National Security Agency/
Central Security Service

DIRECTORATE OF CAPABILITIES

MULTI-SITE CONNECTIVITY CAPABILITY PACKAGE V1.0

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 1.0
February 23, 2017

CHANGE HISTORY

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

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

1 INTRODUCTION

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

The NSA is delivering the CSfC Multi-Site Connectivity (MSC) CP to meet the demand for data in transit solutions using approved cryptographic algorithms and National Information Assurance Partnership (NIAP) evaluated components. These algorithms, known as the Commercial National Security Algorithm (CNSA) Suite, are used to protect classified data using layers of COTS products. MSC CP Version 1.0 enables customers to implement layered encryption between two or more sites. This CP takes lessons learned from multiple proof-of-concept demonstrations. These demonstrations included a layered use of COTS products for the protection of classified information.

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

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

2 PURPOSE AND USE

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

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

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

MSC Solutions shall 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 shall 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 THE MSC SOLUTION

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

The MSC Solution uses two nested, independent encryption tunnels to protect the confidentiality and integrity of data as it transits the untrusted network. The two encryption tunnels protecting a data flow can use either Internet Protocol Security (IPsec) generated by a Virtual Private Network (VPN) Gateway

or Media Access Control Security (MACsec) generated by a MACsec Device. VPN Gateways and MACsec Devices are implemented as part of the network infrastructure.

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

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

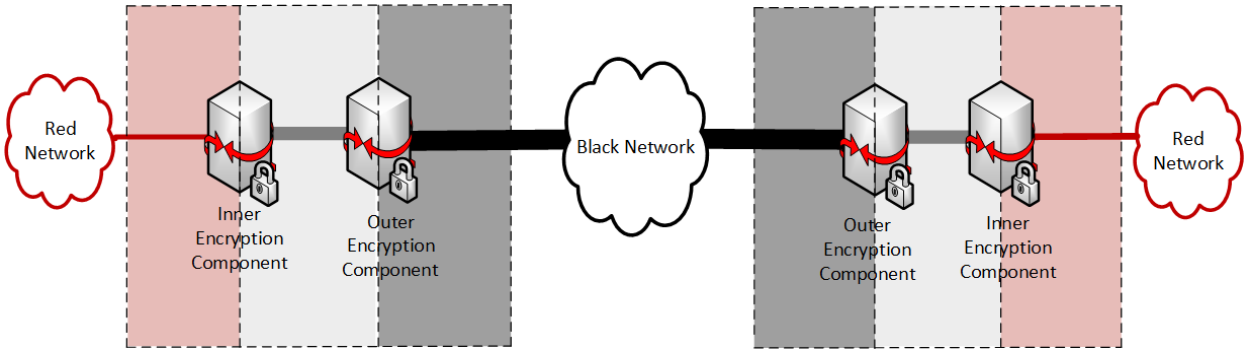

Figure 1. Two Encryption Tunnels Protect Data across an Untrusted Network

The MSC CP instantiations are built using products from the CSfC Components List (see Section 10). Customers who are concerned that their desired products are not yet on the CSfC Components List are encouraged to contact the appropriate vendors to encourage them to sign a Memorandum of Agreement (MoA) with NSA and commence evaluation against a NIAP-approved Protection Profile using the CSfC mandated selections that will enable them to be listed on the CSfC Components List. NIAP Certification alone does not guarantee inclusion on the CSfC Components List. Products listed on the CSfC Components List are not guaranteed to be interoperable with all other products on the CSfC Components List. Customers and Integrators should perform interoperability testing to ensure the components selected for their MSC Solution are interoperable. If you need assistance obtaining vendor Point of Contact (POC) information, please email csfc_components@nsa.gov.

4.1 NETWORKS

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

4.1.1 RED NETWORK

Red data consists of unencrypted classified data. The Red network is logically located behind an Inner Encryption Component. The networks connected to one another through the MSC Solution are Red networks. Red networks are under the control of the Solution Owner or a trusted third party. Red networks may only communicate with one another through the MSC Solution if the networks operate at the same security level.

4.1.2 GRAY NETWORK

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

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

Gray network components consist of the Outer Encryption Component, Gray Firewall, and Gray Management Services. All Gray network components are physically protected at the same level as the Red network components of the MSC Solution. Gray Management Services are physically connected to the Gray Firewall and include, at a minimum, an Administration Workstation. The Gray Management Services may also include a Security Information and Event Manager (SIEM) unless the SIEM is implemented in the Red network in conjunction with a cross domain solution (CDS) (see Section 7). This CP requires the management of Gray network components through the Gray Administration Workstation. As a result, neither Red nor Black Administration Workstations are permitted to manage the Outer Encryption Component, Gray Firewall, or Gray Management Services. Additionally, the Gray Administration Workstation is prohibited from managing Inner Encryption Components. Inner Encryption Components must be managed from a Red Administration Workstation.

4.1.3 BLACK NETWORK

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

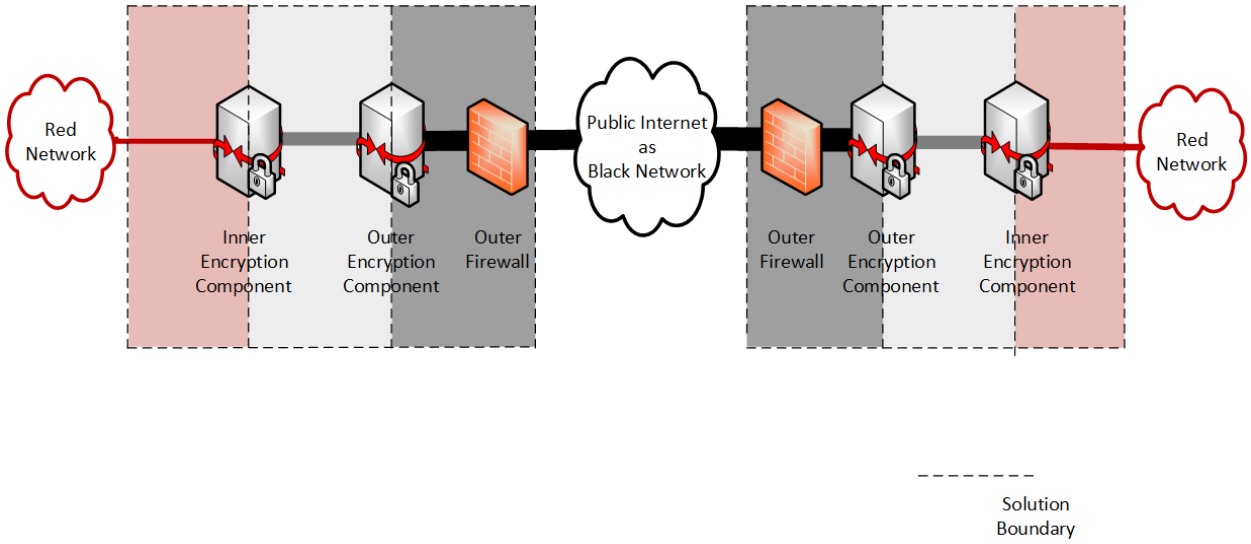

Figure 2. MSC Solution Using the Public Internet as the Black Transport Network

4.1.4 DATA, MANAGEMENT, AND CONTROL PLANE TRAFFIC

Data plane traffic is classified information, encrypted or not, that is being 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 (PTP))

- Route advertisement (e.g., Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), 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 (see Section 8.1.3) where, given their impact on the security of the solution, this CP does provide detailed requirements. Restrictions are also placed on control plane traffic for the Outer Encryption Component. The Outer Encryption Component is prohibited from implementing routing protocols on external and internal interfaces. The Outer Encryption Component may not perform routing functionality. If an Outer Firewall is present, the Outer Firewall can perform routing functionality.

