National Security Agency/
Central Security Service

CYBERSECURITY SOLUTIONS

# MULTI-SITE CONNECTIVITY CAPABILITY PACKAGE V1.1.8

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

Version 1.1.8
May 2021

## 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*".<br>• Updated requirements to use "must" instead of "shall."<br>• Minor administrative changes were made in formatting.<br>• Added bullet #6 to the "Security Administrator" definition. |
| CSfC MSC Capability Package | 1.1.8 | May 2021 | • Clarified Logging<br>• Expanded Administrative Workstation Options<br>• Improved Community of Interest Separation Requirements<br>• Eliminated Transport Mode IPSec as an Alternate to Tunnel Mode IPSec<br>• Clarified Filtering Requirements<br>• Added Objective Requirements for Transport Flow Security (TRANSEC)<br>• IKEv2 for PSK<br>• Updated the CP to fully use the MKA feature set (Objective Requirements)<br>• Ensured clarification across the entire CP and supporting documents.<br>• Minor administrative changes made in editing and formatting |

# TABLE OF CONTENTS

## TABLE OF FIGURES



## LIST OF TABLES

121

# 1 INTRODUCTION

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

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

While CSfC encourages industry innovation, trustworthiness of the components is paramount. Customers and their Integrators are advised that modifying a NIAP-validated component in a CSfC solution may invalidate its certification and require a revalidation process. To avoid delays, customers and Integrators who feel it is necessary to modify a component should engage the component vendor and consult NIAP through their Assurance Continuity Process (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, the NSA's CSfC Program Management Office (PMO) requires a statement from NIAP that the modification does not alter the certification, or the security of the component. Modifications that trigger the revalidation process include, but are not limited to; configuring the component in a manner different from its NIAP-validated configuration, and modifying the Original Equipment Manufacturer's code (to include digitally signing the code).

# 2 PURPOSE AND USE

This CP provides high-level reference designs and corresponding configuration 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 permit the necessary functionality for the selected capabilities. As described in Section 9, to successfully implement a solution based on this CP, all Threshold (T) requirements, or the corresponding Objective (O) requirements applicable to the selected capabilities, must be implemented.

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

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.

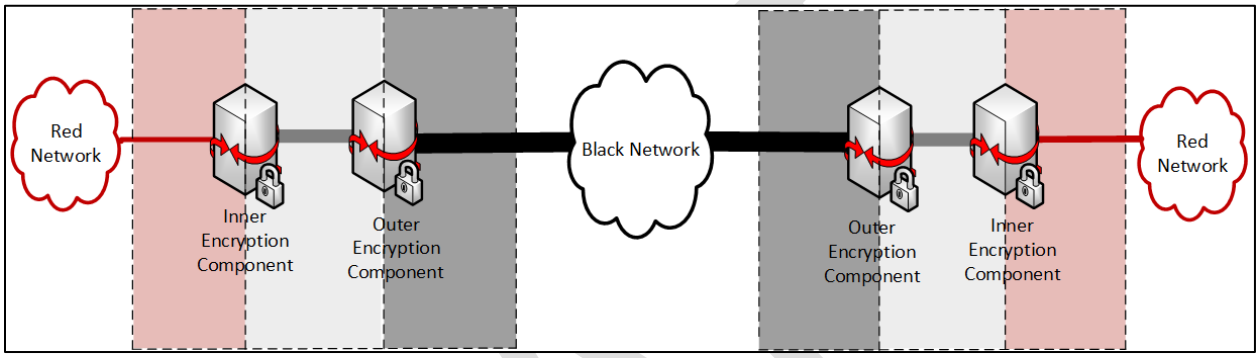


**Figure 1. Two Encryption Tunnels Protect Data Across an Untrusted Network**

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

## 4.1 NETWORKS

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

### 4.1.1 RED NETWORK

Red data consists of unencrypted classified data. The Red Network is logically located behind an Inner Encryption Component. The networks connected to one another through the MSC Solution are Red Networks. Red Networks 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 Management Workstation (MW) that can be a physical workstation or Virtual Machine (VM). The Gray Management Services may also include a Security Information and Event Management (SIEM) unless the SIEM is implemented in the Red Network in conjunction with a cross domain solution (CDS) (see Section 7). This CP requires the management of Gray Network components through a Gray MW. As a result, neither Red nor Black MWs are permitted to manage the Outer Encryption Component, Gray Firewall, or Gray Management Services. Additionally, the Gray MWs are prohibited from managing Inner Encryption Components. Inner Encryption Components must be managed from a Red MW.

### 4.1.3 BLACK NETWORK

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

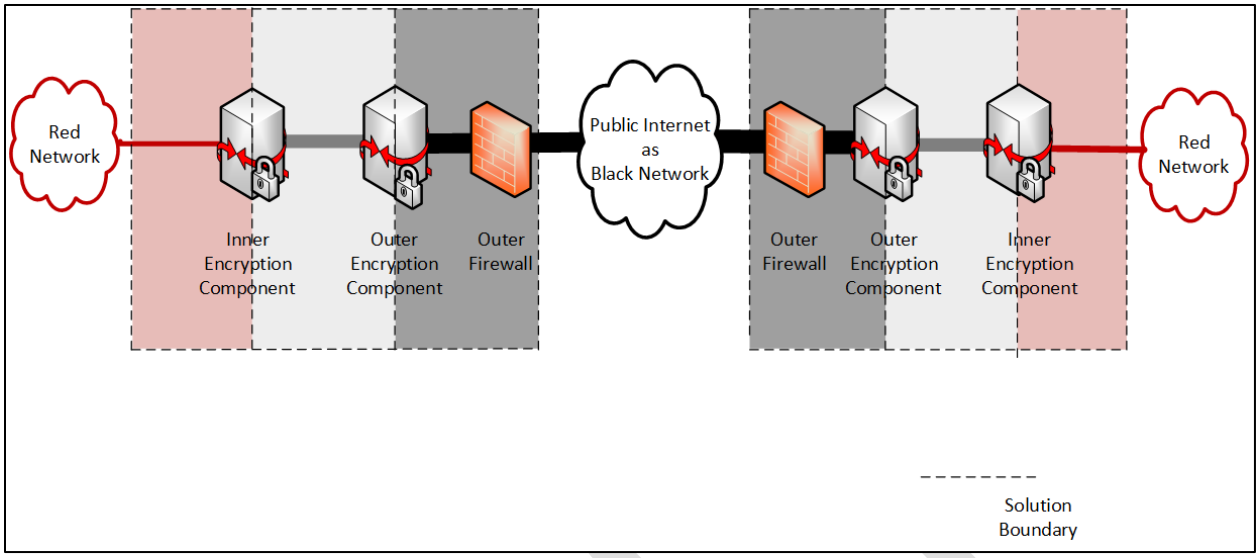


**Figure 2. MSC Solution Using the Public Internet as the Black Transport Network**

### 4.1.4 Data, Management and Control Plane Traffic

Data plane traffic is classified information, encrypted or unencrypted, that is passed 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 functions.

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

Data plane and management plane traffic 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. Unless otherwise specified given that some control plane traffic is necessary for a network to function, there is no general requirement that control plane traffic be similarly separated.

## 4.2 HIGH LEVEL DESIGN

Depending on the needs of the customer implementing the solution, the MSC Solution is adaptable to support capabilities for multiple sites and/or multiple security levels. If a customer does not have a need to support multiple sites or multiple security levels, then those elements need not be included as part of the implementation. As explained in Section 9, any implementation of the MSC Solution must satisfy all of the applicable requirements specified in this CP.

