Langley.	October 2015

RFC 7919	*IETF RFC 7919 Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS).* D. Gillmor.	August 2016
RFC 8446	*IETF RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3*. E. Rescorla.	August 2018
RFC 8784	*IETF RFC 8784 Mixing Preshared Keys in IKEv2 for Post-Quantum Security.* S. Fluhrer, et. al.	June 2020
RFC 9151	*IETF RFC 9151 Commercial National Security Algorithm (CNSA) Profile for TLS and DTLS 1.2 and 1.3.* D. Cooley.	April 2022
RFC 9206	*IETF RFC 9206 Commercial National Security Algorithm (CNSA) Suite Cryptography for Internet Protocol Security (IPsec).* L. Corcoran and M. Jenkins.	February 2022
RFC 9212	*IETF RFC 9212 Commercial National Security Algorithm (CNSA) Suite Cryptography for Secure Shell.* N. Gajcowski and M. Jenkins.	March 2022
RFC 9242	*Intermediate Key Exchanges in IKEv2.* V. Smyslov.	May 2022
RFC 9370	*Multiple Key Exchanges in Internet Key Exchange Protocol version 2 (IKEv2).* C. Jung Tjhai, et. al.	May 2023
SP 800-56A	*NIST Special Publication 800-56A Rev. 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*. E. Barker, et. al.	April 2018
SP 800-56B	*NIST Special Publication 800-56B Rev. 2, Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography*. E. Barker, et. al.	March 2019
SP 800-56C	*NIST Special Publication 800-56C Rev 2, Recommendation for Key Derivation Methods in Key-Establishment Schemes* E. Baker et. Al.	August 2020
SP 800-57	*NIST Special Publication 800-57 Part 1 Rev 5, Recommendation for Key Management Part 1: General.* E. Barker.	May 2020
SP 800-131A	*NIST Special Publication 800-131A Rev. 2, Transitioning the use of Cryptographic Algorithms and Key Lengths*. E. Barker and A. Roginsky.	March 2019
DoDI 8540.01	*Department of Defense Instruction (DoDI) 8540.01: Cross Domain Policy*	August 2017
CSfC KM Requirements Annex	*Commercial Solutions for Classified (CSfC): Key Management Requirements Annex, v3.0.0*	March 2026
CSfC Symmetric KM Requirements Annex	*CSfC Symmetric Key Management Requirements Annex, v3.0.0*	March 2026
CSfC Continuous Monitoring Annex	*CSfC Continuous Monitoring Annex, v1.1.0*	March 2021