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

Data plane and management plane traffic are required to be separated from one another by using physical or cryptographic separation. Use of a Virtual Local Area Network (VLAN) alone is not sufficient to separate data plane and management plane traffic. As a result, a solution may, for example, have a Gray data network and a Gray management network that are separate from one another, where the components on the Gray management network are used to manage the components on the Gray data network. Given that some control plane traffic is necessary for a network to function, there is no general requirement that control plane traffic be similarly separated, unless otherwise specified.

4.2 High-Level Design

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

4.2.1 Multiple Sites

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

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

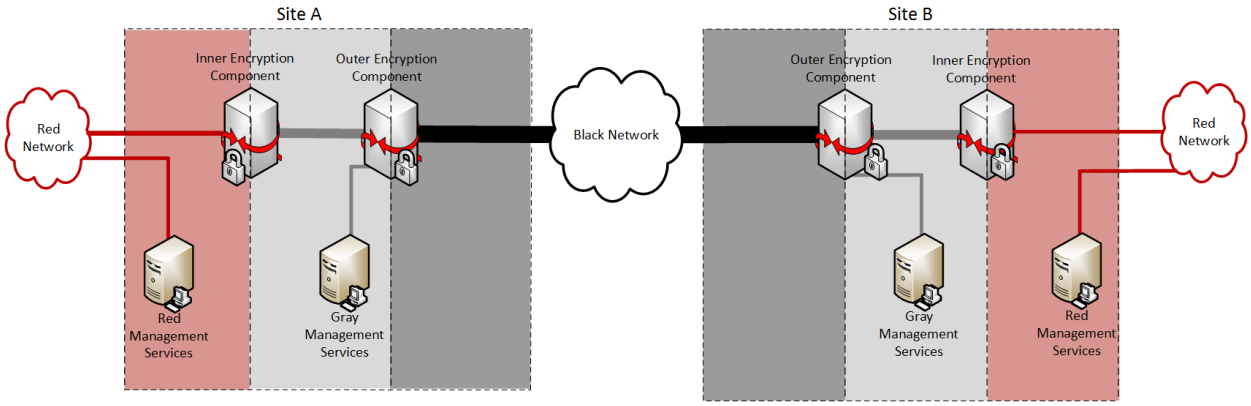

Figure 3. MSC Solution Connecting Two Independently Managed Sites

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

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

4.2.1.1 Independently Managed Sites

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

Since there is no remote management, no management traffic will cross the Black network, encrypted or otherwise. Any VPN Gateways at each site using public key certificates need to have the signing certificates and revocation information for the corresponding CAs used by the other sites in the MSC Solution. This high-level design requires cooperation between the various sites in the solution to ensure that all CAs used by each site are trusted at all the other sites. Similarly, MACsec Devices using a Connectivity Association Key (CAK) need to have the same CAK used by the other site in the MSC Solution.

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

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

4.2.1.2 Centrally Managed Sites

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

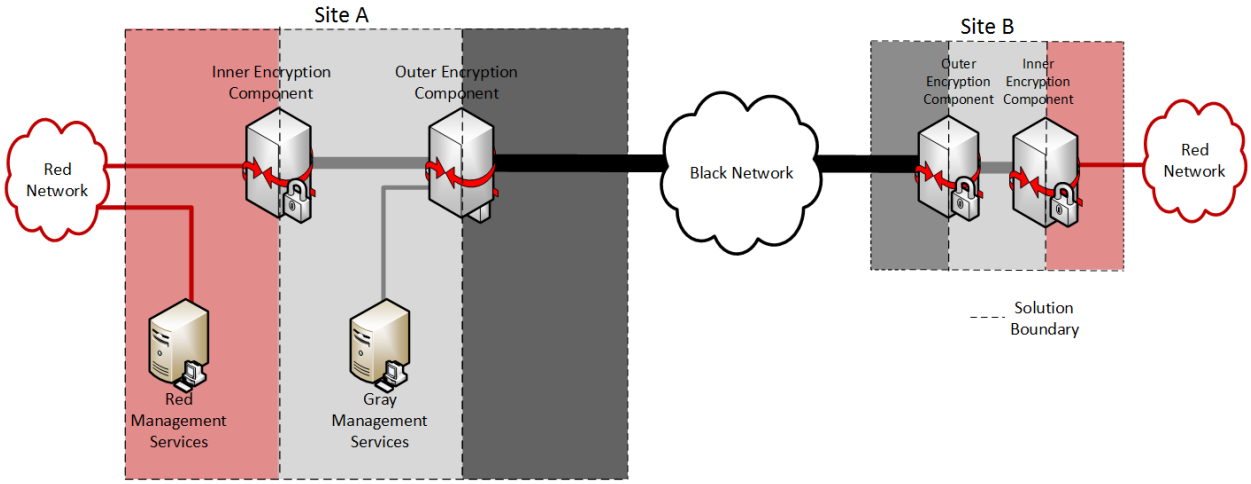

Figure 4. MSC Solution Connecting a Central Management Site and a Remote Site

Because the central management site manages the Encryption Components at the other sites over the network, encryption is used to logically separate data and management traffic as it passes between sites. Gray management traffic is encrypted using SSHv2, TLS 1.2 or later, IPsec, or MACsec before being routed through the Outer Encryption Component to the remote site. The SSHv2, TLS 1.2 or later, IPsec or MACsec serves as the inner layer of encryption for Gray management traffic, and the encryption tunnel provided by the Outer Encryption Component serves as the outer layer of encryption. Red management traffic is similarly encrypted before being routed through the Inner and Outer Encryption Components to another site. As a result, all management traffic between sites is encrypted at least twice before traversing the Black network.

Note that while Figure 4 depicts only two sites, this solution can scale to include numerous sites, with each additional site having the same high-level design as the remotely managed site in the figure.