### 4.2.1 MULTIPLE SITES

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

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

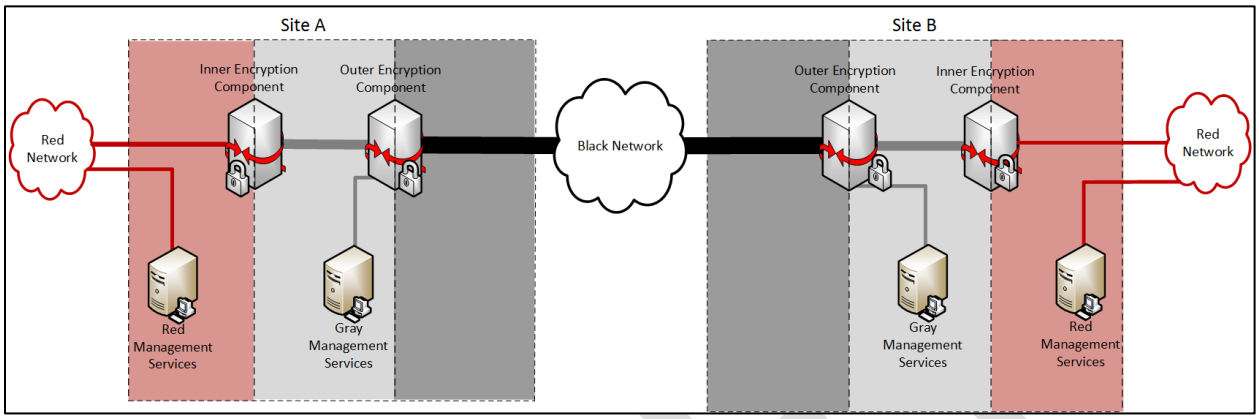


**Figure 3. MSC Solution Connecting Two Independently Managed Sites**

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

#### 4.2.1.1 Independently Managed Sites

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 to use either locally-run CAs that they manage and control or, where available, enterprise CAs that are not necessarily managed by the Solution Owner. Each site needs to ensure that the Encryption Components selected interoperate with those at the other sites.

Since there is no remote management, management traffic will not cross the Black Network, encrypted or unencrypted. 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 shows only two sites, this solution can scale to include numerous sites, with each additional site having the same design as those in the Figure 3.

#### 4.2.1.2 Centrally Managed Sites

As shown in Figure 4, if remote management is used, personnel at a single geographic site administer and perform keying for all the sites included in the solution. In this case, because the administration is done by one group of Security Administrators, CA Administrators, and Key Generation Solution Administrators (see Section 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 used on either or both layers and EAP-TLS is used for authentication then CAs are required. Otherwise, if PSK is used for authentication, CAs are not required.

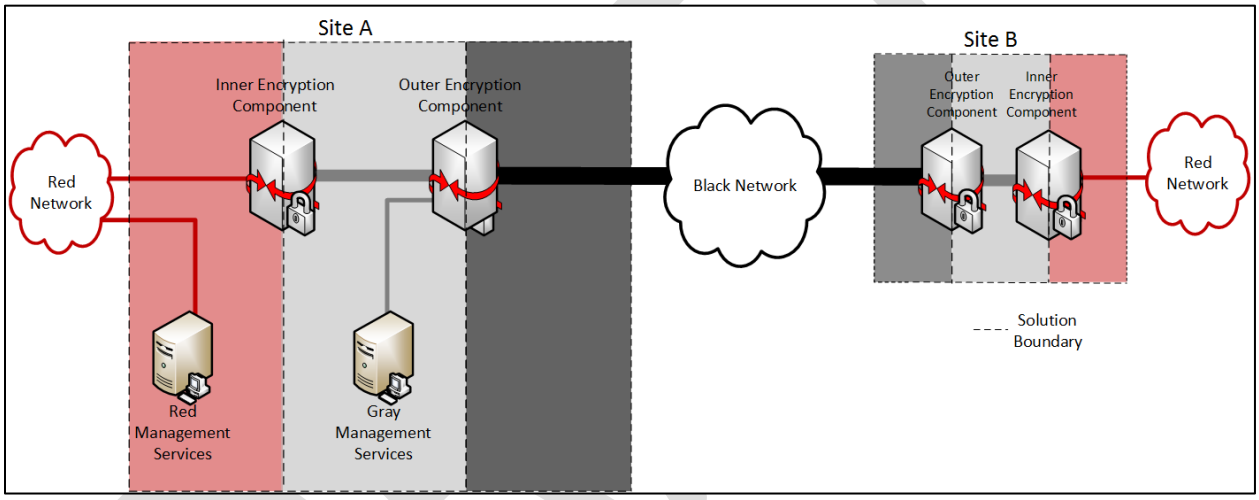


**Figure 4. MSC Solution Connecting a Central Management Site and a Remote Site**

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.

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

### 4.2.2 Multiple Security Levels

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

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

MSC Solutions supporting multiple security levels may include independently managed sites (see Section 4.2.1.1) or centrally managed sites (see Section 4.2.1.2). Given both cases, separate CAs, CAKs, and management devices are needed to manage the Inner Encryption Components at each security level. For example, Figure 5 shows a Central Management Site 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 shows an MSC Solution between two sites that carries traffic between two Red Networks; a Secret U.S.-only Network (Network 1), and a Secret U.S.-only Network (Network 2). Because Network 1 and Network 2 both operate at the same security level, their singly-encrypted traffic can be carried over the Gray Network without any additional security controls in place.

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

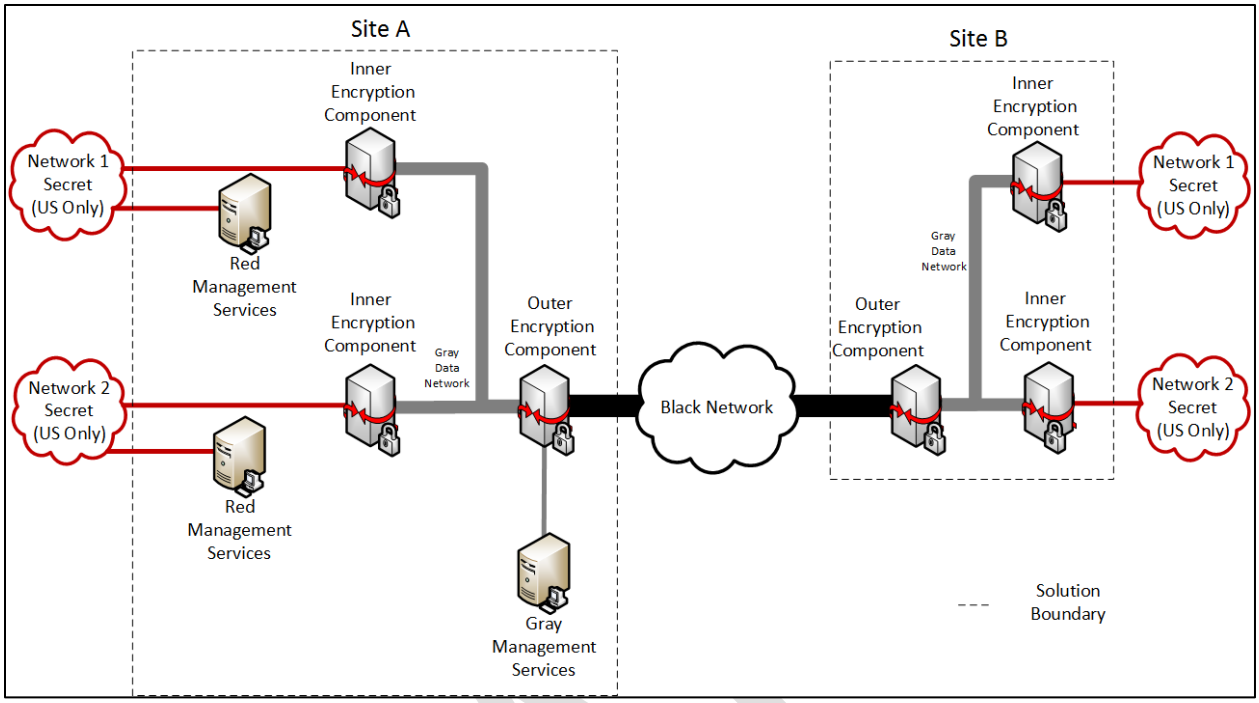


**Figure 5. MSC Solution for Two Networks at the Same Security Level**

#### 4.2.2.2 Networks Operating at Different Security Levels

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

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

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

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

Additionally, filtering components are included between the components used for management of the Gray Networks themselves (namely, Administration Management Workstation (MWs) 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, MWs 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.

