


NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

COMMERCIAL SOLUTIONS for CLASSIFIED (CSfC)

Multi-Site Connectivity Capability Package V1.1

Version 1.1
26 June 2018


CHANGE HISTORY

Title	Version	Date	Change Summary
Commercial Solutions for Classified (CSfC) Multi-Site Connectivity (MSC) Capability Package (CP)	0.8	4 May 2016	• Initial release of CSfC Multi-Site Connectivity guidance.
CSfC MSC Capability Package	1.0	23 February 2017	• Official release of CSfC MSC guidance.
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.

Table of Contents

Table of Figures

List of Tables

1 INTRODUCTION

The Commercial Solutions for Classified (CSfC) program within the National Security Agency (NSA) Directorate of Capabilities uses a series of Capability Packages (CPs) to provide configurations that will 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 is delivering 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. In MSC CP Version 1.1, the Key Management Requirements have been relocated from the CP to a separate Key Management Annex.

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

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

2 PURPOSE AND USE

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

Customers who want to use this CP must register their solution with NSA. Additional information about the CSfC process is available on the CSfC web page.

Please provide comments on usability, applicability, and/or shortcomings to your NSA External Engagement Representative and the MSC CP Maintenance Team at msc_cp@nsa.gov.

MSC Solutions must also comply with Committee on National Security Systems (CNSS) policies and instructions. Any conflicts identified between this CP and CNSS or local policy should be provided to the MSC CP Maintenance Team.

3 LEGAL DISCLAIMER

This CP is provided "as is." Any express or implied warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event must the United States (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.

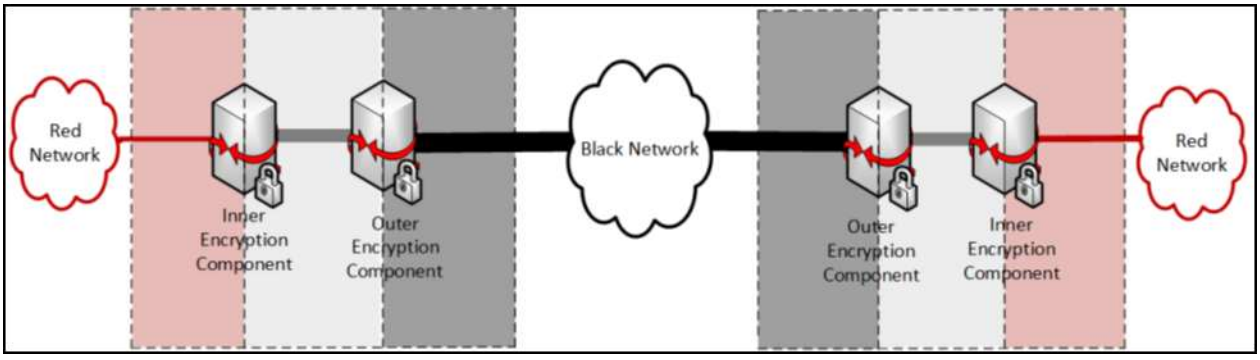

Figure 1. Two Encryption Tunnels Protect Data Across an Untrusted Network

The MSC CP instantiations are built using products from the CSfC Components List (see Section 10). 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 (MoA) with 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 are under the control of the Solution Owner or a trusted third party. Red networks may only communicate with one another through the MSC Solution if the networks operate at the same security level.

4.1.2 GRAY NETWORK

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

The Gray network is physically treated as a classified network even though all classified data is singly encrypted. If a Solution Owner's classification authority determines that 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, as it is 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, an Administration Workstation. The Gray Management Services may also include a Security Information and Event Manager (SIEM) unless the SIEM is implemented in the Red network in conjunction with a cross domain solution (CDS) (see Section 7). This CP requires the management of Gray network components through the Gray Administration Workstation. As a result, neither Red nor Black Administration Workstations are permitted to manage the Outer Encryption Component, Gray Firewall, or Gray Management Services. Additionally, the Gray Administration Workstation is prohibited from managing Inner Encryption Components. Inner Encryption Components must be managed from a Red Administration Workstation.

4.1.3 BLACK NETWORK

A Black network contains classified data that has been encrypted twice. The network connecting the Outer 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. If the Black network is the Public Internet, an Outer Firewall is required between the Black network and the Outer Encryption Component, as shown in Figure 2.

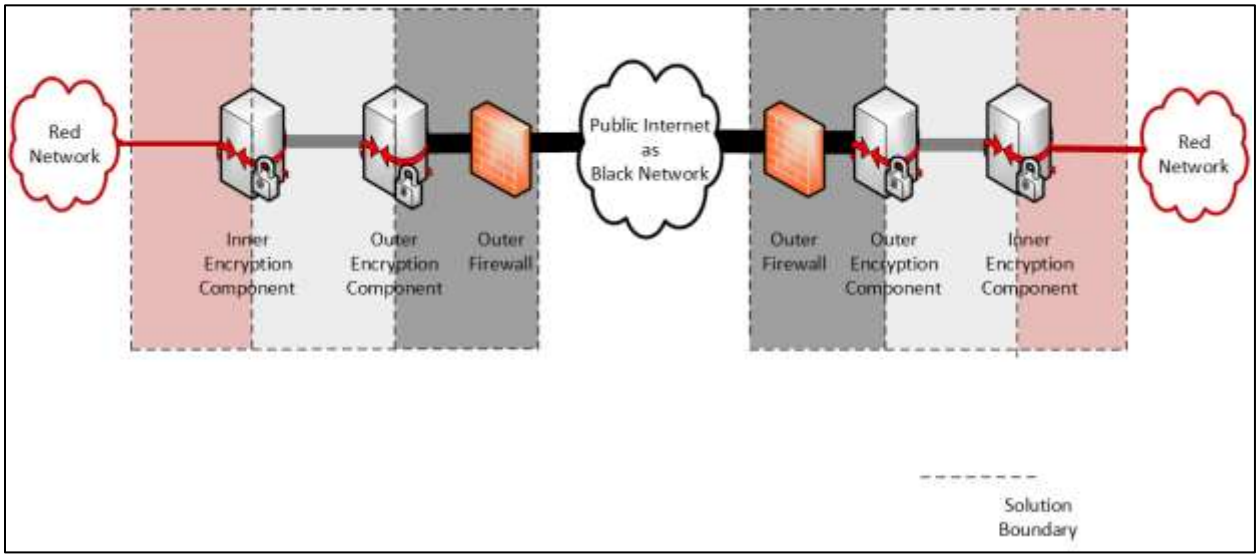

Figure 2. MSC Solution Using the Public Internet as the Black Transport Network

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)
- Name resolution (e.g., Domain Name System (DNS))
- 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 11.1) require that time synchronization be performed, but do 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 functionality.

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 are required to be separated from one another by using physical or cryptographic separation. Use of a Virtual Local Area Network (VLAN) alone is not sufficient

to separate data plane and management plane traffic. As a result, a solution may, for example, have a Gray data network and a Gray management network that are separate from one another, where the components on the Gray management network are used to manage the components on the Gray data network. Given that some control plane traffic is necessary for a network to function, there is no general requirement that control plane traffic be similarly separated, unless otherwise specified.

4.2 HIGH LEVEL DESIGN

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

4.2.1 MULTIPLE SITES

Figure 3 depicts two Red networks at different sites that operate at the same security level, 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.

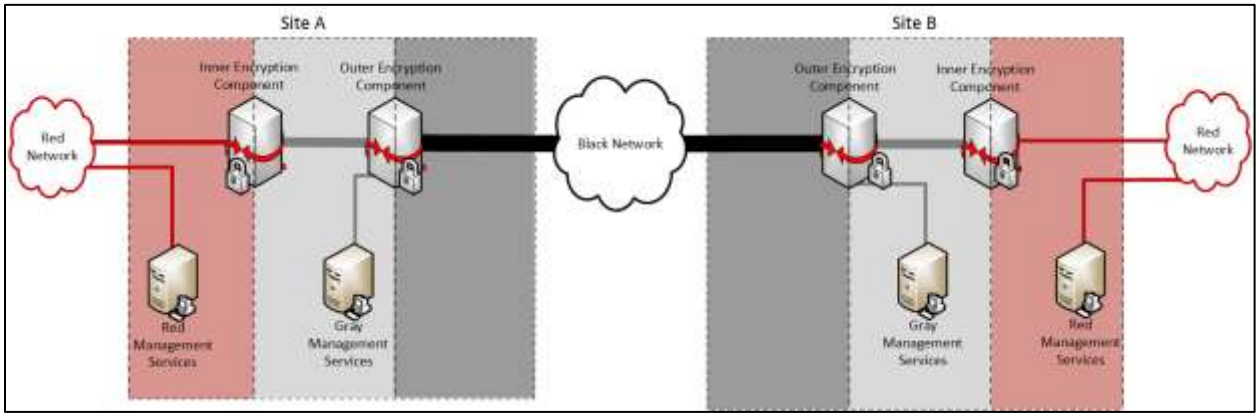

Figure 3. MSC Solution Connecting Two Independently Managed Sites

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

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

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 of using 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.

Since there is no remote management, no management traffic will cross the Black network, encrypted or otherwise. Any VPN Gateways 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 in the MSC Solution. 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.

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 depicts only two sites, this solution can scale to include numerous sites, with each additional site having the same design as those in the figure.

4.2.1.2 Centrally Managed Sites

If remote management is used, personnel at a single geographic site administer and perform keying for all the sites included in the solution, as shown in Figure 4. In this case, because the administration is done by one group of Security Administrators, CA Administrators, and Key Generation Solution Administrators (see Section 13), they can ensure the interoperability of each site as new sites are added. A maximum of two CAs are needed: one on the Red network for all the Inner VPN Gateways and one on the Gray management network for all the Outer VPN Gateways. If available, enterprise CAs should be used. If MACsec Devices are being used on either or both layers, CAs are not required since these devices are using CAKs.