4.2.2 MULTIPLE SECURITY LEVELS

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

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

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

4.2.2.1 Networks Operating at the Same Security Level

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

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

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

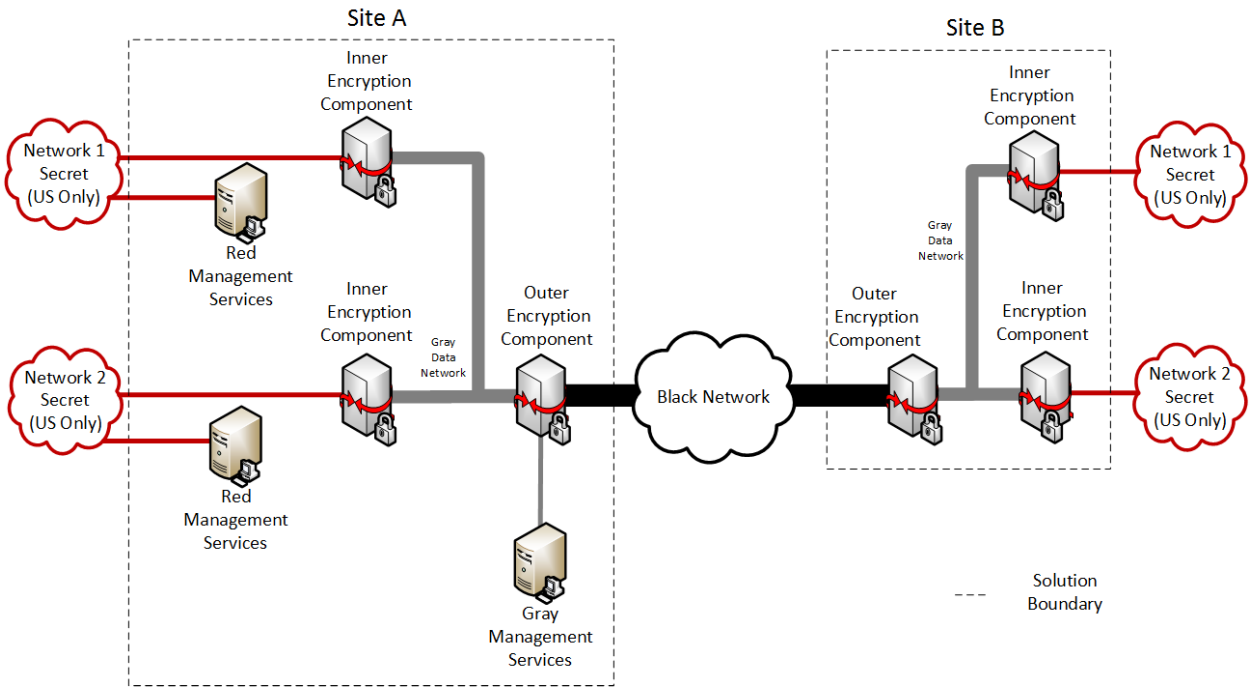

Figure 5. MSC Solution for Two Networks at the Same Security Level

4.2.2.2 Networks Operating at Different Security Levels

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

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

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

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

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

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

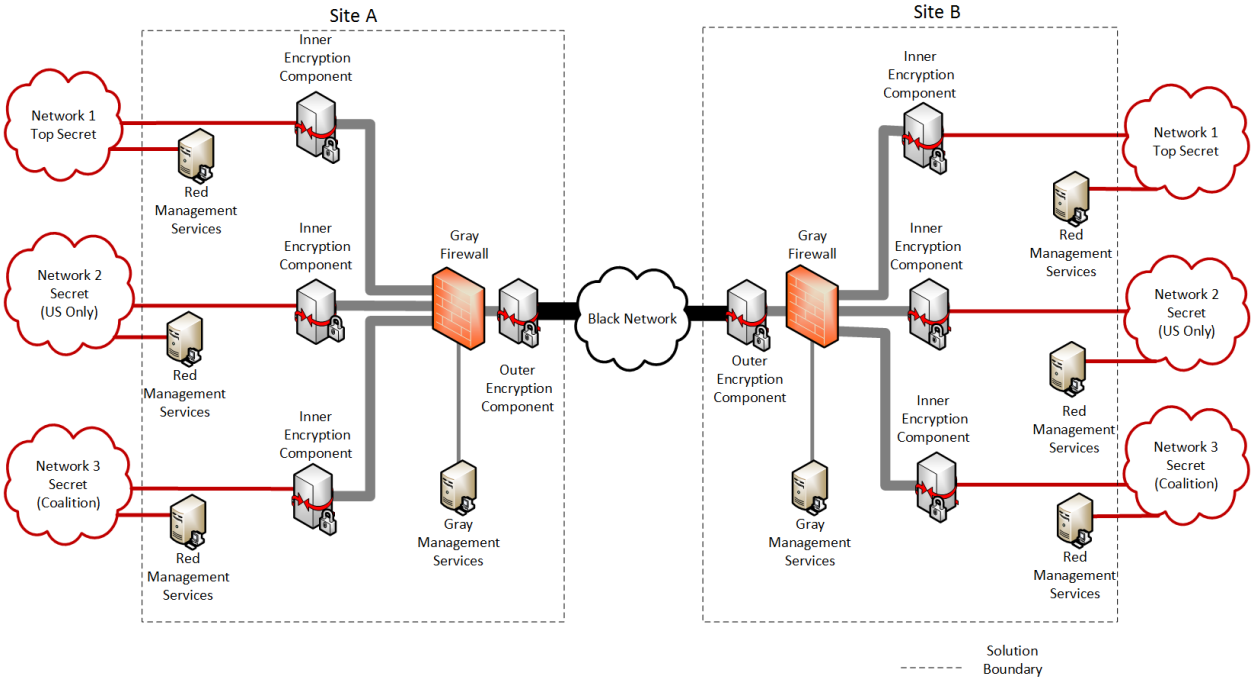

Figure 6. MSC Solution for Networks at Different Security Levels

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

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

4.2.3 LAYERING OPTIONS

Each layer of the MSC Solution can use either an IPsec tunnel or MACsec tunnel. An IPsec tunnel is established between VPN Gateways. A MACsec tunnel is established between MACsec Devices. Table 1 identifies four different layering options provided by this CP.

Table 1. Layering Options

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

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

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

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

This CP does not mandate the use of a specific protocol for encapsulation. Options include, but are not limited to, Layer 2 Tunneling Protocol version 3 (L2TPv3) and Ethernet over Multiprotocol Label Switching (EoMPLS).

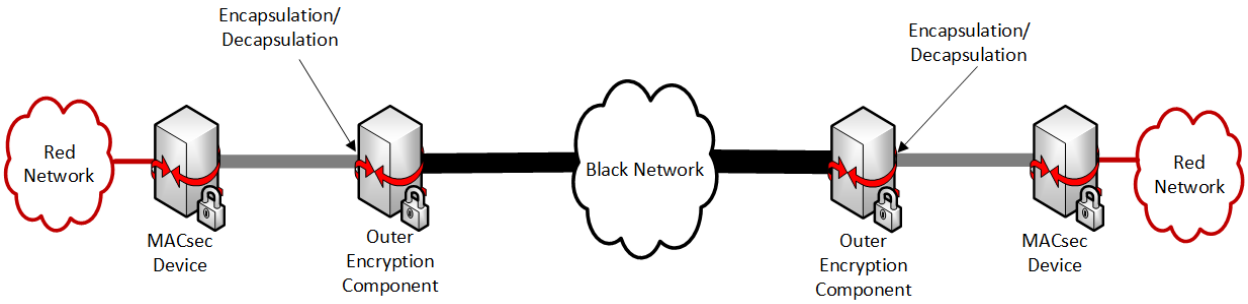

Figure 7. Encapsulating MACsec on an Internal Interface

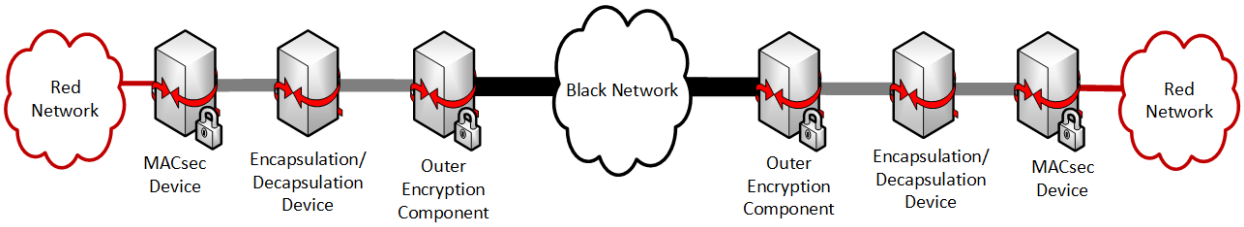

Figure 8. Encapsulating MACsec with a Separate Device

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

In the current MACsec standard, the entire frame is encrypted with the exception of the source and destination addresses. Draft amendment Institute of Electrical and Electronics Engineers (IEEE) 802.1Aecg-2016 provides the option of moving the Virtual LAN (VLAN) identification (ID) tag out of the encrypted payload and into the clear in the header. The benefits of moving the VLAN ID tag into the clear include service multiplexing (i.e., multiple point-to-point or multipoint services existing on a single physical interface) and providing quality of service (QoS) across a Service Provider's network. This CP allows VLAN ID tags to be used in the clear, if supported in the MACsec Device.

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

4.2.4 AUTHENTICATION

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

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

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

4.3 OTHER PROTOCOLS

Throughout this document, when IP traffic is discussed, it can refer to either Internet Protocol version 4 (Ipv4) or Internet Protocol version 6 (Ipv6) traffic, unless otherwise specified, as the MSC Solution is agnostic to most named data handling protocols. In addition, Red, Gray and Black networks can run either Ipv4 or Ipv6, and each network can independently make that decision. In the remainder of the document, if no protocols or standards are specified then any appropriate protocols may be used to achieve the objective.