As shown in Figure 6, one or more Gray Firewalls must be included in the Gray Network to perform filtering. Standalone Gray Firewalls have been placed at each site between the Inner Encryption Components and the Outer Encryption Component; these Gray Firewalls are responsible for dropping packets between Inner Encryption Components of different security levels.

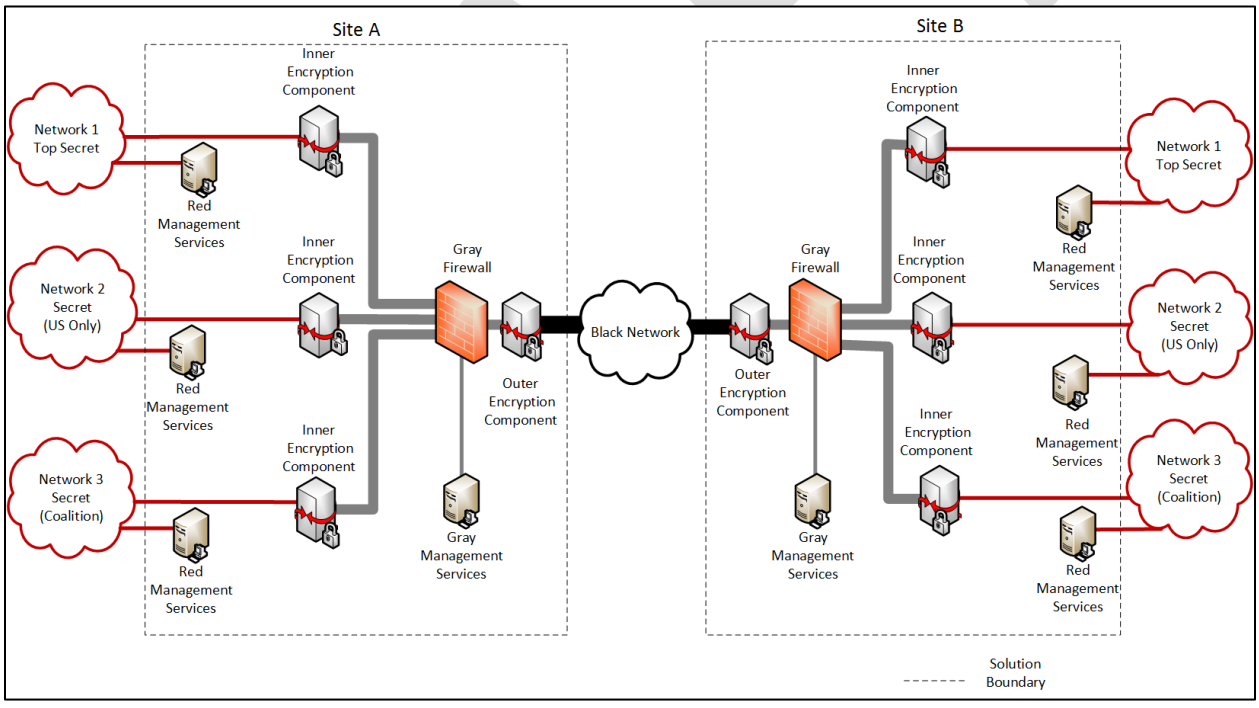


**Figure 6. MSC Solution for Networks at Different Security Levels**

Figure 6 also shows there is flexibility in the specific placement of Gray Firewalls, as long as any path between Inner Encryption Components for networks of different security levels includes a Gray Firewall.

Including one or more standalone Gray Firewalls in a solution does not remove the requirement to perform the filtering on the Outer Encryption Component as well. Outer Encryption Components are

uniquely positioned to block traffic between Inner Encryption Components supporting Red Networks of different security levels when one of those Inner Encryption Components is located at a different site.

### 4.2.3 LAYERING OPTIONS

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

**Table 1. Layering Options**

| Configuration | Inner 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. Encapsulation ensures the MACsec-encrypted traffic is not decrypted prior to reaching its destination and ensures the second layer of encryption can be applied.

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

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

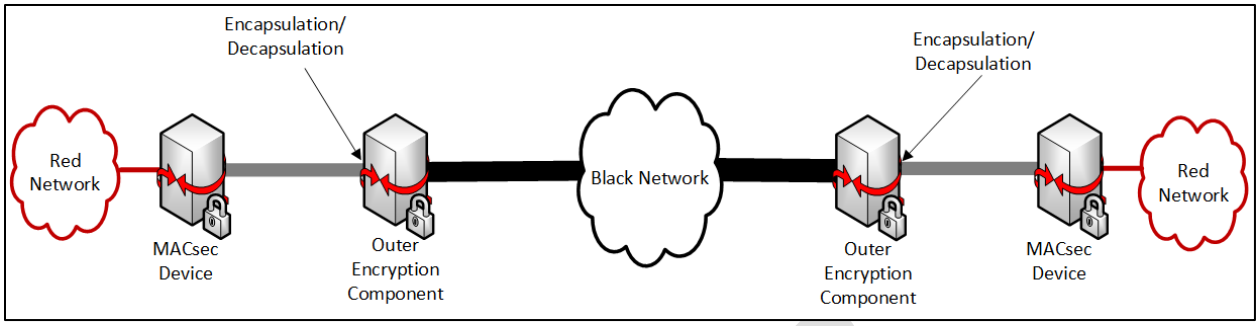


**Figure 7. Encapsulating MACsec on an Internal Interface**

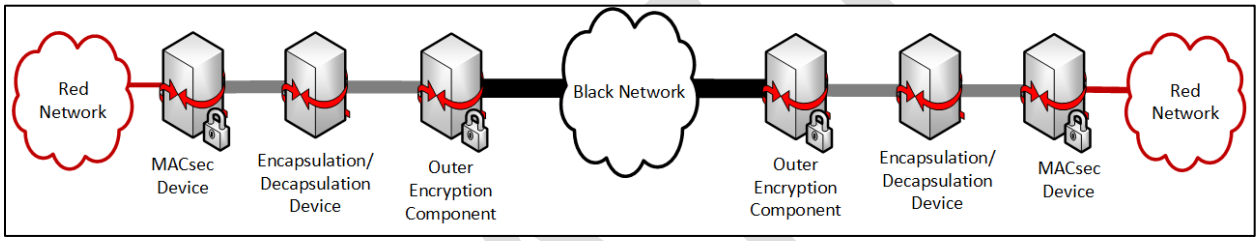


**Figure 8. Encapsulating MACsec with a Separate Device**

There are some scenarios where the MACsec-encrypted traffic needs additional encapsulation before it is passed through the Outer Encryption Component to the Black Network. In these scenarios, this additional step falls outside the boundary of the MSC Solution. However, it is highly recommended to apply the general device management (DM) and port filtering requirements for Solution Components.