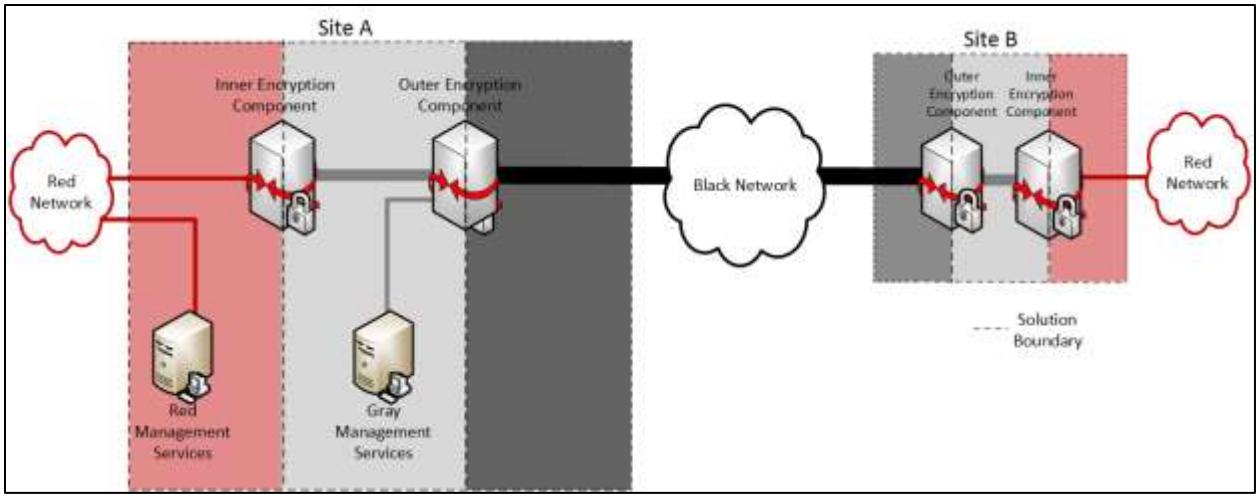

Figure 4. MSC Solution Connecting a Central Management Site and a Remote Site

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. Gray management traffic is encrypted using SSHv2, TLS 1.2 or later, IPsec, or MACsec before being routed through the Outer Encryption Component to the remote site. The SSHv2, TLS 1.2 or later, IPsec

or MACsec serves as the inner layer of encryption for Gray management traffic, and the encryption tunnel provided by the Outer Encryption Component serves as the outer layer of encryption. Red management traffic is similarly 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.

Note that while Figure 4 depicts 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 in the figure.

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 will still require 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 a 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 depicts a Central Management Site and a Remote Site, 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 illustrates a 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.

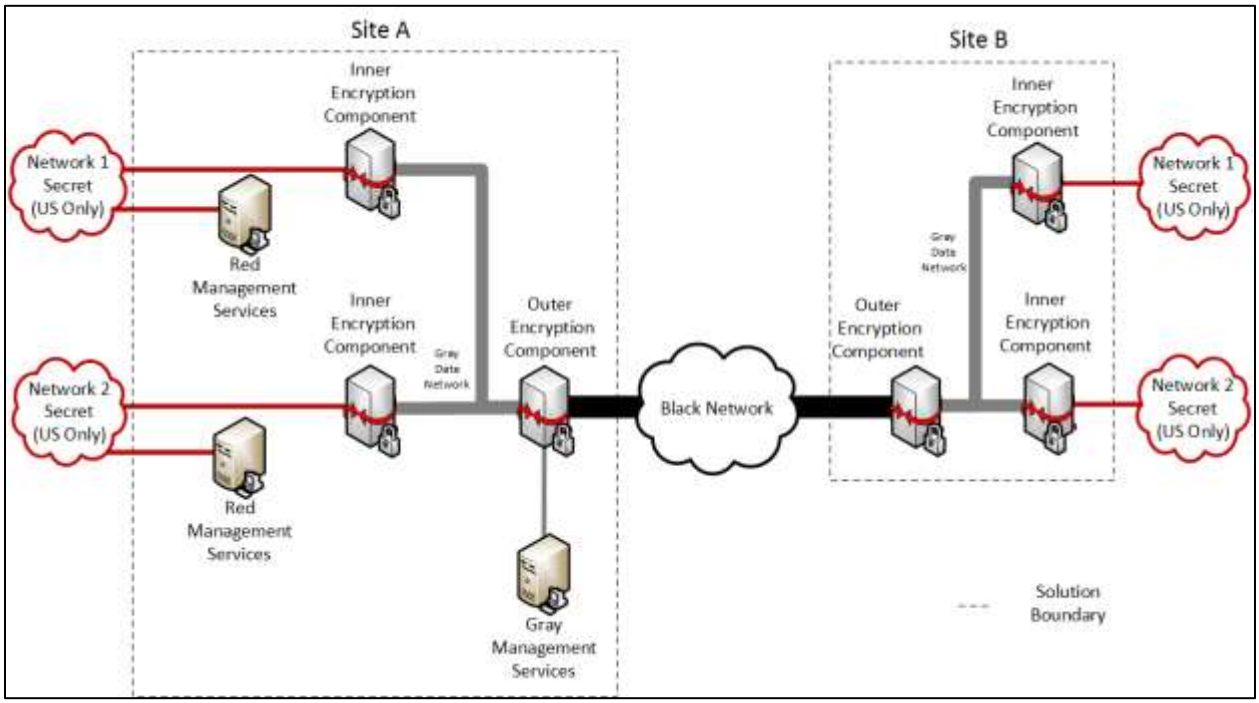

Figure 5. MSC Solution for Two Networks at the Same Security Level

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 further guard against 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 flowing through it based primarily on the Gray network source and destination addresses, only allowing a packet through if the source and destination components are intended to communicate with one another and dropping the packet if they are not.

When multiple security levels are being 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, Administration Workstations 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, Administration Workstations 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 the filtering in addition to the Outer Encryption Components, as shown in Figure 6. 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 any packets between Inner Encryption Components of different security levels.

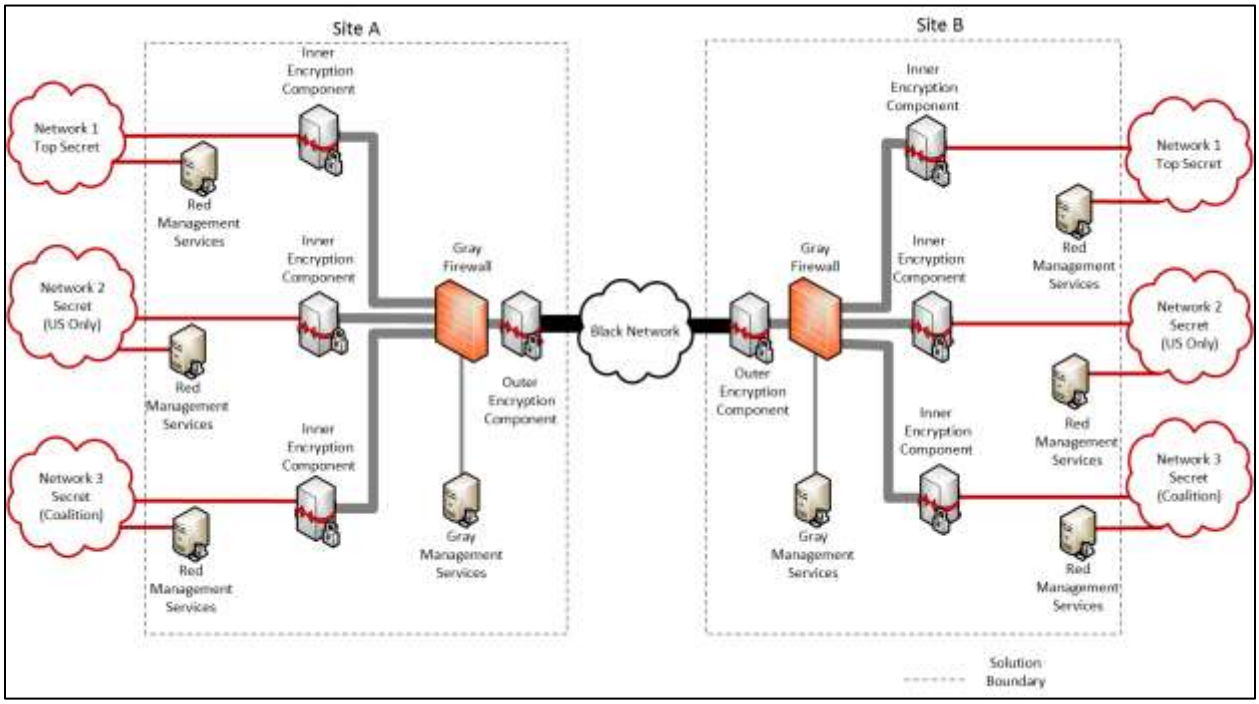

Figure 6. MSC Solution for Networks at Different Security Levels

Figure 6 also illustrates that there is flexibility in the specific placement of Gray Firewalls, as long as their placement satisfies the requirement that any path between Inner Encryption Components for networks of different security levels is met.

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.

Table 1. Layering Options

Configuration	Inner Tunnel	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. The reason for encapsulation is to ensure the MACsec-encrypted traffic is not decrypted prior to reaching its destination and to ensure 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 for it.

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 (L2TPv3) and Ethernet over Multiprotocol Label Switching (EoMPLS).

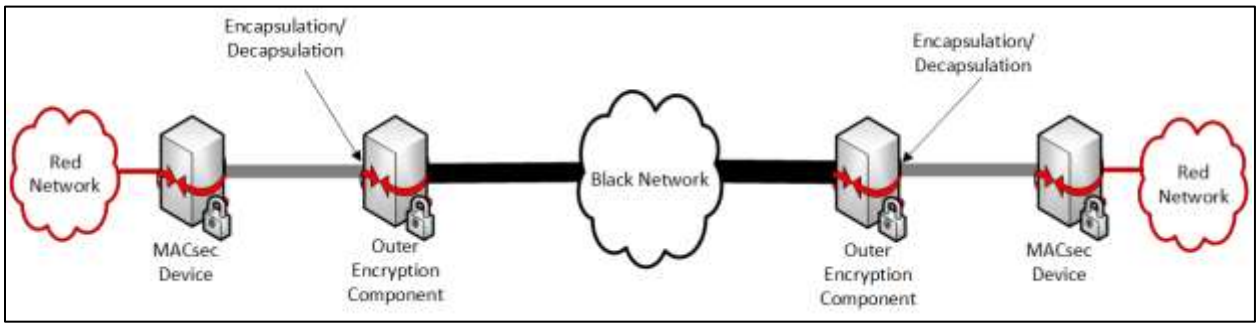

Figure 7. Encapsulating MACsec on an Internal Interface

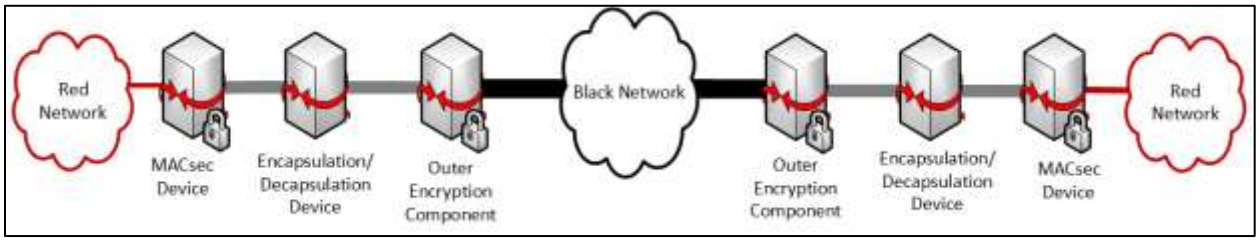

Figure 8. Encapsulating MACsec with a Separate Device

There are some scenarios when a MACsec Device provides the outer tunnel of encryption and the MACsec-encrypted traffic needs to be encapsulated prior to handing it off to the Black network. In these scenarios, this additional step falls outside the boundary of the MSC Solution. However, applying the general device management and port filtering requirements for Solution Components is highly recommended.