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

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

4.4 AVAILABILITY

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

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

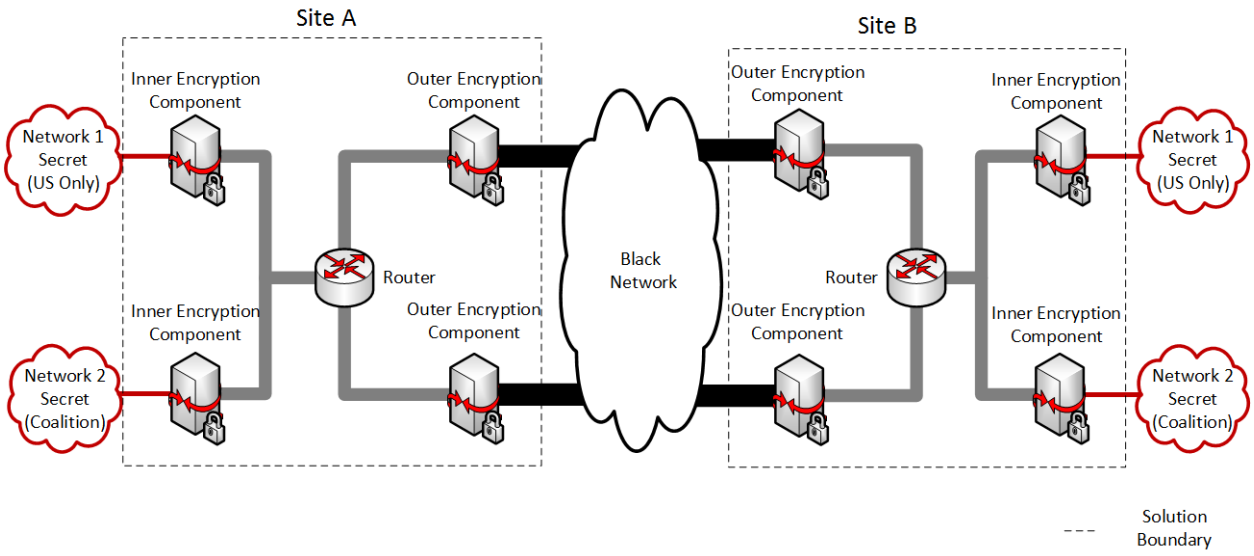

Figure 9. MSC Solution with Redundant Outer Encryption Components

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

5 SOLUTION COMPONENTS

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

Each Solution Component is described in more detail below. The descriptions include information about the security provided by the components as evidence for why they are deemed necessary for the solution. Components are selected from the CSfC Components List in accordance with the Product Selection requirements of this CP (see Section 10).

Additional components, discussed in Section 5.9, can be added to the solution to help reduce the overall risk. However, these are not considered mandatory components for the security of the solution; therefore, this CP does not place configuration or security requirements on the components.

5.1 OUTER FIREWALL

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

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

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

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

5.2 OUTER ENCRYPTION COMPONENT

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

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

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

Although the Outer Encryption Component may be a perimeter device if the Outer Firewall is not present and thus more exposed to external attacks, the Outer Encryption Component is also capable of protecting the network from unauthenticated traffic through use of an internal filtering capability. This allows specification of rules that prohibit unauthorized data flows, which helps mitigate Denial of Service (DoS) attacks and resource exhaustion. This CP does not require that the Outer Encryption Component terminate all tunnels on a single physical interface; however, all such external interfaces shall conform to the port filtering requirements in Section 11.6. The Outer Encryption Component is implemented identically for all the high-level designs covered in this CP.

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

The Outer Encryption Component is prohibited from implementing routing protocols on external and internal interfaces and must rely upon an Outer Firewall or Gray Firewall to provide any dynamic routing functionality. The Outer Encryption Component, selected from the CSfC Components List, must be physically separate from the Outer Firewall and Gray Firewall.

The Outer Encryption Component cannot route packets between Gray and Black networks; any packets received on a Gray network interface and sent out on a Black network interface must be transmitted within an IPsec or MACsec tunnel configured according to this CP. Management traffic on a Gray network, which originates from the Administration Workstation, must include two layers of encryption as described in this CP (see Section 11.8).

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

5.3 GRAY FIREWALL

The Gray Firewall is located between the Outer Encryption Component and Inner Encryption Component(s). A MSC Solution that supports multiple Red networks of different security levels must include one or more Gray Firewalls, as described in Section 4.2.2.2. The primary purpose of a Gray Firewall is to block any packets sent between Inner Encryption Components for Red networks of different security levels. A Gray Firewall also blocks any packets sent between management components on the Gray network and Inner Encryption Components for Red networks that operate at a security level

other than the highest security level of data protected by the solution. Gray Firewalls are physically protected as classified devices.

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

5.4 GRAY MANAGEMENT SERVICES

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

5.4.1 GRAY ADMINISTRATION WORKSTATION

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

5.4.2 GRAY SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

The Gray SIEM collects and analyzes log data from the Outer Encryption Component, Gray Firewall, and other Gray Management Service components. Log data should be encrypted between the originating component and the Gray SIEM with SSHv2, TLS 1.2 or later, IPsec, or MACsec to maintain confidentiality and integrity of the log data. At a minimum, an auditor reviews the Gray SIEM on a daily basis. The SIEM is configured to provide alerts for specific events including if the Outer Encryption Component or Gray Firewall receives and drops any unexpected traffic that could indicate a compromise. These functions can also be performed on a Red SIEM if a CDS is used as described in this CP (see Section 7.2).

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

5.5 INNER ENCRYPTION COMPONENT

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

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

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

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

When an Inner MACsec Device is used, the MACsec traffic will need to be encapsulated prior to being processed by the Outer Encryption Component, regardless of whether it's a VPN Gateway or a MACsec Device. Some VPN Gateways and MACsec Devices allow this encapsulation to occur on the incoming interface, prior to encrypting traffic for the outer tunnel. If the selected VPN Gateway or MACsec Device does not have this feature, a separate standalone router or switch is necessary to provide encapsulation and all requirements for Solution Components in this CP shall 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. An Inner Firewall is not required, unless the MSC Solution is being deployed with solutions from other CSfC CPs. In those cases, the Inner Firewall requirements from the other CSfC CPs must be addressed.

5.7 Red Management Services

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

5.7.1 Red Administration Workstation

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

5.7.2 RED SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

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

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

5.8 KEY AND CERTIFICATE MANAGEMENT COMPONENTS

MSC Solutions may require PKI services to issue and manage device certificates for Outer and Inner VPN Gateways. The PKI services consist of an outer tunnel CA (known as the Outer CA); Gray Network Certification Revocation Status Services; an inner tunnel CA (known as the Inner CA); and Red Network Certification Revocation Status Services. In addition, MSC Solutions may require a symmetric KGS to generate, distribute and manage CAKs for Outer and Inner MACsec Devices. Each of these is described below.

5.8.1 OUTER CERTIFICATION AUTHORITIES

An Outer CA is required to issue digital certificates for Outer VPN Gateways in the MSC Solution. These certificates are used for authentication in establishing the Outer IPsec tunnels between pairs of Outer VPN Gateways. The Outer CA may be an enterprise CA that is accessible[1] via the Gray or Red network, or a locally-run CA that operates in the Gray or Red network. When an Enterprise PKI capability is used, it is managed with that PKI's existing processes and capabilities. Enterprise CAs then provide certificate management services for the MSC Solution over the Gray or Red network (see Section 8 for additional details regarding enterprise and locally-run CAs).

If the Outer CA delivers services to, or operates in the Red network it is critical to have AO-approved mechanisms in place to transfer any certificate-related information (e.g., revocation status information) to the Gray network to ensure it is accessible to the Outer VPN Gateway and Gray Management Services. Furthermore, if the Outer CA is locally-run then this CP also requires a physically separate Inner CA located in the Red network to issue certificates to the Inner VPN Gateways. Physical separation

[1] Access to the enterprise PKI may be via a controlled network connection or via a physical interface (e.g., media transfer).

between locally-run CAs is required to comply with the MSC Solution requirement for two security tunnels with independent layers of encryption.