In the current MACsec standard, the entire frame is encrypted with the exception of the source and destination addresses. Institute of Electrical and Electronics Engineers (IEEE) 802.1Aecg-2017 provides the option of moving the Virtual Local Area Network (VLAN) identification (ID) tag out of the encrypted payload and into the clear in the header. The benefits of moving the VLAN ID tag into the clear include service multiplexing (i.e., multiple point-to-point or multipoint services existing on a single physical interface) and providing quality of service across a Service Provider's network. If supported in the MACsec Device, this CP allows VLAN ID tags to be used in the clear.

At high speeds, 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. If supported in the MACsec Device, this CP allows the XPN feature to be used.

### 4.2.4 AUTHENTICATION

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

VPN Gateways authenticate via public key certificates. This CP requires all authentication certificates issued to VPN Gateways to be Non-Person Entity 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 to provide confidentiality and integrity for the MACsec tunnel.

## 4.3 OTHER PROTOCOLS

Throughout this CP, 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 CP, if no protocols or standards are specified then any appropriate protocols may be used to achieve the objective.

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

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

## 4.4 AVAILABILITY

The high-level designs described in Section 4.2 are not designed with the intent of automatically providing high availability. Supporting solution implementations where high availability is important is not a goal of this version of the CP. However, this CP does not prohibit adding redundant components in

parallel to allow for component failover or to increase the throughput of the MSC Solution, as long as each redundant component adheres to the requirements of this CP.

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

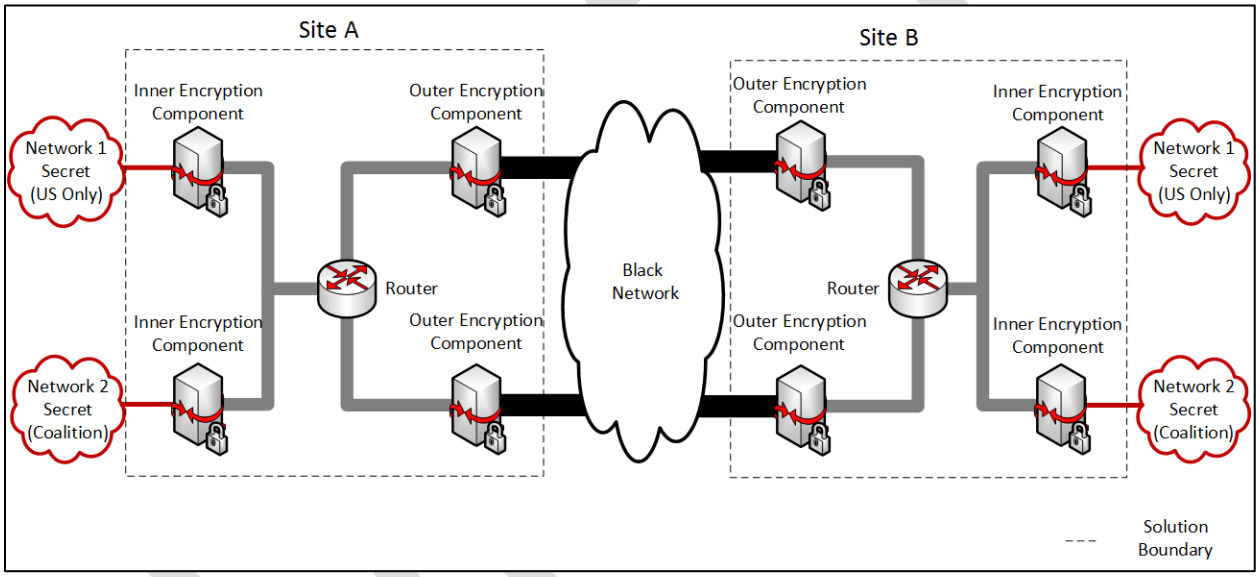


**Figure 9. MSC Solution with Redundant Outer Encryption Components**

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

# 5 SOLUTION COMPONENTS

In the high-level designs discussed in section 4.2, all communications flowing across a Black Network are protected by at least two layers of encryption, implemented using IPsec tunnels generated by VPN Gateways or MACsec tunnels generated by MACsec Devices. Mandatory aspects of the solution also

include MWs, 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).

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

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

## 5.1 Outer Firewall

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

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

The internal interface of the Outer Firewall only permits IPsec or MACsec traffic with a source address of the Outer Encryption Component and any necessary control plane traffic. The minimum requirements for port filtering on the Outer Firewall can be found in Section 11.6.

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

## 5.2 Outer Encryption Component

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

If the Black Network is the Public Internet, the external interface of the Outer Encryption Component is connected to the internal interface of the Outer Firewall. Otherwise, the external interface of the Outer

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

The Outer Encryption Component may be a perimeter device (if the Outer Firewall is not present) and more exposed to external attacks. The Outer Encryption Component may use internal filtering to help protect the network from unauthenticated traffic. This allows specification of rules that prohibit unauthorized data flows, which helps mitigate Denial of Service attacks and resource exhaustion. This CP does not require that the Outer Encryption Component terminate all tunnels on a single physical interface; however, all such external interfaces must conform to the port filtering requirements in Section 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 on an Outer Firewall or Gray Firewall to provide dynamic routing functionality. The Outer Encryption Component, selected from the CSfC Components List, must be physically separate from the Outer Firewall and Gray Firewall.

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

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

## 5.3 GRAY FIREWALL

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

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

## 5.4 GRAY MANAGEMENT SERVICES

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

### 5.4.1 GRAY MANAGEMENT WORKSTATION (MW)

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

### 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 using an approved CDS, as described in the *CSfC Continuous Monitoring Annex.*

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

## 5.5 INNER ENCRYPTION COMPONENTS

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

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

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

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

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

## 5.6 Inner Firewall

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

## 5.7 Red Management Services

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

### 5.7.1 Red Administration Management Components

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

### 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 mandatory components 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. As described in the *CSfC Continuous Monitoring Annex*, a Red SIEM may also be used to analyze log data from Gray Network components when used in conjunction with an approved CDS.

## 5.8 Key and Certificate Management Components

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

# 6 CONFIGURATION AND MANAGEMENT

This CP includes design details for the provisioning and management of Solution Components that require 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. The following sections describe the design in detail and Section 11.8 states specific configuration requirements that must be met to comply with this CP.

## 6.1 Component Provisioning

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

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 (e.g., Root CA certificate). The Security Administrator may also install an initial CRL.

## 6.2 ADMINISTRATION OF COMPONENTS

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

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

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

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

Management traffic for all MSC Solution Components is always encrypted to protect confidentially and integrity, except in the case where components are locally managed through a direct physical connection (e.g., serial cable from a Gray MW to the Outer Encryption Component). Management traffic must be encrypted with SSHv2, TLS 1.2 or later, IPsec or MACsec. When components are managed over the Black Network, a CSfC Solution must be implemented to provide two layers of approved encryption. This requirement is not applicable if the MSC Solution Components are managed from the same LAN or VLAN. For example, a Gray 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 (CM) allows customers to detect, react to, and report any attacks against their solution. CM also enables the detection of 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, should have an Auditor review alerts, events, and logs on a much more frequent basis and in many cases may leverage Operations Centers to perform CM of the solution.