In the current MACsec standard, the entire frame is encrypted with the exception of the source and destination addresses. Draft amendment Institute of Electrical and Electronics Engineers (IEEE) 802.1Aecg-2016 provides the option of moving the Virtual LAN (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 (QoS) across a Service Provider's network. This CP allows VLAN ID tags to be used in the clear, if supported in the MACsec Device.

At high speeds, some MACsec Devices may be configured to use an eXtended Packet Number (XPN), as described in IEEE 802.1Aebw-2013. Without XPN, the unique packet numbers may be exhausted quickly at high speeds and re-keying at high speeds may interrupt traffic flow. This CP allows the XPN feature to be used, if supported in the MACsec Device.

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. This CP requires all authentication certificates issued to VPN Gateways to be Non-Person Entity (NPE) certificates. This CP also requires an Inner CA when the Inner Encryption Component is a VPN Gateway and an Outer CA when the Outer Encryption Component is a VPN Gateway.

MACsec Devices authenticate using a Pre-Shared Key (PSK) called a CAK. This CP requires all CAKs and their associated Connectivity Key Names (CKNs) to be generated using an NSA-approved Key Generation Solution (KGS). For each MACsec tunnel, a Key Server is identified. The Key Server authenticates the other MACsec Device and issues a Secure Association Key (SAK) to provide confidentiality and integrity for the MACsec tunnel.

4.3 OTHER PROTOCOLS

Throughout this document, when IP traffic is discussed, it can 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 document, 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 (IGMP) or Multicast Listener Discovery (MLD) 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 being used in the Black and/or Red network. For example, networks that currently use Generic Routing Encapsulation (GRE), Multiprotocol Label Switching (MPLS) 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 this 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.

For example, Figure 9 illustrates a 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 to. 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.

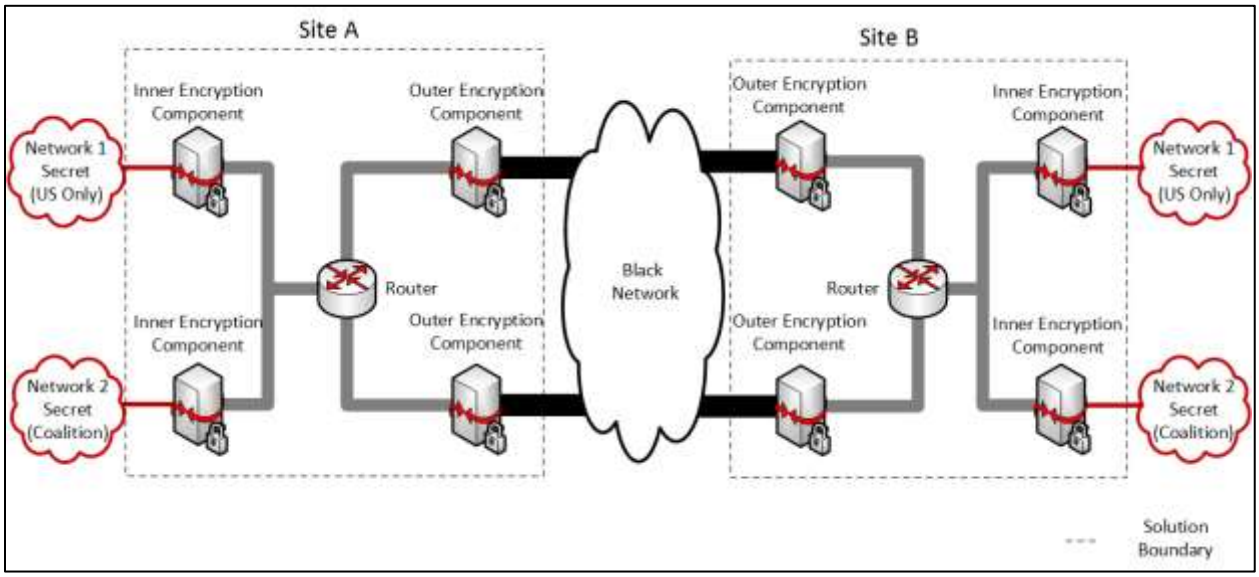

Figure 9. MSC Solution with Redundant Outer Encryption Components

The above is only a simple example of how redundancy could be added, if needed, for a 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 the previous section, 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 Administration Workstations, CAs for key management using Public Key Infrastructure (PKI), a KGS for generating 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 10).

Additional components, discussed in the 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 the components.

5.1 OUTER FIREWALL

An MSC Solution that uses the Public Internet as its Black transport 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 transport 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 11.6.

The Outer Firewall, selected from the CSfC Components List, must be physically separate from the Outer Encryption Component, as depicted in Figure 2.

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 transport 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 transport network. The internal interface of the Outer Encryption Component is connected to Gray Firewalls, if required, or Inner Encryption Components.

Although the Outer Encryption Component may be a perimeter device if the Outer Firewall is not present and thus more exposed to external attacks, the Outer Encryption Component is also capable of protecting the network from unauthenticated traffic through use of an internal filtering capability. This allows specification of rules that prohibit unauthorized data flows, which helps mitigate Denial of Service (DoS) 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 11.6. 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 upon an Outer Firewall or Gray Firewall to provide any 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. Management traffic on a Gray

network, which originates from the Administration Workstation, must include two layers of encryption as described in this CP (see Section 11.8).

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). A MSC Solution that supports multiple Red networks of different security levels must include one or more Gray Firewalls, as described in Section 4.2.2.2. The primary purpose of a Gray Firewall is to block 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.

A standalone Gray Firewall, selected from the CSFC Components List, must be physically separate from the Outer Encryption Component and Inner Encryption Component, as depicted in Figure 6. 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 MANAGEMENT WORKSTATION (MW)

The Gray Administration Workstation is responsible for maintaining, monitoring, and controlling all security functionality for the Outer Encryption Component, Gray Firewall, and all Gray Management Service components. The Gray Administration Workstation is not permitted to maintain, monitor, or control Inner Encryption Components or Red Management Services. All MSC Solutions will have at least one Gray Administration Workstation.

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. At a minimum, an auditor reviews the Gray SIEM on a daily basis. 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 if a CDS is used as described in this CP (see Section 7.2).

A Gray SIEM is not a mandatory component of the MSC Solution.

5.5 Inner Encryption Components

Inner Encryption Components can be either 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 will need to be encapsulated prior to being processed by the Outer Encryption Component, regardless of whether it's 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. This CP allows flexibility in the placement of some Red Management Services as described below.

5.7.1 RED ADMINISTRATION WORKSTATION

The Red Administration Workstation is responsible for maintaining, monitoring, and controlling all security functionality for the Inner Encryption Components, Inner Firewall, and all Red Management Service components. The Red Administration Workstation is not permitted to maintain, monitor, or control Outer Encryption Components or Gray Management Services. All MSC Solutions will have at least one Red Administration Workstation.

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. At a minimum an auditor reviews the Red SIEM on a daily basis. The SIEM is configured to provide alerts for specific events.

While Red SIEMs are not a mandatory component of the MSC Solution, customers are encouraged to leverage existing Enterprise SIEM capabilities to monitor log data from Inner Encryption Components and Red Management Services. Although a Red SIEM is not required, logs from all Inner Encryption Components are still required to be analyzed on at least a daily basis. A Red SIEM may also be used to analyze log data from Gray network components when used in conjunction with an approved CDS as described in this CP (see Section 7.2).

5.8 KEY AND CERTIFICATE MANAGEMENT COMPONENTS

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

6 CONFIGURATION AND MANAGEMENT

This CP includes design details for the provisioning and management of Solution Components that requires the use of Security Administrators to initiate certificate requests and Registration Authorities (RAs) to approve certificate requests. The MSC Solution Owner must identify authorized Security Administrators and RAs to initiate and approve certificate requests, respectively. The following sections describe the design in detail and Section 11.8 articulates 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.

During provisioning, 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 (i.e., 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 Administration Workstations that are responsible for maintaining, monitoring, and controlling all security functions for that component. It should be noted that all of the required administrative functionality does not need to be present in each individual workstation, but the entire set of Administration Workstations must collectively meet administrative functionality requirements.

The Administration Workstation is used for configuration review and management. Implementations 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.

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 Administration Workstation, along with all Gray Management Services, is physically connected to the Gray Firewall, if present, or 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.

Administration Workstations must be dedicated terminals for the purposes given in this CP. For example, Administration Workstations are not to be used as the registration authority for the CA, a SIEM, or as a general user workstation for performing any functions besides management of the solution. Additionally, Administration Workstations cannot be used as an enrollment workstation or provisioning workstation. A virtual machine on an Administration Workstation can be used to manage a CSfC solution as long as the Administration Workstation is dedicated only to administering CSfC solutions. However, a dedicated virtual machine on an Administration Workstation used for a non-CSfC solution cannot be used to manage CSfC solutions.

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 (e.g., serial cable from Gray Administration Workstation to 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 being managed from the same LAN or VLAN. For example, a Gray Administration Workstation residing within the Gray Management Services at the same site as the Outer Encryption Component need not use CNSA Suite algorithms since this traffic does not traverse an untrusted network.

7 CONTINUOUS MONITORING

Continuous monitoring allows customers to detect, react to, and report any attacks against their solution. This continuous monitoring also enables the detection of any configuration errors within Solution Components.

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

7.1 MONITORING POINTS

This CP requires monitoring network traffic in at least two of three listed areas within the solution infrastructure if the Black transport network is the Public Internet. Network traffic can be monitored using a CSfC-approved Intrusion Detection System (IDS); however, it is preferable to use an Intrusion

Prevention System (IPS) to enable real-time responses. While monitoring only two of the three locations is required, customers monitoring all three points have the best visibility enabling detection of malicious activity or misconfiguration of components.

Figure 10 depicts the three locations that customers can select to implement network monitoring capabilities. There are several alternatives for deploying the IDS/IPS at two or all of the Monitoring Points (M1, M2, and M3). IDSs/IPSs can ingest traffic from network taps, Switched Port Analyzers (SPANs), or in line with the solution.