The Outer CA shall have an approved Certificate Policy and Certification Practice Statement (CPS) that are conformant with Internet Engineering Task Force (IETF) Request for Comments (RFC) 3647.

5.8.2 Gray Network Certificate Revocation Status Services

Certificate Revocation List (CRL) Distribution Points (CDPs) and Online Certificate Status Protocol (OCSP) Responders are servers that provide certificate revocation status information to MSC Solution Components. Outer CDPs and OCSP Responders are deployed on the internal side of the Outer VPN Gateway that outer tunnel certificate revocation status information is being made available. Collectively, Outer CDPs and OCSP Responders are referred to as Gray Network Certificate Revocation Status Services.

The Gray Network Certificate Revocation Status Services ensure the Outer VPN Gateway can verify the revocation status of other Outer VPN Gateway authentication certificates. The Gray Network Certificate Revocation Status Services may also provide certificate revocation status information to Gray Management Services.

Outer CDPs and OCSP Responders are not required components of the MSC CP, but if not used the organization must implement other means, such as whitelists, to ensure revoked certificates are never used to establish the Outer IPsec tunnel or a tunnel for Gray Management Services.

The use of CDPs and OCSP Responders in MSC Solutions is discussed in detail in Section 8.1.3.

5.8.3 Inner Certification Authorities

An Inner CA is required to issue digital certificates for the Inner VPN Gateways in the MSC Solution. These certificates are used for authentication in establishing the Inner IPsec tunnel between pairs of Inner VPN Gateways. The Inner CA may be an enterprise CA that is accessible via the Red network, or a locally-run CA that operates in the Red network (see Section 8 for additional details regarding enterprise and locally-run CAs). When an Enterprise PKI capability is used, it is managed with that PKI's existing processes and capabilities. Enterprise CAs then provide certificate management services for the MSC Solution over the Red network.

The Inner CA shall have an approved Certificate Policy and CPS that are conformant with IETF RFC 3647. If the solution is supporting Red networks of different security levels, then a separate CA is needed for the Inner VPN Gateways of each security level.

5.8.4 Red Network Certificate Revocation Status Services

Inner CDPs and OCSP Responders are deployed either between the Inner VPN Gateway and Inner Firewall, if present, or on the internal side of the Inner VPN Gateway. Inner CDPs and OCSP Responders make certificate revocation status information available to Inner VPN Gateways of the MSC Solution.

Collectively, Inner CDPs and OCSP Responders are referred to as Red Network Certificate Revocation Status Services.

The Red Network Certificate Revocation Status Services ensure the Inner VPN Gateway can verify the status of other Inner VPN Gateway authentication certificates. The Red Network Certificate Revocation Status Services may also provide certificate revocation status information to Red Management Services.

Inner CDPs and OCSP Responders are not required components of the MSC CP, but if not used the organization must implement other means, such as whitelists, to ensure revoked certificates are never used to establish the Inner IPsec tunnel or a tunnel for Red Management Services.

The use of CDPs and OCSP Responders in MSC Solutions is discussed in detail in Section 8.1.3.

5.8.5 Symmetric Key Generation Solutions

MSC Solutions that use at least one MACsec Device for the Outer or Inner Encryption Component require a single symmetric KGS located in the Red network to generate, distribute and manage CAKs for the MACsec Device. These CAKs are used for authentication in establishing the MACsec tunnel between a pair of Outer or Inner MACsec Devices. If MACsec Devices are used for both the Outer and Inner Encryption Components, the single KGS operating in the Red network generates, distributes and manages CAKs for both of the MACsec Devices.

Since the KGS operates in the Red network, AO-approved mechanisms are required to distribute CAKs from the KGS to Outer MACsec Devices that operate in the Gray network. The use of a KGS in MSC Solutions is discussed in detail in Section 8.2.

5.9 Other Controls

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

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

6 CONFIGURATION AND MANAGEMENT

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

6.1 COMPONENT PROVISIONING

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

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

6.2 ADMINISTRATION OF COMPONENTS

Each component in the solution has one or more Administration Workstations that are responsible for maintaining, monitoring, and controlling all security functions for that component. It should be noted that all of the required administrative functionality does not need to be present in each individual workstation, but the entire set of Administration Workstations must collectively meet administrative functionality requirements.

The Administration Workstation is used for configuration review and management. Implementations may employ a SIEM in the Gray Management Services for log management of Gray infrastructure components except where AOs use a CDS to move Gray network log data to a Red SIEM.

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

The Gray Administration Workstation, along with all Gray Management Services, is physically connected to the Gray Firewall, if present, or Outer Encryption Component. The Gray Firewall maintains separate

Access Control Lists (ACLs) to permit management traffic to/from the Gray Management Services, but prohibits such traffic from all other components. These ACLs ensure that approved management traffic is only capable of flowing in the intended direction. This architecture provides the separation necessary for two independent layers of protection.

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

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

7 CONTINUOUS MONITORING

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

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

7.1 MONITORING POINTS

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

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

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

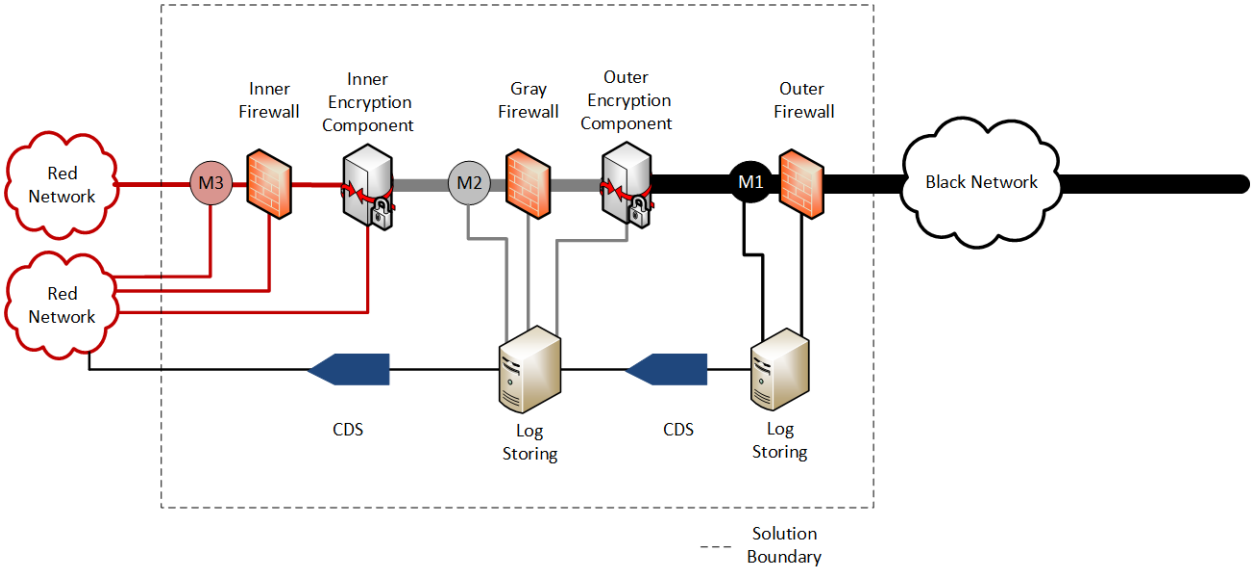

Figure 10. MSC Solution Continuous Monitoring

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

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

Monitoring Point 2 (M2): Located between the Outer Encryption Component and the Gray Firewall (or Inner Encryption Component if a Gray Firewall is not required), a M2 IDS/IPS is, at a minimum, configured to send an alert upon detection of any traffic that should have been blocked by the Outer

Encryption Component. These alerts can indicate a failure of the Outer Firewall or Outer Encryption Component's filtering functions and are evidence of either an improper configuration or a potential compromise. Normal traffic at M2 is not as narrowly defined, but includes IPsec, MACsec, control plane traffic, and management traffic. Nearly all traffic traversing M2 is encrypted with IPsec, MACsec or SSHv2, which prevents the ability to perform deep packet inspection. Management of a M2 IDS/IPS occurs within the Gray Management Services.