## 7.1 MONITORING POINTS

The MSC CP requires CM of all network traffic and system log data from the components within the solution infrastructure. This monitoring allows customers to detect, react to, and report any attacks against their solution. CM also enables the detection of any configuration errors within solution infrastructure components.

Figure 10 shows the monitoring points in the *CSfC Continuous Monitoring Annex*. CM requirements have been relocated to the *CSfC Continuous Monitoring Annex*.

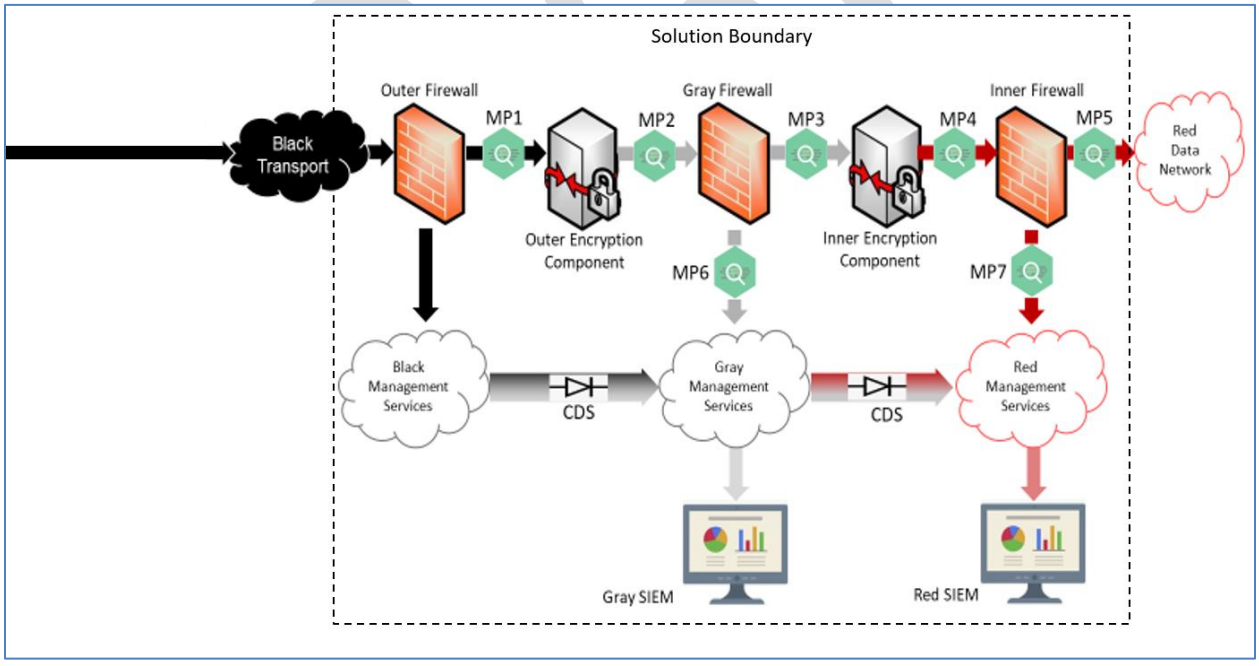


**Figure 10. MSC Solution Continuous Monitoring**

# 8 KEY MANAGEMENT

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

# 9 REQUIREMENTS OVERVIEW

Sections 10 through Section 14, and the *CSfC Key Management Requirements Annex*, specify requirements for implementations of MSC Solutions compliant with this CP. KM Requirements have been relocated to a separate *CSfC Key Management Requirements Annex*.

## 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.

## 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., "PS"), and a sequence number (e.g., 11). Table 2 lists the

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

777 **Table 2. Requirement Digraphs**

| Digraph | Description | Section | Table |
|---|---|---|---|
| PS | Product Selection Requirements | Section 10 | Table 3 |
| SR | Overall Solution Requirements | Section 11.1 | Table 4 |
| VG | VPN Gateway Requirements | Section 11.2 | Tables 5 & 6 |
| MD | MACsec Device Requirements | Section 11.3 | Table 7 & 8 |
| IR | Additional Requirements for Inner Encryption Components | Section 11.4 | Table 9 |
| OR | Additional Requirements for Outer Encryption Components | Section 11.5 | Table 10 |
| PF | Port Filtering Requirements for Solution Components | Section 11.6 | Table 11 |
| CM | Configuration Change Detection Requirements (see *CSfC Continuous Monitoring Annex*) | | |
| DM | Device Management Requirements | Section 11.8 | Table 12**Error! Reference source not found.** |
| MR | Continuous Monitoring Requirements (see *CSfC Continuous Monitoring Annex*) | | |
| AU | Auditing Requirements (see *CSfC Continuous Monitoring Annex*) | | |
| GD | Requirements for the Use and Handling of Solutions | Section 12.1 | Table 13 |
| RP | Incident Reporting Requirements | Section 12.2 | Table 14 |
| RB | Role-Based Personnel Requirements | Section 13 | Table 15 |
| TR | Testing Requirements | Section 14.1 | Table 16 |
| KM | Key Management Requirements (See *CSfC Key Management Requirements Annex*) | | |

778 # 10 REQUIREMENTS FOR SELECTING COMPONENTS

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

784 The CSfC Components List, contains the approved products for use in this solution. No single
785 commercial product must be used to protect classified information. The only approved method for
786 using COTS products to protect classified information in transit is through an approved CP.

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

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

794 **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-2 | The products used for any MACsec Device must be chosen from the list of MACsec Ethernet Encryptors on the CSfC Components List. | T=O | |
| MSC-PS-3 | The products used for any Firewalls must be chosen from the list of Traffic Filtering Firewalls on the CSfC Components List. | T=O | |
| MSC-PS-4 | The products used for any CA 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-7 | The Inner Encryption Component and the Outer Encryption Component must not use the same Operating System. Differences between Service Packs and version numbers for a particular vendor's OS do not provide adequate diversity. | T=O | |
| MSC-PS-8 | The cryptographic libraries used by the Inner Encryption Component and Outer Encryption Component must either; come from different manufacturers, where neither manufacturer is a subsidiary of the other; or be different libraries from | O | None |

| Req. # | Requirement Description | Threshold/ Objective | Alternative |
|---|---|---|---|
| | the same manufacturer, where NSA has determined that the libraries meet the CSfC criteria for implementation independence. | | |
| MSC-PS-9 | If the solution contains an Inner CA and an Outer CA, the cryptographic libraries must either; come from different manufacturers, where neither manufacturer is a subsidiary of the other; or be different libraries from the same manufacturer, where NSA has determined that the libraries meet the CSfC criteria for implementation independence. | O | None |
| MSC-PS-10 | If Gray Firewalls are used, the Gray Firewalls and Inner Encryption Components must either; come from different manufacturers, where neither manufacturer is a subsidiary of the other; or be two different products from the same manufacturer, where NSA has determined that the two products meet the CSfC criteria for implementation independence. | T=O | |
| MSC-PS-11 | The Inner Encryption Component and Outer Encryption Component must use physically separate components, such that no component is used for more than one function. | T=O | |
| MSC-PS-12 | If an Outer Firewall and/or Gray Firewall is required, the Outer Firewall, Outer Encryption Component, Gray Firewall and Inner Encryption Component must use physically separate components, such that no component is used for more than one function. | T=O | |
| MSC-PS-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:<br>• The CAs come from different manufacturers, where neither manufacturer is a subsidiary of the other.<br>• The CAs are different products from the same manufacturer, where the NSA has determined that the products meet the CSfC criteria for implementation independence.<br>• The CAs use an Enterprise PKI approved by the AO. | O | None |
| MSC-PS-15 | Each component selected from the CSfC Components List must go through a Product Supply Chain Threat Assessment to determine the | T=O | |

| Req. # | Requirement Description | Threshold/ Objective | Alternative |
|---|---|---|---|
| | 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). | | |
| MSC-PS-16 | MSC Solution Components must be configured to use the NIAP-certified evaluated configuration. | T=O | |