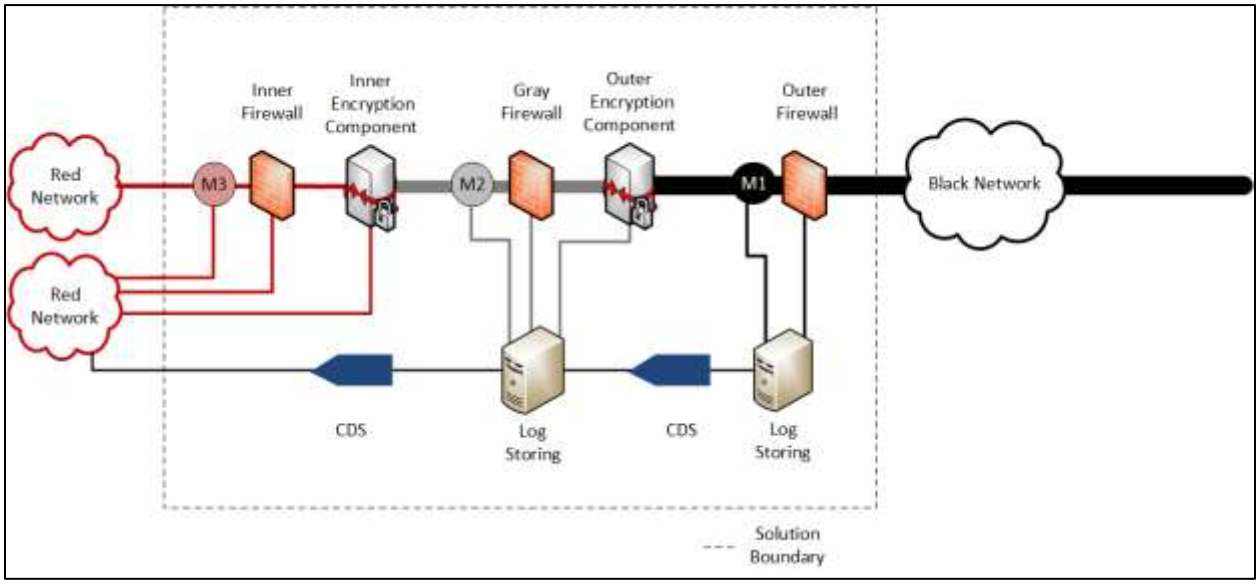

Figure 10. MSC Solution Continuous Monitoring

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

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

Monitoring Point 2 (M2): Located between the Outer Encryption Component and the Gray Firewall (or Inner Encryption Component if a Gray Firewall is not required), a M2 IDS/IPS is, at a minimum, configured to send an alert upon detection of any traffic that should have been blocked by the Outer Encryption Component. These alerts can indicate a failure of the Outer Firewall or Outer Encryption Component's filtering functions and are evidence of either an improper configuration or a potential compromise. Normal traffic at M2 is not as narrowly defined, but includes IPsec, MACsec, control plane traffic, and management traffic. Nearly all traffic traversing M2 is encrypted with IPsec, MACsec or SSHv2, which prevents the ability to perform deep packet inspection. Management of a M2 IDS/IPS occurs within the Gray Management Services.

Monitoring Point 3 (M3): Located between the Inner Encryption Component and the Inner Firewall (or Red network if an Inner Firewall is not required), a M3 IDS/IPS is, at a minimum, configured to send an alert upon detection of any traffic that should have been blocked by the Inner Encryption Component. These alerts indicate a failure of the Inner Encryption Component's filtering function. Of the three monitoring points, M3 is the most difficult to define a normal baseline, but in many implementations, using M3 allows for deep packet inspection since traffic may not be encrypted. Management of the M3 IDS/IPS occurs within the Red Management Services.

Monitoring Multiple Points: Although this CP only requires monitoring of two of the three points when the Black transport network is the Public Internet, customers are encouraged to monitor all three locations. Implementation of three separate components to monitor each point safeguards against malicious traffic from inadvertently being transferred to the Red network.

Movement of network traffic from M3 to the Gray or Black network is explicitly prohibited. Additionally, movement of network traffic from M2 to the Black Network is explicitly prohibited. The advantages of consolidated monitoring at all three points are fully realized when data from all devices is collected within the Red monitoring enclave using a CDS (see Section 7.5) and event correlations (see Section 7.6).

7.2 LOG DATA

SIEMs are not mandatory components of the MSC Solution. However, customers are still required to analyze logs from all Solution Components on at least a daily basis.

SIEMs collect, aggregate, correlate, and analyze security data from Solution Components and provide alerts to Auditors when anomalous behavior is detected.

To allow correlation of data from both Gray and Red components, this CP allows an approved CDS to transport Gray security data to a Red SIEM.

The Gray SIEM is not permitted to collect logs from the Outer Firewall or M1 unless used in conjunction with an approved CDS.

To protect the integrity of the data, all logs sent to the SIEM should be encrypted with SSHv2, TLS 1.2 or later, IPsec or MACsec.

7.3 NETWORK FLOW DATA

Network flow data (e.g., NetFlow, J-Flow, and NetStream) is generated from network devices (e.g., routers, switches and standalone probes) and must be collected and analyzed to provide a picture of network traffic flow and volume. Network flow data consists of IP protocols, source and destination IP addresses, and source and destination ports.

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

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

To maximize the effectiveness of collecting flow data from multiple network segments, all data should be centralized within the Red monitoring enclave for ingest into a single SIEM solution. Section 7.5 below outlines the various use cases for implementing an approved CDS to move Black and Gray data to the Red network.

7.4 CHANGE DETECTION

One method of automating the detection of configuration changes without the complexity and expense of dedicated configuration management systems is to leverage the collection of syslog. In addition to collecting basic security events, the syslog facility is also capable of sending events related to system configuration changes. Queries, which generate alerts for administrators and auditors to review, can be developed on either the log collection server or the SIEM. Change detection is a required component of this CP (see Section 10.7).

7.5 COLLECTION

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

Security event data includes, but is not limited to, syslog, IDS/IPS alerts, and network flow data. The syslog facility can be very broad and include security relevant events, configuration changes, health and status alerts, and other data that may prove useful when assembling the overall status of the security posture of a system. To protect the confidentiality and integrity of the data, all feeds should be encrypted with SSHv2, TLS 1.2 or later, IPsec, or MACsec.

Black Network Segment – The two key components within the Black Network segment are the Outer Firewall and the optional M1 monitoring point. The recommended solution would receive data from both devices on a single data collection server and forward this data to the Gray collection server through an approved CDS.

Gray Network Segment – The key components within the Gray network segment are the Outer Encryption Component, Gray Firewall (if required), the M2 monitoring point (if required), and the associated Gray Management Services.

This CP recommends, at a minimum, that security data be sent directly to a SIEM located within the Gray network. The Gray SIEM may receive data feeds from a central data collection server, as depicted in Figure 10. The Gray SIEM is not permitted to collect data from the Black network segment unless an approved CDS is used.

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

Red Network Segment – The key components within the Red network segment include the Inner Firewall (if required), the Inner Encryption Component, and the M3 monitoring point (if required). All security event data must be sent to a single collection server located within the Red monitoring enclave and may be fed into the Red SIEM solution; however, the Red SIEM is permitted to receive data flows directly from the Red components.

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

7.6 CORRELATION

To support correlation of data from the Black, Gray, and Red components, this CP allows for the use of an approved CDS to feed data from the Black and Gray components into the Red enclave. A Red SIEM should be located within an enclave protected from the larger enterprise of the Red network (see Section 11.9.

8 KEY MANAGEMENT

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

9 REQUIREMENTS OVERVIEW

The following five sections (Sections 10 through Section 14, and the *Key Management Requirements Annex*), specify requirements for implementations of MSC Solutions compliant with this CP. Key Management Requirements have been relocated to a separate Key Management Requirements Annex.

9.1 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 "None" 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 that are listed as Objective in this CP may become Threshold requirements in a future version of this CP. Solution Owners are encouraged to implement Objective requirements where possible to facilitate compliance with future versions of this CP.

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 2 lists the digraphs used to group together related requirements and identifies the sections where those requirement groups can be found.

9.2 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., "KM"), and a sequence number (e.g., 11). Table 2 lists the digraphs used to group together related requirements and identifies the sections where those requirement groups can be found.

Table 2. Requirement Digraphs

Digraph	Description	Section	Table
PS	Product Selection Requirements	Section 10	Table 3
SR	Overall Solution Requirements	Section 10.1	Table 4
VG	VPN Gateway Requirements	Section 10.2	Table 6
MD	MACsec Device Requirements	Section 11.3	Table 7
IR	Additional Requirements for Inner Encryption Components	Section 11.4	Table 9
OR	Additional Requirements for Outer Encryption Components	Section 11.6	Table 10
PF	Port Filtering Requirements for Solution Components	Section 11.6	Table 11
CM	Configuration Change Detection Requirements	Section 11.7	Table 12
DM	Device Management Requirements	Section 11.8	Table 13
MR	Continuous Monitoring Requirements	Section 11.9	Table 14
AU	Auditing Requirements	Section 11.10	Table 15
GD	Requirements for the Use and Handling of Solutions	Section 12.1	Table 16
RP	Incident Reporting Requirements	Section 12.2	Table 17
RB	Role-Based Personnel Requirements	Section 13	Table 18
TR	Testing Requirements	Section 14.1	Table 19
KM	Key Management Requirements (See Key Management Requirements Annex)		

10 REQUIREMENTS FOR SELECTING COMPONENTS

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

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

Once the products for the solution are selected, each product must go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO-approved Product Supply Chain Threat Assessment process (see CNSSD 505 Supply Chain Risk Management (SCRM) for additional guidance).