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

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

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

7.2 Log Data

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

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

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

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

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

7.3 NETWORK FLOW DATA

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

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

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

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

7.4 CHANGE DETECTION

One method of automating the detection of configuration changes without the complexity and expense of dedicated configuration management systems is to leverage the collection of syslog. In addition to collecting basic security events, the syslog facility is also capable of sending events related to system configuration changes. Queries, which generate alerts for administrators and auditors to review, can be developed on either the log collection server or the SIEM. Change detection is a required component of this CP (see Section 11.7).

7.5 COLLECTION

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

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

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

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

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

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

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

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

7.6 CORRELATION

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

8 KEY MANAGEMENT

One of the most difficult parts of any solution is determining how the key management will be implemented in a secure manner for component authentication to establish the outer and inner encryption tunnels. In the MSC Solution, certificates are used for VPN Gateways and CAKs are used for MACsec Devices.

To provide confidentiality services within the MSC Solution, the Encryption Components use key agreement protocols to generate ephemeral encryption keys. The use of ephemeral encryption keys is

not part of key management discussed in this section, as CAs are not required in issuing and managing these keys.

8.1 CERTIFICATES

This section provides details on issuing, rekeying and revoking certificates for VPN Gateways. Certificate renewal of VPN Gateway certificates is prohibited in MSC Solutions.

8.1.1 CERTIFICATE ISSUANCE

MSC Solutions with VPN Gateways use asymmetric algorithms (as defined in Table 6) and X.509 certificates for component authentication to establish the outer and inner encryption tunnels. If you have long data life concerns, please contact the CSfC PMO for additional details on how symmetric key cryptography can be leveraged in this CP.

Each VPN Gateway contains a private authentication key and a corresponding public certificate issued by an authorized CA. In addition, a trusted CA certificate is installed, as well as any other CA signing certificates that connect to the trusted CA, so that a trusted certificate chain is established between the VPN Gateway certificate and the trusted CA certificate. Each VPN Gateway should also contain the required CRLs to support revocation status checking of other VPN Gateway certificates. If CRLs are not used, other mechanisms can be implemented (e.g., whitelists) in VPN Gateways.

Authentication keys (public/private key pair) for VPN Gateways are to be generated on the VPN Gateway, where the private keys are never exported out of the component. If the VPN Gateway cannot generate its own key pair, a dedicated management workstation is required to generate the key pair for the component. The public keys are sent in certificate requests to the Outer and Inner CAs that create and sign authentication certificates containing the public keys. The authentication certificates are delivered to, and installed on, the VPN Gateways during provisioning, along with the private keys if they were not generated on the component.

The CAs also issue signed CRLs to provide revocation status information for the certificates issued by the CAs. CRLs are transferred to CDPs or OCSP Responders as discussed in Section 8.1.3, where the certificate revocation status information is made available to the VPN Gateways.

To provide confidentiality services within MSC Solutions, the components use key agreement protocols (such as Elliptic Curve Diffie-Hellman (ECDH)) to generate ephemeral encryption keys. The use of ephemeral encryption keys is not part of key management discussed in this section, as CAs are not required in issuing and managing these keys.

The CAs that issue authentication certificates to VPN Gateways operate either as Enterprise CAs (e.g., National Security Systems (NSS) PKI, Key Management Infrastructure (KMI), and Agency PKI) or locally-run CAs. Existing Enterprise CAs should be used whenever possible, as the advantages for using these CAs outweigh those associated with locally-run CAs. However, Enterprise CAs that operate on or are accessible via the Black Network are not permitted to be used in MSC Solutions.

Enterprise CAs have established operations, as well as Certificate Policies and CPSs that customer organizations can leverage for their MSC Solution. These Enterprise CAs operate at Federal Department and Agency levels (e.g., NSS PKI, KMI), and offer wide-scale interoperability across MSC Solutions (i.e., the Certificate Policies and their registered policy Object Identifiers (OIDs) are widely accepted across the Federal Department or Agency). When an Enterprise Root CA is used to support a MSC Solution that uses Outer and Inner VPN Gateways, this CP requires that at least two existing Subordinate CAs are used to issue certificates. One Subordinate CA issues certificates to the Outer VPN Gateway (known as the Outer CA) and the other CA issues certificates to the Inner VPN Gateway (known as the Inner CA). To ensure that the same certificate cannot be used for authenticating both the outer and inner tunnels, the Outer CA and Inner CA are used as trust anchors to validate the outer tunnel and inner tunnel authentication certificates, respectively.

For MSC Solutions requiring interoperability across a Federal Department or Agency, Department/Agency-level Enterprise CAs should be leveraged. Examples of Department/Agency-level Enterprise CAs include the NSA KMI, the National Security Systems (NSS) PKI, and the Intelligence Community (IC) PKI. Enterprises like this leverage Department/Agency-level Trusted CAs that reside under the same Root CA. Trusted CAs like this can be used as trust anchors in multiple MSC Solutions throughout a Federal Department or Agency, thereby providing certificate trust interoperability across those MSC Solutions. In addition, certificates issued by Department/Agency-level Enterprise CAs may assert registered policy OIDs that are acceptable for use through the Federal Department or Agency.

For the Enterprise CAs described above, an MSC Solution Owner could deploy and operate independent Subordinate CAs that are issued certificates by a higher-level Enterprise CA. The benefit of this configuration is that it allows tailoring of the Subordinate CA operations to the local environment without losing the interoperability benefits gained by leveraging Enterprise CAs. However, the MSC Solution Owner is responsible for defining and implementing CPSs for the Subordinate CAs that are approved by the Enterprise CA policy authorities.

Finally, MSC Solutions requiring minimal or no interoperability can deploy and operate their own locally-run CAs that are independent of any Enterprise CAs. In this configuration, certificate policy and interoperability is constrained to the specific MSC Solution. Furthermore, the MSC Solution Owner is required to develop and maintain CPSs that detail the operational procedures for the locally-run CAs. In addition, the customer may need to develop and maintain a higher-level Certificate Policy if one does not already exist.[2] Table 2 summarizes the differences between Enterprise and locally-run CAs.

[2] CNSSP 25 is the governing policy for PKI solutions in support of Secret MSC Solutions. For MSC Solutions that are higher than Secret, the MSC Solution Owner is required to develop a Certificate Policy that is approved by the local Approving Official (AO).

Table 2. Certification Authority Deployment Options

CA Type	Certificate Policy	Interoperability	Operations
Department/ Agency-level Enterprise	Owned and managed at the Department/Agency level (e.g., NSA KMI, NSS PKI, IC PKI)	Department-wide/Agency-wide	Performed by the Enterprise
Subordinate CA (Enterprise)	Owned and managed at the Department/Agency level	Department-wide/Agency-wide	Performed by the Enterprise and the MSC Solution Owner
Locally-run (Non-Enterprise)	Owned and managed at the MSC Solution level	Constrained to the MSC Solution	Performed by the MSC Solution Owner

In all CA configurations identified above, Outer CAs issue and manage authentication certificates for Outer VPN Gateways and Gray Management Service Components; Inner CAs issue and manage authentication certificates for Inner VPN Gateways and Red Management Service Components. Outer CAs can be included as either part of the Gray network or Red network. Inner CAs can only be located in the Red network.