# 11 CONFIGURATION REQUIREMENTS

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

## 11.1 OVERALL SOLUTION REQUIREMENTS

Table 4 defines 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 Encryption Components selected by each site for each tunnel are interoperable. | T=O | |
| MSC-SR-3 | The time of day on the Inner Encryption Component and Red Management Services must be synchronized to a 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 | T=O | |

| Req. # | Requirement Description | Threshold/ Objective | Alternative |
|---|---|---|---|
| | between the requirements in this CP and local policy, this CP takes precedence. | | |
| 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 CRL Distribution Point (CDP)/OCSP Responder and an Inner Encryption Component for Red Networks of different security levels must include a Gray Firewall. | T=O | |
| MSC-SR-9 | Gray Network components must be physically protected to the level of the highest classified network. | T=O | |
| MSC-SR-10 | The Outer Encryption Component must use a unique physical internal interface for each Red Network in the MSC Solution (i.e., VLAN trunking of multiple enclaves is not permitted). | T=O | |
| MSC-SR-11 | A Gray Firewall 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, the Inner Firewall requirements from that CP must be followed. | T=O | |
| MSC-SR-14 | The only approved physical paths leaving the Red Network must be through 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 | |

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

| Req. # | Requirement Description | Threshold/ Objective | Alternative |
|---|---|---|---|
| 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 on boot). | T=O | |

## 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<br>IETF RFC 6379<br>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<br>IETF RFC 4754<br>IETF RFC 6380<br>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<br>IETF RFC 3526<br>IETF RFC 5903<br>IETF RFC 6379<br>IETF RFC 6380<br>IETF RFC 7296 |
| Integrity (Hashing) | SHA-384 | FIPS PUB 180-4<br>IETF RFC 6379<br>IETF RFC 6380 |

808 **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 and the Encapsulating Security Payload (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 | |
| 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 for integrity. | T | MSC-VG-12 |
| MSC-VG-12 | All VPN Gateways must use Galois Counter Mode for ESP encryption. | O | MSC-VG-11 |
| MSC-VG-13 | All VPN Gateways must set the IKE SA lifetime to at most 24 hours. | T=O | |
| MSC-VG-14 | All VPN Gateways must set the ESP SA lifetime to no more than 8 hours. | T=O | |

| Req. # | Requirement Description | Threshold / Objective | Alternative |
|---|---|---|---|
| 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 |
| MSC-VS-18 | All VPN Gateways must use IKEv2 (IETF RFC 7296) key exchange with Pre-Shared Keys (PSK) | O | |

## 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<br>GCM-AES-XPN-256 | FIPS PUB 197<br>IEEE 802.1AEbn-2011<br>IEEE 802.1AEbw-2013 |
| 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 size of 256 bits. | T=O | |
| MSC-MD-3 | MACsec Devices must authenticate using Pre-Shared Keys (PSKs), known as Connectivity Association Keys (CAKs). | T | MSC-MD-14 |
| MSC-MD-4 | Requirement has been relocated to the *CSfC Key Management Requirements Annex*. | 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 | |

| Req. # | Requirement Description | Threshold / Objective | Alternative |
|---|---|---|---|
| MSC-MD-6 | For each pair of MACsec Devices establishing an encryption tunnel, one of the two must be configured to be the Key Server by setting its Key Server value to 0 (zero). The other MACsec Device must have its Key Server value set to 1. If a Central Management Site is part of the MSC Solution, it must be the Key Server. | T=O | |
| MSC-MD-7 | MACsec Devices must enable data delay protection for MACsec Key Agreement (MKA). | T=O | |
| MSC-MD-8 | MACsec Devices must have an MKA Lifetime Timeout limit set to 6.0 seconds and Hello Timeout limit set to 2.0 seconds. | T=O | |
| MSC-MD-9 | MACsec Devices must have the replay window set to 2 or as low as possible given the nature of the Black Network being traversed. | T=O | |
| MSC-MD-10 | MACsec Devices must require all data traffic on an external facing port to be encrypted (e.g., must-secure). | T=O | |
| MSC-MD-11 | MACsec Device configuration files, whether printed or electronically copied, must be physically protected to the highest classification of the MACsec Device's CAK. | T=O | |
| MSC-MD-12 | MACsec Devices must have the Confidentiality Offset set to 0 (zero). | T=O | |
| MSC-MD-13 | If a standalone device is required to provide encapsulation of MACsec traffic between an Inner MACsec Device and an Outer Encryption Component, the standalone device must be considered a Solution Component when satisfying requirements in Section 11.1. | T=O | |
| MSC-MD-14 | MACsec Devices must authenticate using EAP-TLS (certificate based). | O | MSC-MD-3 |

## 11.4 ADDITIONAL INNER ENCRYPTION COMPONENT REQUIREMENTS

Table 9 defines additional Inner Encryption Component Requirements.

**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, with an associated IP tunneling protocol. | T=O | |

| Req. # | Requirement Description | Threshold / Objective | Alternative |
|---|---|---|---|
| MSC-IR-2 | Packet sizes, or frames leaving the external interface of the Inner Encryption Component must be configured to reduce fragmentation and lessen the impact on performance. This requires proper 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 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 aMandatory Access Control policy to not allow packets received on an interface connected to a Red Network to bypass encryption and be forwarded out through an interface connected to a Gray Network. | O | MSC-IR-3 |
| MSC-IR-5 | The Inner Encryption Component must not allow packets received on an interface connected to a Gray Network to bypass decryption and be forwarded out through an interface connected to a Red Network. | T | MSC-IR-6 |
| MSC-IR-6 | The Inner Encryption Component must use Mandatory Access Control policy to not allow packets received on an interface connected to a Gray Network to bypass decryption and be forwarded out through an interface connected to a Red Network. | O | MSC-IR-5 |
| MSC-IR-7 | The Inner Encryption Component must not permit split-tunneling. | T=O | |

## 11.5 ADDITIONAL REQUIREMENTS FOR OUTER ENCRYPTION COMPONENTS

Table 10 defines additional Outer Encryption Components Requirements.

**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 packets received on an interface connected to a | T | MSC-OR-3 |

| Req. # | Requirement Description | Threshold / Objective | Alternative |
|---|---|---|---|
| | Gray Network to bypass encryption and be forwarded out through an interface connected to a Black Network. | | |
| MSC-OR-3 | Outer Encryption Components must use Mandatory Access Control policy to not allow packets received on an interface connected to a Gray Network to 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

Table 11 defines Port Filtering Solution Components Requirements.