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

Table 3. 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-1
MSC-PS-2	The products used for any MACsec Device must be chosen from the list of MACsec Ethernet Encryptors on the CSfC Components List.	T=O	
MSC-PS-3	The products used for any Firewalls must be chosen from the list of Traffic Filtering Firewalls (TFFWs) on the CSfC Components List.	T=O	
MSC-PS-4	The products used for any CAs must either be chosen from the list of CAs on the CSfC Components List or the CAs must be pre-existing Enterprise CAs of the applicable network.	T=O	
MSC-PS-5	Intrusion Prevention Systems (IPSs) must be chosen from the list of IPS on the CSfC Components List.	O	None
MSC-PS-6	The Inner Encryption Component and the Outer Encryption Component must either: come from different manufacturers, where neither manufacturer is a subsidiary of the other; or be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence.	T=O	MSC-PS-6
MSC-PS-7	The Inner Encryption Component and the Outer Encryption Component must not use the same Operating System (OS). Differences between Service Packs and version numbers for a particular vendor's OS do not provide adequate diversity.	T=O	
MSC-PS-8	The cryptographic libraries used by the Inner Encryption Component and Outer Encryption Component must either: come from different manufacturers, where neither manufacturer is a subsidiary of the other; or be different libraries from the same manufacturer, where NSA has determined that the libraries meet the CSfC criteria for implementation independence.	O	None
MSC-PS-9	If the solution contains an Inner CA and an Outer CA, the cryptographic libraries must either: come from different manufacturers, where neither manufacturer is a subsidiary of the other; or be	O	None

Req. #	Requirement Description	Threshold/ Objective	Alternative
	different libraries from the same manufacturer, where NSA has determined that the libraries meet the CSfC criteria for implementation independence.		
MSC-PS-10	If Gray Firewalls are used, the Gray Firewalls and Inner Encryption Components must either: come from different manufacturers, where neither manufacturer is a subsidiary of the other; or be two different products from the same manufacturer, where NSA has determined that the two products meet the CSfC criteria for implementation independence.	T=O	
MSC-PS-11	The Inner Encryption Component and Outer Encryption Component must use physically separate components, such that no component is used for more than one function.	T=O	
MSC-PS-12	If an Outer Firewall and/or Gray Firewall is required, the Outer Firewall, Outer Encryption Component, Gray Firewall and Inner Encryption Component must use physically separate components, such that no component is used for more than one function.	T=O	MSC-PS-12
MSC-PS-13	Black Network Enterprise PKI is prohibited from being used as the Outer or Inner tunnel CA.	T=O	
MSC-PS-14	If the solution contains an Inner CA and an Outer CA, the CAs must follow one of the following guidelines: • The CAs come from different manufacturers, where neither manufacturer is a subsidiary of the other. • The CAs are different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence. • The CAs use an Enterprise PKI approved by the AO.	O	None
MSC-PS-15	Each component that is selected from the CSfC Components List must go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO-approved Product Supply Chain Threat Assessment process (see CNSSD 505 SCRM for additional guidance).	T=O	
MSC-PS-16	MSC Solution Components must be configured to use the NIAP-certified evaluated configuration.	T=O	

11 CONFIGURATION REQUIREMENTS

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

11.1 OVERALL SOLUTION REQUIREMENTS

Table 4 provides the overall solution requirements for this CP.

Table 4. Overall Solution Requirements (SR)

Req. #	Requirement Description	Threshold/ Objective	Alternative
MSC-SR-1	Network services provided by control plane protocols (such as DNS and NTP) must be located on the inside network (i.e., Gray network for Outer Encryption Component and Red network for Inner Encryption Component).	T=O	
MSC-SR-2	Sites that need to communicate must ensure that each tunnel's Encryption Components selected by each site are interoperable.	T=O	
MSC-SR-3	The time of day on the Inner Encryption Component and Red Management Services must be synchronized to a time source located in the Red network.	T=O	
MSC-SR-4	The time of day on the Outer Encryption Component, Gray Management Services and Gray Firewall (if present) must be synchronized to a time source located in the Gray management network.	T=O	
MSC-SR-5	Default accounts, passwords, community strings, and other default access control mechanisms for all Solution Components must be changed or removed.	T=O	
MSC-SR-6	All components must be properly configured in accordance with local policy and applicable U.S. Government guidance. In the event of conflict between the requirements in this CP and local policy, this CP takes precedence.	T=O	
MSC-SR-7	All physical paths within a Gray network between Inner Encryption Components for Red networks of different security levels must include a Gray Firewall.	T=O	
MSC-SR-8	All physical paths within a Gray network between a CA, an Administration Workstation, or a CDP/OCSP Responder and an Inner Encryption Component for Red networks of different security levels must include a Gray Firewall.	T=O	
MSC-SR-9	Gray network components must be physically protected to the level of the highest classified network.	T=O	

Req. #	Requirement Description	Threshold/ Objective	Alternative
MSC-SR-10	The Outer Encryption Component must use a unique physical internal interface for each Red network in the MSC Solution (e.g., VLAN trunking of multiple enclaves is not permitted).	T=O	
MSC-SR-11	A Gray Firewall is required if the MSC Solution is combined with another CSfC solution that requires a Gray Firewall.	T=O	
MSC-SR-12	If the MSC Solution uses the Public Internet for its Black transport network, an Outer Firewall must be located between the Black transport network and the Outer Encryption Component.	T=O	
MSC-SR-13	If the MSC Solution is combined with other CSfC data-in-transit solutions that include end user devices, an Inner Firewall is required. All firewall requirements for the other CSfC solution supersede firewall requirements for the MSC CP.	T=O	
MSC-SR-14	The only approved physical paths leaving the Red network must be through a MSC Solution in accordance with this CP or via an AO-approved solution for protecting data in transit[1].	T=O	
MSC-SR-15	Solution Components must receive virus signature updates as required by the local agency policy and the AO.	T=O	
MSC-SR-16	When multiple Inner Encryption Components share an Outer Encryption Component, they must be placed in parallel.	T=O	
MSC-SR-17	Inner Encryption Components must not perform switching or routing for other Encryption Components.	T=O	
MSC-SR-18	Solution Components must only be configured over an interface dedicated for management.	T=O	
MSC-SR-19	DNS lookup services on network devices must be disabled.	O	None
MSC-SR-20	DNS server addresses on Solution Components must be specified or DNS services must be disabled.	T=O	
MSC-SR-21	Automatic remote boot-time configuration services must be disabled (e.g., automatic configuration via Trivial File Transfer Protocol (TFTP) on boot).	T=O	

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

11.2 VPN GATEWAY REQUIREMENTS

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

Table 5. IPsec Encryption (Approved Algorithms for Classified)

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

Table 6. 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 (SA) and the ESP SA for inner and outer tunnels must be configured to offer algorithm suite(s) containing only CNSA Suite algorithms (see Table 5).	T=O	
MSC-VG-2	Default, self-signed or proprietary device certificates, which are frequently preinstalled by the vendor, for any VPN Gateway must not be used for establishing SAs.	T	MSC-VG-3
MSC-VG-3	Default, self-signed or proprietary device certificates, which are frequently preinstalled by the vendor, for any VPN Gateway must be removed.	O	MSC-VG-2
MSC-VG-4	A unique device certificate must be loaded onto each VPN Gateway along with the corresponding CA certificate chain, to include the Trust Anchor CA certificate.	T=O	
MSC-VG-5	The private key stored on VPN Gateways must not be accessible through an interface.	T=O	

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-VG-6	A device certificate must be used for VPN Gateway authentication during IKE.	T=O	
MSC-VG-7	VPN Gateway authentication must include a check that the certificate is not revoked, which can include a CRL, OCSP Responder, whitelist, or other similar revocation reporting mechanism.	T=O	
MSC-VG-8	The VPN Gateway authentication must include a check that certificates are not expired.	T=O	
MSC-VG-9	All VPN Gateways must use IKEv2 (IETF RFC 7296) key exchange.	T=O	
MSC-VG-10	All VPN Gateways must use Cipher Block Chaining for IKE encryption.	T=O	
MSC-VG-11	All VPN Gateways must use Cipher Block Chaining for ESP encryption with a Host-based Message Authentication Code (HMAC) for integrity.	T	MSC-VG-12
MSC-VG-12	All VPN Gateways must use Galois Counter Mode for ESP encryption.	O	MSC-VG-11
MSC-VG-13	All VPN Gateways must set the IKE SA lifetime to at most 24 hours.	T=O	
MSC-VG-14	All VPN Gateways must set the ESP SA lifetime to at most 8 hours.	T=O	
MSC-VG-15	Inner VPN Gateways must only authenticate and establish an IPsec tunnel with one another if their Red networks operate at the same security level (as defined in this CP).	T=O	
MSC-VG-16	All VPN Gateways must re-authenticate the identity of the VPN Gateway at the other end of the established tunnel before rekeying the IKE SA.	T=O	
MSC-VG-17	The Mandatory Access Control policy must only allow the VPN Gateway to access the private key of the VPN Gateway.	O	None

11.3 MACSEC DEVICE REQUIREMENTS

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

Table 7. MACsec Encryption (Approved Algorithms for Classified)

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

Table 8. 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 sizes of 256 bits.	T=O	
MSC-MD-2	MACsec Devices must use AES GCM for MACsec with a cryptographic key sizes of 256 bits.	T=O	
MSC-MD-3	MACsec Devices must authenticate using Pre-Shared Keys (PSKs), known as Connectivity Association Keys (CAKs).	T=O	
MSC-MD-4	Requirement has been relocated to the Key Management Requirements Annex.	T=O	
MSC-MD-5	MACsec Devices must have the length of the CKN set to a minimum of 16 bytes (128 bits) and generate the CKN using an NSA-approved KGS.	T=O	
MSC-MD-6	For each pair of MACsec Devices establishing an encryption tunnel, one of the two must be configured to be the Key Server by setting its Key Server value to 0 (zero). The other MACsec Device must have its Key Server value set to 1. If a Central Management Site is part of the MSC Solution, it must be the Key Server.	T=O	
MSC-MD-7	MACsec Devices must enable data delay protection for MACsec Key Agreement (MKA).	T=O	
MSC-MD-8	MACsec Devices must have an MKA Lifetime Timeout limit set to 6.0 seconds and Hello Timeout limit set to 2.0 seconds.	T=O	
MSC-MD-9	MACsec Devices must have the replay window set to 2 or as low as possible given the nature of the Black network being traversed.	T=O	MSC-MD-9
MSC-MD-10	MACsec Devices must require all data traffic on an external facing port to be encrypted (e.g., must-secure).	T=O	MSC-MD-10
MSC-MD-11	MACsec Device configuration files, whether printed or electronically copied, must be physically protected to the highest classification of the MACsec Device's CAK.	T=O	MSC-MD-11
MSC-MD-12	MACsec Devices must have the Confidentiality Offset set to 0 (zero).	T=O	MSC-MD-12
MSC-MD-13	If a standalone device is required to provide encapsulation of MACsec traffic between an Inner MACsec Device and an Outer Encryption Component, the standalone device must be	T=O	MSC-MD-13

Req. #	Requirement Description	Threshold / Objective	Alternative
	considered a Solution Component when satisfying requirements in Section 11.1.		