To assist the CAs in their operations, the CAs may communicate with management services (e.g., Device Managers (DMs)) deployed in the corresponding network to support enrollment and life-cycle certificate management for MSC Solution Components. Outer and Inner CAs in the Red network are limited to directly communicating with Red Management Services. Outer CAs in the Gray network are limited to directly communicating with Gray Management Services. When the CA is not located in the same network as the required management services, an AO-approved CDS may be used allowing indirect communication (e.g., Certificate Enrollment). The Red and Gray Management Services enable the certificate request/response process between a VPN Gateway and a CA. This CP recommends initially provisioning the VPN Gateways (Outer and Inner) in the Red network, and that all enrollment and life-cycle certificate management be performed in accordance with the applicable CPSs.

The MSC Solution uses device authentication certificates, and the device certificates and private keys are considered Controlled Unclassified Information (CUI) (unless determined to be higher by the AO) because they are only used for mutual authentication, not for traffic encryption or granting access to classified data. An out-of-band method must be used to issue the initial device certificates to the VPN Gateways; however, subsequent rekeying may take place over the network through this solution prior to the current key's expiration (see Section 8.1.2 for additional details regarding over-the-network remote certificate rekey). The key validity period for certificates issued by locally-run CAs cannot exceed 14 months, while the key validity period for certificates issued by an Enterprise CA are inherited from the Enterprise CA Certificate Policy. Updates to CRLs are distributed to VPN Gateways within 24 hours of CRL issuance.

8.1.2 CERTIFICATE REKEY

If the Outer and/or Inner VPN Gateway is capable of generating its own public/private key pairs and can communicate with the Outer and/or Inner CA using Enrollment over Secure Transport (EST) as defined in IETF RFC 7030, the VPN Gateway can have its device certificate remotely rekeyed, as opposed to physically returning the VPN Gateway to the provisioning environment as described in Section 8.1.1.

The VPN Gateway uses its current device authentication certificate to authenticate to an EST Server associated with the CA that initially issued the device authentication certificate to the VPN Gateway. Once authenticated, the VPN Gateway generates a new public/private key pair. The newly generated public key is placed into a new certificate request in accordance with RFC 7030. The certificate request is then submitted to the CA for processing using EST. The CA validates that the certificate request came from a valid and authenticated VPN Gateway, processes the certificate request, and returns a newly signed certificate containing the new public key to the VPN Gateway. The VPN Gateway receives and installs the newly rekeyed certificate.

8.1.3 DISTRIBUTION OF CERTIFICATE REVOCATION LISTS

CRLs are used by CAs to convey the revocation status of certificates issued by those CAs, and those CRLs need to be made available to the VPN Gateways.

A CDP is a web server whose sole function is to provide external distribution of, and access to CRLs issued by CAs. CDPs do not serve any other content, and, in particular, do not host any dynamically generated content. CDPs also do not provide any other services other than the distribution of CRLs. CDPs are optional in this CP, and they can exist in the Gray or Red networks. The Outer VPN Gateway accesses an Outer CDP, located in the Gray network, to obtain CRLs and check revocation status of the other VPN Gateway prior to establishing the outer encryption tunnel. Furthermore, a CDP operating in the Gray network can be accessed by Gray Management Service components to obtain CRLs and check the revocation status of the Outer VPN Gateway's certificate prior to establishing a device management tunnel with the Outer VPN Gateway.

Inner VPN Gateways access an Inner CDP, located in the Red network, to obtain CRLs and check revocation status of another site's Inner VPN Gateway prior to establishing the inner encryption tunnel. Likewise, a CDP operating in the Red network can be accessed by Red Management Service components to obtain CRLs and check the revocation status of the Inner VPN Gateway's certificate prior to establishing a device management tunnel with the Inner VPN Gateway.

An Outer CDP and an Outer CA may reside on the same or different networks. For example, the Outer CA may be operated in the Red network, while the Outer CDP operates in the Gray network. If they reside on different networks, a one-way transfer mechanism is required to periodically distribute the current CRL from the CA to the CDP. The details and procedures of the one-way transfer mechanism are left to a solution's AO.

Since CRLs are digitally signed objects that contain minimally identifying information about MSC Solution Components, there are few concerns with the confidentiality of CRLs. Therefore, CRLs can be downloaded by MSC Solution Components over unencrypted HTTP. Furthermore, a CRL's integrity is protected by the digital signature of the CA that issued it, and additional integrity protection during CRL download is not required. Additionally, placement of CDPs on the Gray network for the Outer VPN Gateway and Red network for Inner VPN Gateway reduces the exposure to external threat actors.

Use of HTTP Secure (HTTPS) for CRL downloading is discouraged, as it introduces a circular dependency between the CDP and the MSC Solution Component attempting to download the CRL. The MSC Solution Component would need a CRL to determine whether the CDP's certificate is revoked before establishing an HTTPS connection to the CDP. However, the CDP cannot deliver the CRL to the MSC Solution Component until the MSC Solution Component authenticates the CDP by validating its certificate. (Note: Distributing CRLs via HTTP follows the recommendation in IETF RFC 5280 not to use HTTPS to distribute CRLs.)

To provide redundancy and ensure that current CRLs are always made available to MSC Solution Components, multiple Outer and Inner CDPs may be deployed. The use of multiple CDPs is left to the discretion of the MSC Solution Owner. Furthermore, CDPs may host partial or delta CRLs in addition to complete CRLs. In large MSC Solutions, the use of partial or delta CRLs can reduce the amount of network traffic needed to distribute updates to CRLs. A CA's Certificate Policy will define whether the use of partial or delta CRLs is permissible.

OCSP Responders or white lists can be used in lieu of CDP Servers. OCSP Responders located in the Gray network can provide certificate revocation status information to the Outer VPN Gateway. Additionally, OCSP Responders in the Red network can provide certificate revocation status information to Inner VPN Gateway.

8.2 Connectivity Association Keys

This section provides details for securely managing pre-shared symmetric CAKs, which is a sensitive and critical function within an MSC Solution. CAK management includes secure generation, distribution, installation, update (rekey), accounting, compromise reporting, and destruction of CAKs. In addition to generating CAKs of appropriate strength to protect classified information, CAKs need to be securely distributed and further managed to mitigate the risk of unauthorized disclosure of the CAKs (e.g., insider threat). If a CAK is compromised, all MACsec Devices using that CAK need to be updated with a new CAK. This is different from a certificate-based solution in that revocation of any given certificate only impacts the device associated with that certificate.

CAK management can be provided by Enterprise services (e.g., KMI) or via a locally-operated, NSA-approved KGS. Enterprise CAK management services are those services that can be provided on a Department-wide or Agency-wide scale, such as by the NSA KMI. The KMI also allows Agencies to locally manage CAKs using a specialized NSA-approved Management Client (MGC), although currently the MGC

does not have a commercial standard interface to securely distribute CAKs to MACsec Devices. However, customers can acquire or develop a custom application that can receive CAKs from KMI and reformat it for secure distribution to and installation on MACsec Devices. KMI refers to these customer applications as Delivery Only Clients (DOCs). DOCs must be NSA-approved. If Enterprise CAK management is not feasible, customers can deploy a locally-operated, NSA-approved KGS to generate and manage CAKs for MACsec Devices. In either case, enterprise or locally-operated, the customer is responsible for developing a Key Management Plan (KMP) for the CAKs used in the MSC Solution, and obtaining approval for the KMP by the National Cryptographic Solutions Management Office (NCSMO). The KMP addresses secure life-cycle management of the CAKs, and the NCSMO can assist in developing the KMP.

In addition to a KMP, customers may need to obtain an Information Assurance Directorate Management Directive 110 (IAD MD-110), *Cryptographic Key Protection*, waiver since commercial equipment typically allows CAKs to exist in red form during part of the CAK life-cycle management process. Customers are strongly encouraged to contact their Client Advocate early in the process to obtain the NCSMO's assistance in developing the KMP, selecting an NSA-approved KGS, or obtaining an IAD MD-110 waiver.