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

| Req. # | Requirement Description | Threshold/ Objective | Alternative |
|---|---|---|---|
| MSC-PF-1 | All Solution Components must have all network interfaces restricted to the smallest address ranges, ports, and protocols possible. | T=O | |
| MSC-PF-2 | All Solution Components must have all unused network interfaces disabled. | T=O | |
| MSC-PF-3 | For all Outer VPN Gateway interfaces connected to a Black Network, traffic filtering rules must be applied to both inbound and outbound traffic, such that only IKE, ESP, and control plane protocols (as defined in this CP) approved by organization-defined policy are allowed. | T=O | |

| Req. # | Requirement Description | Threshold/ Objective | Alternative |
|---|---|---|---|
| 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 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 a Gray MW with the exception of logging or authentication traffic that may be initiated from Outer Encryption Components. | T=O | |
| MSC-PF-9 | Multicast messages received on external interfaces of Outer Encryption Components must be dropped. | T=O | |
| MSC-PF-10 | For solutions using IPv4, Outer VPN Gateways using IPsec must drop all packets that use IP options. | O | |
| MSC-PF-11 | For solutions using IPv4, each VPN Gateway must only accept packets with Transmission Control Protocol (TCP), User Datagram Protocol (UDP), ESP, or ICMP in the IPv4 Protocol field and drop all other packets. | T=O | |
| MSC-PF-12 | For solutions using IPv6, each VPN Gateway must only accept packets with ESP, TCP, UDP, or ICMPv6 in the IPv6 Next Header field and drop all other packets. | T=O | |
| MSC-PF-13 | The Gray Network interfaces of Outer Encryption Components must allow IKE and IPsec, or MKA and MACsec traffic, as appropriate, between two Inner Encryption Components protecting networks of the | T=O | |

| Req. # | Requirement Description | Threshold/ Objective | Alternative |
|---|---|---|---|
| | same security level or that is being used for management of the Gray Network. | | |
| MSC-PF-14 | *Withdrawn* | | |
| MSC-PF-15 | The Gray Network interfaces of Outer VPN Gateways must allow HTTP traffic that is necessary to perform CRL checking for the Inner encryption layer (i.e., requests/replies between the Inner VPN Gateways and the CDPs/OCSP Responders) and block all other HTTP traffic. Refer to IETF RFC 5280 and IETF RFC 6960 for further details on this type of traffic. | T=0 | |
| MSC-PF-16 | *Withdrawn* | | |
| MSC-PF-17 | The Gray Network interfaces of Outer Encryption Components must only permit packets whose source and destination IP addresses match the external interfaces of Inner Encryption Components that support Red Networks of the same security level. | T=O | |
| MSC-PF-18 | The Gray Network interfaces of Outer Encryption Components must block all packets whose source address does not match a list of addresses or address ranges known to be reachable from the interface where the packet was received. | T=O | |
| MSC-PF-19 | The Gray Network interfaces of Outer Encryption Components must allow management and control plane protocols (as defined in this CP) that have been approved by policy. | T=O | |
| MSC-PF-20 | The Gray Network interfaces of Outer Encryption Components must deny all traffic that is not explicitly allowed by requirements MSC-PF-8, MSC-PF- 13, MSC-PF-14, MSC-PF-15, 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. | 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 (i.e., networks of multiple protection levels are included in the solution) the Gray Firewall must allow appropriate | T=O | |

| Req. # | Requirement Description | Threshold/ Objective | Alternative |
|---|---|---|---|
| | traffic (IKE, IPsec, MKA and MACsec) between Red Networks operating at the same security level. | | |
| 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 |
| MSC-PF-25 | If a Gray Firewall is required, the Gray Firewall must allow HTTP traffic that is necessary to perform CRL checking for the Inner encryption layer (i.e., requests/replies between the Inner VPN Gateways and CDPs/OCSP Responders) and block all other HTTP traffic. Refer to IETF RFC 5280 and IETF RFD 6960 for further details on this type of traffic. | O | MSC-PF-24 |
| MSC-PF-26 | *Withdrawn* | | |
| MSC-PF-27 | If a Gray Firewall is required, the Gray Firewall must only accept management traffic on the physical ports connected to the Gray Management Network. | T=O | |
| MSC-PF-28 | If a Gray Firewall is required, the Gray Firewall must only permit packets whose source and destination IP addresses match the external interfaces of Inner Encryption Components that support Red Networks of the same security level. | T=O | |
| MSC-PF-29 | If a Gray Firewall is required, the Gray Firewall must block all packets whose source address does not match a list of addresses or address ranges known to be reachable from the interface where the packet was received. | T=O | |
| MSC-PF-30 | If a Gray Firewall is required, the Gray Firewall must allow control plane traffic (e.g., NTP, 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-27 or MSC-PF-30. | T=O | |

## 11.7 CONFIGURATION CHANGE DETECTION REQUIREMENTS

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

## 11.8 DEVICE MANAGEMENT REQUIREMENTS

Table 12 defines Device Management Requirements.

**Table 12. Device Management (DM) Requirements**

| Req. # | Requirement Description | Threshold / Objective | Alternative |
|---|---|---|---|
| MSC-DM-1 | If using physical Administration Workstations, they must be dedicated for the purposes given in this CP and must be physically separated from workstations used to manage non-CSfC solutions. | T=O | |
| MSC-DM-2 | Administration Workstations (or hosts/servers hosting VMs serving as MWs) must physically reside within a protected facility where CSfC solution(s) are managed. | T=O | |
| MSC-DM-3 | MWs 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 MWremotely 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. | 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 | MWs that interact with the Certificate Authority for the Outer VPN Gateways must be located on the Gray Network. | T=O | |
| MSC-DM-15 | Requirement has been relocated to the *CSfC Key Management Requirements Annex*. | | |
| MSC-DM-16 | Requirement has been relocated to the *CSfC Key Management Requirements Annex*. | | |
| MSC-DM-17 | The same MWmust not be used to manage Inner Encryption Components and Outer Encryption Components. | T=O | |
| MSC-DM-18 | Requirement has been relocated to the *CSfC Continuous Monitoring Annex.* | | |
| MSC-DM-19 | Requirement has been relocated to the *CSfC Continuous Monitoring Annex.* | | |
| MSC-DM-20 | Requirement has been relocated to the *CSfC Continuous Monitoring Annex.* | | None |
| MSC-DM-21 | Requirement has been relocated to the *CSfC Continuous Monitoring Annex.* | | 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 | |
| MSC-DM-23 | Hosts/servers for management VMs may not host VMs that perform non-CSfC functions | T=O | |
| MSC-DM-24 | VMs that perform management services may not also perform other functions within the solution (i.e., provisioning, enrollment, CA registration, SIEM, etc. must be performed by separate workstations or VMs). | T=O | |
| MSC-DM-25 | Management workstations (physical or virtual) must be configured, patched, and operated in accordance | T=O | |

| Req. # | Requirement Description | Threshold / Objective | Alternative |
|---|---|---|---|
| | with applicable Operating System vendor hardening guide and the organizational or local policy. | | |
| MSC-DM-26 | Management workstations must be powered off when not in use. | T=O | |
| MSC-DM-27 | The Management workstation must not also be used for provisioning, certificate registrations, and SIEM services. | T=O | |
| MSC-DM-28 | Each MW admin must have a unique login credential. Group accounts are prohibited. | T=O | |

### 11.9 CONTINUOUS MONITORING REQUIREMENTS

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

### 11.10 AUDITING REQUIREMENTS

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

### 11.11 KEY MANAGEMENT REQUIREMENTS

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

## 12 SOLUTION OPERATIONS, MAINTENANCE, AND HANDLING REQUIREMENTS

### 12.1 USE AND HANDLING OF SOLUTIONS REQUIREMENTS

Table 13 defines the Use and Handling of the Solution Requirements.