11.4 Additional Inner Encryption Component Requirements

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

Table 9. 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, or ESP Transport mode IPsec using an associated IP tunneling protocol (e.g., Transport Mode IPsec with GRE).	T=O	
MSC-IR-2	Sizes for packets or frames leaving the external interface of the Inner Encryption Component must be configured to reduce fragmentation and impact performance. This requires proper configuration of the Maximum Transmission Unit (MTU) (for IPv4 or MACsec) or Path MTU (PMTU) (for IPv6) and should consider Black network and Outer Encryption Component MTU/PMTU values to achieve this.	O	None
MSC-IR-3	The Inner Encryption Component must not allow any packets received on an interface connected to a Red network to bypass encryption and be forwarded out through an interface connected to a Gray network.	T	MSC-IR-4
MSC-IR-4	The Inner Encryption Component must use Mandatory Access Control policy to not allow any packets received on an interface connected to a Red network to bypass encryption and be forwarded out through an interface connected to a Gray network.	O	MSC-IR-3
MSC-IR-5	The Inner Encryption Component must not allow any packets received on an interface connected to a Gray network to bypass decryption and be forwarded out through an interface connected to a Red network.	T	MSC-IR-6
MSC-IR-6	The Inner Encryption Component must use Mandatory Access Control policy to not allow any packets received on an interface connected to a Gray network to bypass decryption and be forwarded out through an interface connected to a Red network.	O	MSC-IR-5
MSC-IR-7	The Inner Encryption Component must not permit split-tunneling.	T=O	

11.5 Additional Requirements for Outer Encryption Components

Additional requirements for Outer Encryption Components are identified Table 10.

Table 10. 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 any packets received on an interface connected to a Gray network to bypass encryption and be forwarded out through an interface connected to a Black network.	T	MSC-OR-3
MSC-OR-3	Outer Encryption Components must use Mandatory Access Control policy to not allow any packets received on an interface connected to a Gray network to bypass encryption and be forwarded out through an interface connected to a Black network.	O	MSC-OR-2
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	

11.6 Port Filtering Solution Components Requirements

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

Table 11. Port Filtering (PF) Requirements for Solution Components

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	

Req. #	Requirement Description	Threshold/ Objective	Alternative
MSC-PF-3	For all Outer VPN Gateway interfaces connected to a Black network, traffic filtering rules must be applied to both inbound and outbound traffic, such that only IKE, ESP, and control plane protocols (as defined in this CP) approved by organization-defined policy are allowed.	T=O	
MSC-PF-4	For all Outer MACsec Device interfaces connected to a Black network, traffic filtering rules must be applied to both inbound and outbound traffic, such that only MACsec Protocol Data Units (MPDUs) and control plane protocols (as defined in this CP) approved by organization-defined policy are allowed.	T=O	
MSC-PF-5	For all Inner Encryption Component interfaces connected to a Gray network, traffic filtering rules must be applied to both inbound and outbound traffic, such that only IKE, IPsec, MKA, MACsec, and 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 the Gray Administration Workstation with the exception of logging or authentication traffic that may be initiated from Outer Encryption Components.	T=O	
MSC-PF-9	Multicast messages received on external interfaces of Outer Encryption Components must be dropped.	T=O	
MSC-PF-10	For solutions using IPv4, Outer VPN Gateways using IPsec must drop all packets that use IP options.	O	
MSC-PF-11	For solutions using IPv4, each VPN Gateway must only accept packets with Transmission Control Protocol (TCP), User Datagram Protocol (UDP), ESP, or ICMP in the IPv4 Protocol field and drop all other packets.	T=O	
MSC-PF-12	For solutions using IPv6, each VPN Gateway must only accept packets with ESP, TCP, UDP, or ICMPv6 in the IPv6 Next Header field and drop all other packets.	T=O	
MSC-PF-13	The Gray network interfaces of Outer Encryption Components must allow IKE and IPsec, or MKA and MACsec traffic, as appropriate, that is between two Inner Encryption Components protecting networks of the same security level or that is being used for management of the Gray network.	T=O	
MSC-PF-14	The Gray network interfaces of Outer VPN Gateways must allow HTTP traffic between Inner VPN Gateways and Inner CDPs/OCSP Responders.	T	MSC-PF-15 and MSC-PF-16
MSC-PF-15	The Gray network interfaces of Outer VPN Gateways must allow HTTP GET and OCSP requests from Inner VPN	O	MSC-PF-14

Req. #	Requirement Description	Threshold/ Objective	Alternative
	Gateways to Inner CDPs and OCSP Responders, respectively, for the Uniform Resource Locator (URL) of the CRL or OCSP response needed by the Inner VPN Gateway, and block all other HTTP requests.		
MSC-PF-16	The Gray network interfaces of Outer VPN Gateways must allow HTTP responses from Inner CDPs/OCSP Responders to Inner VPN Gateways that contain a well-formed CRL per IETF RFC 5280 or a well-formed OCSP response per IETF RFC 6960, and block all other HTTP responses.	O	MSC-PF-14
MSC-PF-17	The Gray network interfaces of Outer Encryption Components must only permit packets whose source and destination IP addresses match the external interfaces of Inner Encryption Components that support Red networks of the same security level.	T=O	
MSC-PF-18	The Gray network interfaces of Outer Encryption Components must block all packets whose source address does not match a list of addresses or address ranges known to be reachable from the interface where the packet was received.	T=O	
MSC-PF-19	The Gray network interfaces of Outer Encryption Components must allow management and control plane protocols (as defined in this CP) that have been approved by policy.	T=O	
MSC-PF-20	The Gray network interfaces of Outer Encryption Components must deny all traffic that is not explicitly allowed by requirements MSC-PF-8, MSC-PF- 13, MSC-PF-14, MSC-PF-15, MSC-PF-16, or MSC-PF-19.	T=O	
MSC-PF-21	CDPs/OCSP Responders must only allow inbound and outbound HTTP traffic per requirements MSC-PF-14, MSC-PF-15, and MSC-PF-16.	T=O	
MSC-PF-22	If an Outer Firewall is required, for all Outer Firewall interfaces, traffic filtering rules must be applied to both inbound and outbound traffic, such that only IKE, ESP, MKA, MACsec and control plane protocols (as defined in this CP) approved by organization-defined policy are allowed.	T=O	
MSC-PF-23	If a Gray Firewall is required, the Gray Firewall must permit IKE, IPsec, MKA and MACsec traffic between two Inner Encryption Components protecting networks of the same security level.	T=O	
MSC-PF-24	If a Gray Firewall is required, the Gray Firewall must allow HTTP traffic between Inner VPN Gateways and Inner CDP/OCSP Responder.	T	MSC-PF-25 and MSC-PF-26
MSC-PF-25	If a Gray Firewall is required, the Gray Firewall must allow HTTP GET and OCSP requests from Inner VPN Gateways to Inner CDPs/OCSP Responders for the URL of the CRL or OCSP response needed by the Inner VPN Gateway, and block all other HTTP requests.	O	MSC-PF-24

Req. #	Requirement Description	Threshold/ Objective	Alternative
MSC-PF-26	If a Gray Firewall is required, the Gray Firewalls must allow HTTP responses from Inner CDPs/OCSP Responders to Inner VPN Gateways that contain a well-formed CRL per IETF RFC 5280 or well-formed OCSP response per IETF RFC 6960, and block all other HTTP responses.	O	MSC-PF-24
MSC-PF-27	If a Gray Firewall is required, the Gray Firewall must only accept management traffic on the physical ports connected to the Gray management network.	T=O	
MSC-PF-28	If a Gray Firewall is required, the Gray Firewall must only permit packets whose source and destination IP addresses match the external interfaces of Inner Encryption Components that support Red networks of the same security level.	T=O	
MSC-PF-29	If a Gray Firewall is required, the Gray Firewall must block all packets whose source address does not match a list of addresses or address ranges known to be reachable from the interface where the packet was received.	T=O	
MSC-PF-30	If a Gray Firewall is required, the Gray Firewall must allow control plane traffic (e.g., NTP, DHCP, and DNS).	T=O	
MSC-PF-31	If a Gray Firewall is required, the Gray Firewall must deny all traffic that is not explicitly allowed by requirements MSC-PF-23, MSC-PF- 24, MSC-PF-25, MSC-PF-26, MSC-PF-27 or MSC-PF-30.	T=O	

11.7 Configuration Change Detection Requirements

Table 12. defines the requirements for Configuration Change Detection.

Table 12. Configuration Change Detection (CM) Requirements

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

11.8 Device Management Requirements

Table 13 defines the requirements for Device Management.

Table 13. Device Management (DM) Requirements

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-DM-1	Administration Workstations must be dedicated for the purposes given in this CP and must be physically separated from workstations used to manage non-CSfC solutions.	T=O	
MSC-DM-2	Administration Workstations must physically reside within a protected facility where CSfC solution(s) are managed.	T=O	
MSC-DM-3	Administration Workstations must connect from an internal port. Specifically, the Inner Encryption Component must be managed from the Red network, and the Outer Encryption Component and Gray Firewall, if present, must be managed from the Gray network.	T=O	
MSC-DM-4	A separate LAN or VLAN on the Red network must be used exclusively for all management of Inner Encryption Components and Solution Components within the Red network.	T=O	
MSC-DM-5	A separate LAN or VLAN on the Gray network must be used exclusively for all management of the Outer Encryption Component, Gray Firewall, if present, and Solution Components within the Gray network.	T=O	
MSC-DM-6	The Gray management network must not be directly connected to the Non-secure Internet Protocol Router Network (NIPRNet) or any other Unclassified network not dedicated to the administration of CSfC solutions.	T=O	
MSC-DM-7	All components must be configured to restrict the IP address range for the network administration device to the smallest range possible. Note that locally managing Solution Components is also acceptable.	T=O	
MSC-DM-8	All administration of Solution Components must be performed from an Administration Workstation remotely using an NSA-approved solution (e.g., CP or Type 1 encryptor), or by managing the Solution Components locally.	T=O	
MSC-DM-9	Security Administrators must authenticate to Solution Components before performing administrative functions.	T	MSC-DM-10
MSC-DM-10	Security Administrators must authenticate to Solution Components with CNSA Suite compliant certificates before performing administrative functions remotely.	O	MSC-DM-9

Req. #	Requirement Description	Threshold / Objective	Alternative
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	Authentication of Security Administrators must be enforced by either procedural or technical means.	O	None
MSC-DM-14	Administration Workstations that interact with the Certificate Authority for the Outer VPN Gateways must be located on the Gray network.	T=O	
MSC-DM-15	Requirement has been relocated to the Key Management Requirements Annex.		
MSC-DM-16	Requirement has been relocated to the Key Management Requirements Annex.		
MSC-DM-17	The same Administration Workstation must not be used to manage Inner Encryption Components and Outer Encryption Components.	T=O	
MSC-DM-18	If SIEMs are used in the solution, Outer Encryption Components and Solution Components within the Gray network must forward log entries to a SIEM on the Gray management network (or SIEM in the Red network if using a CDS) within 10 minutes of the event's occurrence.	T=O	
MSC-DM-19	If SIEMS are used in the solution, Inner Encryption Components and Solution Components within the Red network must forward log entries to a SIEM on the Red management network within 10 minutes of the event's occurrence.	T=O	
MSC-DM-20	If SIEMS are used in the solution, all logs forwarded to a SIEM on the Gray management network must be encrypted using SSHv2, IPsec, MACsec, or TLS 1.2 or later.	O	None
MSC-DM-21	If SIEMS are used in the solution, all logs forwarded to a SIEM on a Red management network must be encrypted using SSHv2, IPsec, MACsec, or TLS 1.2 or later.	O	None
MSC-DM-22	Outer Encryption Components must only be managed by Security Administrators cleared to at least the highest level of classification of each Red network supported by the Outer Encryption Component at the physical site the Outer Encryption Component is located.	T=O	

11.9 CONTINUOUS MONITORING REQUIREMENTS

Continuous monitoring requirements are identified in Table 14.

Table 14. Requirements for Continuous Monitoring (MR)

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

Req. #	Requirement Description	Threshold / Objective	Alternative
	• Between the Inner Encryption Component and Inner Firewall, if present, or the Red network (M3).		
MSC-MR-7	If IDSs are part of the solution, each IDS must be configured to provide a dashboard or send alerts to the Security Administrator.	T	MSC-MR-8
MSC-MR-8	If IPSs are part of the solution, each IPS must be configured to block malicious traffic flows and alert the Security Administrator.	O	MSC-MR-7
MSC-MR-9	If IDSs are part of the solution, each IDS must be configured with rules that generate alerts upon detection of any unauthorized destination IP addresses.	T	MSC-MR-10
MSC-MR-10	If IPSs are part of the solution, each IPS must be configured with rules that block and generate alerts upon detection of any unauthorized destination IP addresses.	O	MSC-MR-9
MSC-MR-11	If IDSs are part of the solution, each IDS must be configured with rules that generate alerts upon detection of any unauthorized source IP addresses.	T	MSC-MR-12
MSC-MR-12	If IPSs are part of the solution, each IPS must be configured with rules that block and generate alerts upon detection of any unauthorized source IP addresses.	O	MSC-MR-11
MSC-MR-13	If SIEMs are part of the solution, a SIEM component must be placed within the Gray network unless devices are configured to push events to a Red network SIEM through an approved CDS.	T=O	
MSC-MR-14	If SIEMs are part of the solution, the SIEM must be configured to send alerts to the Security Administrator when anomalous behavior is detected (e.g., blocked packets from the Outer Encryption Component or Gray Firewall).	T=O	
MSC-MR-15	If a Gray SIEM is part of the solution, the Gray SIEM must collect logs from the Outer Encryption Component, Gray Firewall, and any components located within the Gray Management Services.	T=O	
MSC-MR-16	If a Gray SIEM is part of the solution, the Gray SIEM must maintain an up-to-date table of Certificate Common Name and assigned IP address used for the Outer VPN Gateway.	T=O	
MSC-MR-17	If a Gray SIEM is part of the solution, the Gray SIEM must provide a dashboard or alert for sites attempting to establish a connection with the Outer Encryption Component using misconfigured settings.	T=O	
MSC-MR-18	If a Gray SIEM is part of the solution, the Gray SIEM must provide an alert or dashboard for three or more invalid login attempts in a 24-hour period to the Outer Encryption Component and Gray Firewall, if present.	T=O	

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-MR-19	If a Gray SIEM is part of the solution, the Gray SIEM must provide an alert or dashboard of privilege escalations on the Outer Encryption Component and Gray Firewall, if present.	T=O	
MSC-MR-20	If a Gray SIEM is part of the solution, the Gray SIEM must provide an alert or dashboard of configuration changes to the Outer Encryption Component and Gray Firewall, if present.	T=O	
MSC-MR-21	If a Gray SIEM is part of the solution, the Gray SIEM must provide an alert or dashboard of new accounts created on the Outer Encryption Component and Gray Firewall, if present.	T=O	
MSC-MR-22	If a Gray SIEM is part of the solution, the Gray SIEM must provide an alert or dashboard for attempted connections to the Outer Encryption Component that use invalid certificates or keys.	T=O	
MSC-MR-23	If a Gray SIEM is part of the solution, the Gray SIEM must provide an alert, graph or table of blocked traffic at the Gray Firewall (if present) grouped by Common Name.	T=O	
MSC-MR-24	If a Gray SIEM is part of the solution, the Gray SIEM must provide a dashboard or alert for DNS queries other than expected values for IP addresses and domains.	O	None
MSC-MR-25	Network flow data must be enabled on all routers and switches in the Red network.	T=O	
MSC-MR-26	A network flow data collector (e.g., SILK, IPFlow, and NetFlow Collector) must be installed in the Red network.	T=O	
MSC-MR-27	A baseline for network flow data must be established.	O	None
MSC-MR-28	A baseline for network flow data must be updated regularly at an interval determined by the AO.	O	None
MSC-MR-29	Network flow data must be reviewed daily for: • Systems generating excessive amounts of traffic. • Systems trying to connect to improper IP addresses. • Systems trying to connect to closed ports on internal servers.	O	None
MSC-MR-30	Network flow data must be reviewed for systems generating an excessive number of short packets (e.g., over 60% of packets containing 150 bytes or less).	O	None
MSC-MR-31	Network flow data must be reviewed for excessive numbers of ICMP messages.	O	None

11.10 AUDITING REQUIREMENTS

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

Table 15. Auditing (AU) Requirements

Req. #	Requirement Description	Threshold/ Objective	Alternative
MSC-AU-1	Encryption Components must log establishment of an encryption tunnel.	T=O	
MSC-AU-2	Encryption Components must log termination of an encryption tunnel.	T=O	
MSC-AU-3	Solution Components must log all actions performed on the audit log (e.g., off-loading, deletion).	T=O	
MSC-AU-4	Solution Components must log all actions involving identification and authentication.	T=O	
MSC-AU-5	Solution Components must log attempts to perform an unauthorized action (e.g., read, write, execute, delete) on an object.	T=O	
MSC-AU-6	Solution Components must log all actions performed by a user with super-user or administrator privileges.	T=O	
MSC-AU-7	Solution Components must log escalation of user privileges.	T=O	
MSC-AU-8	Solution Components must log generation, loading, and revocation of certificates.	T=O	
MSC-AU-9	Solution Components must log changes to time.	T=O	
MSC-AU-10	Solution Components must log when packets received on Gray network interfaces are dropped or blocked.	T=O	
MSC-AU-11	Solution Components must log the results of built-in self-tests.	T=O	
MSC-AU-12	MACsec Devices must log the installation of a CAK into the MACsec Device, including all subsequent installations of new CAKs (i.e., CAK rekey).	T=O	
MSC-AU-13	MACsec Devices must log creation and updates of SAKs.	T=O	
MSC-AU-14	MACsec Devices must log administrator lockout due to excessive authentication failures.	T=O	
MSC-AU-15	MACsec Devices must log detected replay attempts.	T=O	
MSC-AU-16	Each log entry must record the date and time of the event.	T=O	
MSC-AU-17	Each log entry must include the identifier of the event.	T=O	
MSC-AU-18	Each log entry must record the type of event.	T=O	
MSC-AU-19	Each log entry must record the success or failure of the event to include failure code, when available.	T=O	
MSC-AU-20	Each log entry must record the subject identity.	T=O	
MSC-AU-21	Each log entry must record the source address for network-based events.	T=O	
MSC-AU-22	Each log entry must record the user and, for role-based events, role identity, where applicable.	T=O	
MSC-AU-23	VPN Gateways must log the failure to download the CRL from a CDP.	T=O	

Req. #	Requirement Description	Threshold/ Objective	Alternative
MSC-AU-24	VPN Gateways must log if the version of the CRL downloaded from a CDP is older than the current cached CRL.	T=O	
MSC-AU-25	VPN Gateways must log if signature validation of the CRL downloaded from a CDP fails.	T=O	
MSC-AU-26	Auditors must compare and analyze collected network flow data against the established baseline on at least a daily basis.	T=O	
MSC-AU-27	Locally-run CAs must comply with the audit and archival requirements defined in IETF RFC 3647 Sections 4.5.4 and 4.5.5, respectively.	T=O	
MSC-AU-28	Locally-run CAs must comply with periodic audit and assessment requirements defined in IETF RFC 3647 Section 4.8.	T=O	
MSC-AU-29	Audits and assessments for a CA must be performed by personnel who are knowledgeable in the CA's operations, as well as the CA's Certificate Policy and CPS requirements and processes, respectively.	T=O	
MSC-AU-30	KGSs that deliver CAK Management Services for MSC Solutions are to comply with audit and assessment requirements defined by the customer's operational security doctrine and enterprise KGS (if applicable).	T=O	
MSC-AU-31	Audits and assessments for a KGS are to be performed by personnel who are knowledgeable in the KGS's operations, as well as the KGS's audit requirements and processes, respectively.	T=O	

11.11 Key Management Requirements

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

12 REQUIREMENTS FOR SOLUTION OPERATIONS, MAINTENANCE, AND HANDLING

12.1 Requirements for the Use and Handling of Solutions

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

Table 16. Requirements for the Use and Handling of Solutions

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	T=O	

Req. #	Requirement Description	Threshold / Objective	Alternative
	with the highest classification in the solution or in any other MSC Solutions with which it is interconnected.		
MSC-GD-2	Only authorized and appropriately cleared (or escorted) administrators and security personnel must have physical access to the Solution Components.	T=O	
MSC-GD-3	All components of the solution must be disposed of as classified devices, unless declassified using AO-approved procedures.	T=O	
MSC-GD-4	Acquisition and procurement documentation must not include information concerning the purpose of the equipment, to include that it will be used to protect classified information.	T=O	
MSC-GD-5	The Solution Owner must allow, and fully cooperate with, NSA or its authorized agent to perform an Information Assurance (IA) compliance audit (including, but not limited to, inspection, testing, observation, and interviewing) of the solution implementation to ensure it meets the latest version of this CP.	T=O	
MSC-GD-6	The AO will ensure that a compliance audit must be conducted every year against the latest version of this CP as part of the annual solution re-registration process.	T=O	
MSC-GD-7	Results of the compliance audit must be provided to and reviewed by the AO.	T=O	
MSC-GD-8	Customers interested in registering their solution against this CP must register with NSA and receive approval prior to operating the solution.	T=O	
MSC-GD-9	The implementing organization must complete and submit an MSC CP requirements compliance matrix to their respective AO.	T=O	
MSC-GD-10	Registration and re-registration against this CP must include submission of CP registration forms and compliance matrix to NSA.	T=O	
MSC-GD-11	When a new approved version of the MSC CP is published by NSA, the AO must ensure compliance against this new CP within 6 months.	T=O	
MSC-GD-12	Solution implementation information that was provided to NSA during solution registration must be updated annually (in accordance with Section 14.3) as part of the annual re-registration process.	T=O	
MSC-GD-13	Audit log data must be maintained for a minimum of 1 year.	T=O	
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	