**Table 13. Use and Handling of Solutions Requirements**

| Req. # | Requirement Description | Threshold / Objective | Alternative |
|---|---|---|---|
| MSC-GD-1 | All Solution Components, with the exception of the Outer Firewall (if present), must be physically protected as classified devices, classified at the level of the network with the highest classification in the solution or in any other MSC Solutions with which it is interconnected. | T=O | |
| MSC-GD-2 | Only authorized and appropriately cleared (or escorted) administrators and security personnel must have physical access to the Solution Components. | T=O | |

| Req. # | Requirement Description | Threshold / Objective | Alternative |
|---|---|---|---|
| MSC-GD-3 | All components of the solution must be disposed of as classified devices, unless declassified using AO-approved procedures. | T=O | |
| MSC-GD-4 | Acquisition and procurement documentation must not include information concerning the purpose of the equipment, to include that it will be used to protect classified information. | T=O | |
| MSC-GD-5 | The Solution Owner must allow, and fully cooperate with, the NSA or its authorized agent to perform an Information Assurance (IA) compliance audit (including, but not limited to, inspection, testing, observation, and interviewing) of the solution implementation to ensure it meets the latest version of this CP. | T=O | |
| MSC-GD-6 | 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 the NSA and receive approval prior to operating the solution. | T=O | |
| MSC-GD-9 | The implementing organization must complete and submit an MSC CP requirements compliance matrix to their respective AO. | T=O | |
| MSC-GD-10 | Registration and re-registration against this CP must include submission of CP registration forms and compliance matrix to the NSA. | T=O | |
| MSC-GD-11 | When the NSA publishes a new approved MSC CP, the AO has six months to ensure their organization is in compliance with the new CP. | T=O | |
| MSC-GD-12 | Solution implementation information that was provided to the NSA during solution registration must be updated annually (in accordance with Section 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 | |
| MSC-GD-15 | Audit data must be off-loaded to a backup storage medium at least once a week. | T=O | |

| Req. # | Requirement Description | Threshold / Objective | Alternative |
|---|---|---|---|
| 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-22 | The implementing organization must test and subsequently apply security critical patches to all components in the solution in accordance with local policy and this CP. | T=O | |
| MSC-GD-23 | Local policy must dictate how the Security Administrator installs patches to Solution Components. | T=O | |
| MSC-GD-24 | Solution Components must comply with local TEMPEST policy. | T=O | |
| MSC-GD-25 | All hardware components must be tracked through an AO-approved inventory management process that identifies each component as part of a CSfC solution. | T=O | |
| MSC-GD-26 | A baseline configuration for all components must be maintained by the Security Administrator and be available to the Auditor. | T=O | |

## 12.2 INCIDENT REPORTING REQUIREMENTS

Table 14 lists incident reporting requirements for reporting security incidents to the NSA. These requirements will be followed in the event that a Solution Owner identifies a security incident that affects the solution. These reporting requirements are intended to augment, not replace incident reporting procedures already in use within the Solution Owner's organization. It is critical that Security

Administrators, Certification Authority Administrators (CAAs), Key Generation Solution Administrator (KGSAs), and Auditors are familiar with maintaining the solution in accordance with this CP. Familiarity with the known-good configuration of the solution will better equip personnel responsible for the operations and maintenance of the solution to identify reportable incidents.

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

Table 14 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 14. 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 or contacting the 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:<br>• CSfC Registration Number<br>• Primary POC name, phone, email<br>• Alternate POC name, phone, email<br>• Security level of affected solution<br>• Name of affected network(s)<br>• Affected component(s) manufacturer/ vendor<br>• Affected component(s) model number<br>• Affected component(s) version number<br>• Date and time of incident<br>• Description of incident<br>• Description of remediation activities<br>• Is Technical Support from the NSA requested? (Yes/No) | T=O | |
| MSC-RP-3 | Solution Owners must report a security failure in any of the CSfC Solution Components. | T=O | |
| MSC-RP-4 | Solution Owners must report any evidence of a compromise or spillage of classified data caused by a failure of the CSfC solution. | T=O | |
| MSC-RP-5 | For Gray Network interfaces, Solution Owners must report any malicious inbound and outbound traffic. | T=O | |

| Req. # | Requirement Description | Threshold/ Objective | Alternative |
|---|---|---|---|
| MSC-RP-6 | Solution Owners must report any evidence of an unauthorized device/user gaining access to the classified network via the solution. | T=O | |
| MSC-RP-7 | Solution Owners must report if a Solution Component sends traffic with an unauthorized destination address. | T=O | |
| MSC-RP-8 | Solution Owners must report any malicious configuration changes to the components. | T=O | |
| MSC-RP-9 | Solution Owners must report any unauthorized escalation of privileges to any of the CSfC Solution Components. | T=O | |
| MSC-RP-10 | Solution Owners must report if two or more simultaneous VPN connections from different IP addresses are established using the same device certificate. | T=O | |
| MSC-RP-11 | Solution Owners must report any evidence of malicious physical tampering with Solution Components. | T=O | |
| MSC-RP-12 | Solution Owners must report any evidence that one or both layers of the solution failed to protect the data. | T=O | |
| 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.

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

895 3) Document, test, and maintain the solution.

896 4) Respond to incidents affecting the solution.

897 Additional policies related to the personnel that perform these roles in a MSC Solution are identified in
898 Table 15.

899 **Table 15. 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 protected by the MSC Solution. When an Enterprise CA/KGS is used in the solution, the CAA/KGSA already in place may also support this solution, provided they meet this requirement. Black Network Administrators may be cleared at the Black Network security level. | T=O | |
| MSC-RB-2 | The Security Administrator, CAA, KGSA, and Auditor roles must be performed by different people. | T=O | |
| MSC-RB-3 | All Security Administrators, CAAs, KGSAs, and Auditors must meet local IA training requirements. | T=O | |
| MSC-RB-4 | The CAA(s) for the inner tunnel must be different individuals from the CAA(s) for the outer tunnel. | T=O | |
| MSC-RB-5 | The Security Administrator(s) for the Inner Encryption Components and supporting components on the Red Network must be different individuals from the Security Administrator(s) for the Outer Encryption Components and supporting components on the Gray Network. | T=O | |
| 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 Certification Practice Statement (CPS), or integration of the MSC Solution. | T=O | |

| Req. # | Requirement Description | Threshold/ Objective | Alternative |
|---|---|---|---|
| MSC-RB-10 | Auditing of the KGS operations must be performed by individuals who were not involved in the development of the Key Management Plan, 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 likely will be necessary for the customer to obtain approval from the system AO. The customer and AO have obligations to perform the following:

- The customer, possibly with support from an Integrator, instantiates a solution implementation that follows the NSA-approved CP.
- The customer'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 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 must ensure 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.
- The AO ensures that certificate and CAK revocation information is updated on all the Solution Components in the MSC Solution in the case of a compromise.
- 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 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 a MSC Solution. This T&E will be a critical part of the approval process for the AO, providing a robust body of evidence that shows compliance with this CP.

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

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

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

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

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

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

The test requirement in table 16 was developed to ensure that the MSC Solution functions properly and meets the configuration requirements in 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 16. Test (TR) Requirements**

| Req. # | Requirement Description | Threshold / Objective | Alternative |
|---|---|---|---|
| MSC-TR-1 | The organization implementing the CP must perform all tests listed in the *CSfC MSC CP Testing Annex*. | 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 is available on the SIPRNet CSfC website. The AO must be provided a copy of the NSA Risk Assessment for their consideration in approving the use of the solution.

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

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

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

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

1068 # 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 |

| Acronym | Meaning |
|---|---|
| IPS | Intrusion Prevention System |
| IPsec | Internet Protocol Security |
| IPv4 | Internet Protocol version 4 |
| IPv6 | Internet Protocol version 6 |
| KGS | Key Generation Solution |
| 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 |

1069

# 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-2017 | *IEEE Standard for Media Access Control (MAC) Security Amendment: Ethernet Data Encryption Devices, 2017* | June 2017 |
| 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 |


1071