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-GD-15	Audit data must be off-loaded to a backup storage medium at least once a week.	T=O	
MSC-GD-16	The implementing organization must develop a set of procedures to provide guidance for identifying and reporting security incidents associated with the audit events to the proper authorities and to the data owners.	T=O	
MSC-GD-17	The implementing organization must develop a continuity of operations plan for auditing capability that includes a mechanism or method for determining when the audit log is reaching its maximum storage capacity.	T=O	
MSC-GD-18	The implementing organization must develop a continuity of operations plan for auditing capability that includes a mechanism or method for off-loading audit log data for long-term storage.	T=O	
MSC-GD-19	The implementing organization must develop a continuity of operations plan for auditing capability that includes a mechanism or method for responding to an overflow of audit log data within a product.	T=O	
MSC-GD-20	The implementing organization must develop a continuity of operations plan for auditing capability that includes a mechanism or method for ensuring the audit log can be maintained during power events.	T=O	
MSC-GD-21	Strong passwords must be used that comply with the requirements of the AO.	T=O	
MSC-GD-10	Registration and re-registration against this CP must include submission of CP registration forms and compliance matrix to NSA.	T=O	
MSC-GD-22	The implementing organization must test and subsequently apply security critical patches to all components in the solution in accordance with local policy and this CP.	T=O	
MSC-GD-23	Local policy must dictate how the Security Administrator will install patches to Solution Components.	T=O	
MSC-GD-24	Solution Components must comply with local TEMPEST policy.	T=O	
MSC-GD-25	All hardware components must be tracked through an AO-approved inventory management process that identifies each component as part of a CSfC solution.	T=O	

12.2 Requirements for Incident

Table 17 lists requirements for reporting security incidents to NSA to be followed in the event that a Solution Owner identifies a security incident that affects the solution. These reporting requirements are intended to augment, not replace, any incident reporting procedures already in use within the Solution

Owner's organization. It is critical that Security Administrators, Certification Authority Administrators (CAAs), KGSAs, and Auditors are familiar with maintaining the solution in accordance with this CP. Based on familiarity with the known-good configuration of the solution, personnel responsible for the operations and maintenance of the solution will be better equipped to identify reportable incidents.

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

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

Table 17. Incident Reporting 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-14 within 24 hours of detection via the Joint Incident Management System (JIMS) or contacting NSA as specified in the CSfC Registration Letter issued for the solution.	T=O	
MSC-RP-2	At a minimum, the organization must provide the following information when reporting security incidents: • CSfC Registration Number • Primary POC name, phone, email • Alternate POC name, phone, email • Security level of affected solution • Name of affected network(s) • Affected component(s) manufacturer/ vendor • Affected component(s) model number • Affected component(s) version number • Date and time of incident • Description of incident • Description of remediation activities • Is Technical Support from NSA requested? (Yes/No)	T=O	
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	

Req. #	Requirement Description	Threshold/ Objective	Alternative
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	
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	

13 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.

Certification Authority Administrator (CAA) – The CAA must maintain, monitor, and control all security functions for the CA products. CAA duties include, but are not limited to:

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

2) Maintain and update the CRL.

3) Provision and maintain certificates in accordance with this CP for implementations that use them.

Key Generation Solution Administrator (KGSA) – The KGSA must maintain, monitor, and control all security functions for the KGS products. KGSA duties include, but are not limited to:

1) Administer the KGS, including authentication of all components requesting CAKs and CAK Encryption Key (CEKs).

2) Maintain and update the CAK and CEK revocation lists.

3) Provision and maintain CAKs and CEKs in accordance with this CP for implementations that use them.

Auditor – The Auditor must review the actions performed by the Security Administrator, CAA or KGSA, 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.

Additional policies related to the personnel that perform these roles in a MSC Solution are identified in Table 18.

Table 18. Role-Based Personnel Requirements

Req. #	Requirement Description	Threshold/ Objective	Alternative
MSC-RB-1	The Security Administrators, CAAs, KGSAs, Auditors, and Integrators must be cleared to the highest level of data	T=O	

Req. #	Requirement Description	Threshold/ Objective	Alternative
	protected by the MSC Solution. When an Enterprise CA/KGS is used in the solution, the CAA/KGSA already in place may also support this solution, provided they meet this requirement. Black network Administrators may be cleared at the Black network security level.		
MSC-RB-2	The Security Administrator, CAA, KGSA, and Auditor roles must be performed by different people.	T=O	
MSC-RB-3	All Security Administrators, CAAs, KGSAs, and Auditors must meet local IA training requirements.	T=O	
MSC-RB-4	The CAA(s) for the inner tunnel must be different individuals from the CAA(s) for the outer tunnel.	T=O	
MSC-RB-5	The Security Administrator(s) for the Inner Encryption Components and supporting components on the Red network must be different individuals from the Security Administrator(s) for the Outer Encryption Components and supporting components on the Gray network.	T=O	
MSC-RB-6	Administrators must periodically inspect the physical attributes of infrastructure hardware for signs of tampering or other unauthorized changes.	T=O	
MSC-RB-7	The Auditor must review all logs specified in this CP at least once a day.	T=O	
MSC-RB-8	Security Administrators must initiate the certificate revocation/CAK destruction process prior to disposal of any Solution Component.	T=O	
MSC-RB-9	Auditing of the Outer and Inner CA operations must be performed by individuals who were not involved in the development of the Certificate Policy and CPS, or integration of the MSC Solution.	T=O	
MSC-RB-10	Auditing of the KGS operations must be performed by individuals who were not involved in the development of the KMP, or integration of the MSC Solution.	T=O	
MSC-RB-11	Mandatory Access Control policy must specify roles for Security Administrator, CAA, KGSA, and Auditor using role-based access controls.	O	None

14 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 14.1).
- The customer has the security control assessment and system authorization performed using the risk assessment information referenced in Section 14.2.
- 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 14.3.
- 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 Table 12.2.

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.

14.1 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 following test requirements has been developed to ensure that the MSC Solution functions properly and meets the configuration requirements from Section 11. Testing of these requirements should be used as a minimum framework for the development of the detailed T&E plan and procedures.

Table 19. Test (TR) Requirement

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-TR-1	The organization implementing the CP must perform all tests listed in the MSC CP Testing Annex.	T=O	

14.2 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.

14.3 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/everyone/csfc).

Solution registrations are valid for one year from the date the solution registration is approved, at which time customers are required to re-register their solution 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 Administration Workstation to the device in a hardwired fashion (such as a console cable).

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

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
BGP	Border Gateway Protocol
CA	Certification Authority
CAA	Certification Authority Administrator
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
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
KGS	Key Generation Solution

Acronym	Meaning
KGSA	Key Generation Solution Administrator
KM	Key Management
MACsec	Media Access Control Security
MKA	MACsec Key Agreement
MSC	Multi-Site Connectivity
MTU	Maximum Transmission Unit
NDP	Neighbor Discovery Protocol
NIAP	National Information Assurance Partnership
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
VPN	Virtual Private Network
XPN	eXtended Packet Number

APPENDIX C. REFERENCES

CNSSD 505	*CNSS Directive (CNSSD) Number 505, Supply Chain Risk Management (SCRM)*	March 2012
CNSSI 1253	*CNSS Instruction (CNSSI) 1253, Security Categorization and Control Selection for National Security Systems*	March 2014
CNSSI 1300	*CNSS Instruction (CNSSI) 1300, National Security Systems Public Key Infrastructure X.509 Certificate Policy*	December 2014
CNSSI 4009	*CNSS Instruction (CNSSI) 4009, Committee on National Security Systems Glossary*	April 2015
CNSSP 11	*CNSS Policy (CNSSP) Number 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products*	June 2013
CNSSP 15	*CNSS Policy (CNSSP) Number 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems Committee for National Security Systems*	October 2016
FIPS 140-2	*Federal Information Processing Standard 140, Security Requirements For Cryptographic Modules.* National Institute for Standards and Technology (NIST).	May 2001
FIPS 180-4	*Federal Information Processing Standard 180-4, Secure Hash Standard (SHS).* NIST.	August 2015
FIPS 186-4	*Federal Information Processing Standard 186-4, Digital Signature Standard (DSS).* NIST.	July 2013
FIPS 197	*Federal Information Processing Standard 197, Advanced Encryption Standard (AES).* NIST.	November 2001
IAD MD-110	*Information Assurance Directorate Management Directive No. 110, Cryptographic Key Protection*	July 2011
IEEE 802.1AE-2006	*IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security*	August 2006
IEEE 802.1AEbn-2011	*IEEE Standard for Local and Metropolitan Area Networks--Media Access Control (MAC) Security Amendment 1: Galois Counter Mode--Advanced Encryption Standard-- 256 (GCM-AES-256) Cipher Suite*	October 2011
IEEE 802.1 AEbw-2013	*IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Security Amendment 2: Extended Packet Numbering*	February 2013
IEEE 802.1AEcg-2016 (draft)	*IEEE Standard for Media Access Control (MAC) Security Amendment: Ethernet Data Encryption Devices, Draft, June 2016*	June 2016
RFC 3526	*IETF RFC 3526 More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE).* T. Kivinen and M. Kojo.	May 2003
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 4307	*IETF RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*. J. Schiller.	December 2005
RFC 4308	*IETF RFC 4308 Cryptographic Suites for IPsec*. P. Hoffman.	December 2005
RFC 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 5759	*IETF RFC 5759 Suite B Certificate and Certificate Revocation List (CRL) Profile*. J. Solinas and L. Zieglar.	January 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 6379	*IETF RFC 6379 Suite B Cryptographic Suites for IPsec*. L. Law and J. Solinas.	October 2011
RFC 6380	*IETF RFC 6380 Suite B Profile for Internet Protocol Security (IPsec)*. K. Burgin and M. Peck.	October 2011
RFC 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 6818	*IETF RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. P. Yee.	January 2013
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 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 7905	*IETF RFC 7905 ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS).* A. Langley, et. al.	June 2016
RFC 7919	*IETF RFC 7919 Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS).* D. Gillmor.	August 2016
SP 800-56A	*NIST Special Publication 800-56A Rev. 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*. E. Barker, et. al.	May 2013
SP 800-56B	*NIST Special Publication 800-56B Rev. 1, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*. E. Barker, et. al.	September 2014
SP 800-56C	*NIST Special Publication 800-56C, Recommendation for Key Derivation through Extraction-then-Expansion*. L. Chen.	November 2011
SP 800-57	*NIST Special Publication 800-57 Part 1 Rev 4, Recommendation for Key Management Part 1: General.* E. Barker.	January 2016
SP 800-131A	*NIST Special Publication 800-131A Rev. 1, Recommendation for Transitioning of Cryptographic Algorithms and Key Lengths*. E. Barker and A. Roginsky.	November 2015