8.2.1 Connectivity Association Key Issuance, Renewal and Rekey

Each MACsec Device has at least one CAK, which is used by the MACsec Device to authenticate with another MACsec Device. A different and unique CAK is required for every pair of MACsec Devices establishing an encryption tunnel. Also, if both layers of the solution use MACsec, different and unique CAKs are required for the inner and outer encryption tunnels. Every CAK has a unique Connectivity Association Key Name (CKN) to distinguish it from other CAKs that may be loaded in the MACsec Device.

CAKs and CKNs must be generated by an NSA-approved KGS (enterprise or locally-operated) and securely distributed and installed into the MACsec Devices. Secure distribution and installation can be achieved via technical means (e.g., encryption) or procedural controls, or a combination of both. A pre-placed CAK Encryption Key (CEK) can be used to encrypt CAKs during the distribution process; however, installation of CAKs into MACsec Devices is performed with the CAKs in red (plaintext) form as the MACsec Devices do not have the technical capabilities to accept and decrypt encrypted CAKs. CEKs are also generated by the NSA-approved KGS, and a separate and unique CEK should be used for each MSC Solution site.

KGS Administrators (KGSAs) are highly trusted personnel that follow two-person control procedures to install the CAKs into the MACsec Devices and destroy any copies of CAKs after installation into the MACsec Device is complete. KGSAs also account for CAKs to ensure their location and use is known at all times. In the case of compromise, KGSAs need to be able to determine where all instances of a given CAK exist and update that CAK in accordance with compromise reporting and recovery procedures.

CAKs require periodic updating (rekeying) to limit the amount of operational exposure for the CAKs. This CP requires CAKs to be updated (rekeyed) at least every 30 days, and CEKs to be updated (rekeyed) at least every 90 days.

8.2.2 CONNECTIVITY ASSOCIATION KEY COMPROMISE RECOVERY

CAK compromise recovery is a critical function within the MSC Solution. Therefore, good accounting records are necessary to know which CAKs are installed on which MACsec Devices. When a CAK is compromised, the CAK must be updated (rekeyed) immediately within both MACsec Devices at both solution sites by generating a new CAK at the KGS. The specific CAK compromise recovery procedures are documented in the KMP.

9 REQUIREMENTS OVERVIEW

The following five sections (Sections 10 through 14) specify requirements for implementations of MSC Solutions compliant with this CP.

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., “KM”), and a sequence number (e.g., 11). Table 3 lists the

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

Table 3. Requirement Digraphs

Digraph	Description	Section	Table
PS	Product Selection Requirements	Section 10	Table 4
SR	Overall Solution Requirements	Section 11.1	Table 5
VG	VPN Gateway Requirements	Section 11.2	Table 7
MD	MACsec Device Requirements	Section 0	Table 9
IR	Additional Requirements for Inner Encryption Components	Section 11.4	Table 10
OR	Additional Requirements for Outer Encryption Components	Section 11.5	Table 11
PF	Port Filtering Requirements for Solution Components	Section 11.6	Table 12
CM	Configuration Change Detection Requirements	Section 11.7	Table 13
DM	Device Management Requirements	Section 11.8	Table 14
MR	Continuous Monitoring Requirements	Section 11.9	Table 15
AU	Auditing Requirements	Section 11.10	Table 16
KM	Key Management Requirements	Section 11.11	Table 17 through Table 24
GD	Requirements for the Use and Handling of Solutions	Section 12.1	Table 25
RP	Incident Reporting Requirements	Section 12.2	Table 26
RB	Role-Based Personnel Requirements	Section 13	Table 27
TR	Testing Requirements	Section 14.1	Table 28

10 REQUIREMENTS FOR SELECTING COMPONENTS

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

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

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

In this section, a series of requirements are given for maximizing the independence between the components within the solution. The requirements in Table 4 will increase the level of effort required to compromise this solution.

Table 4. Product Selection (PS) Requirements

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-PS-1	The products used for any VPN Gateway shall 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 shall 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 shall be chosen from the list of Traffic Filtering Firewalls (TFFWs) on the CSfC Components List.	T=O	
MSC-PS-4	The products used for any CAs shall either be chosen from the list of CAs on the CSfC Components List or the CAs shall be pre-existing Enterprise CAs of the applicable network.	T=O	
MSC-PS-5	Intrusion Prevention Systems (IPSs) shall 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 shall 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 shall not use the same Operating System. Differences between Service Packs and version numbers for a particular vendor's operating system (OS) do not provide adequate diversity.	T=O	
MSC-PS-8	The cryptographic libraries used by the Inner Encryption Component and Outer Encryption Component shall either: come from different manufacturers, where neither manufacturer is a subsidiary of the other; or be different libraries from the same manufacturer, where NSA has determined that the libraries meet the CSfC criteria for implementation independence.	O	None

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-PS-9	If the solution contains an Inner CA and an Outer CA, the cryptographic libraries shall 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 shall 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 shall 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 shall 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 shall follow one of the following guidelines: • The CAs come from different manufacturers, where neither manufacturer is a subsidiary of the other. • The CAs are different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence. • The CAs use an Enterprise PKI approved by the AO.	O	None
MSC-PS-15	Each component that is selected from the CSfC Components List shall go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO-approved Product Supply Chain Threat Assessment process (see CNSSD 505 SCRM for additional guidance).	T=O	
MSC-PS-16	MSC Solution Components shall be configured to use the NIAP-certified evaluated configuration.	T=O	

11 CONFIGURATION REQUIREMENTS

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

11.1 OVERALL SOLUTION REQUIREMENTS

Table 5 provides the overall solution requirements for this CP.

Table 5. Overall Solution Requirements (SR)

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-SR-1	Network services provided by control plane protocols (such as DNS and NTP) shall 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 shall ensure that each tunnel's Encryption Components selected by each site are interoperable.	T=O	
MSC-SR-3	The time of day on the Inner Encryption Component and Red Management Services shall 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) shall 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 shall be changed or removed.	T=O	
MSC-SR-6	All components shall be properly configured in accordance with local policy and applicable U.S. Government guidance. In the event of conflict between the requirements in this CP and local policy, this CP takes precedence.	T=O	
MSC-SR-7	All physical paths within a Gray network between Inner Encryption Components for Red networks of different security levels shall include a Gray Firewall.	T=O	
MSC-SR-8	All physical paths within a Gray network between a CA, an Administration Workstation, or a CDP/OCSP Responder and an Inner Encryption Component for Red networks of different security levels shall include a Gray Firewall.	T=O	

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-SR-9	Gray network components shall be physically protected to the level of the highest classified network.	T=O	
MSC-SR-10	The Outer Encryption Component shall use a unique physical internal interface for each Red network in the MSC Solution (e.g., VLAN trunking of multiple enclaves is not permitted).	T=O	
MSC-SR-11	A Gray Firewall is required if the MSC Solution is combined with another CSfC solution that requires a Gray Firewall.	T=O	
MSC-SR-12	If the MSC Solution uses the Public Internet for its Black transport network, an Outer Firewall shall be located between the Black transport network and the Outer Encryption Component.	T=O	
MSC-SR-13	If the MSC Solution is combined with other CSfC data-in-transit solutions that include end user devices, an Inner Firewall is required. All firewall requirements for the other CSfC solution supersede firewall requirements for the MSC CP.	T=O	
MSC-SR-14	The only approved physical paths leaving the Red network shall be through a MSC Solution in accordance with this CP or via an AO-approved solution for protecting data in transit.[3]	T=O	
MSC-SR-15	Solution Components shall receive virus signature updates as required by the local agency policy and the AO.	T=O	
MSC-SR-16	When multiple Inner Encryption Components share an Outer Encryption Component, they shall be placed in parallel.	T=O	
MSC-SR-17	Inner Encryption Components shall not perform switching or routing for other Encryption Components.	T=O	
MSC-SR-18	Solution Components shall only be configured over an interface dedicated for management.	T=O	
MSC-SR-19	DNS lookup services on network devices shall be disabled.	O	None
MSC-SR-20	DNS server addresses on Solution Components shall be specified or DNS services shall be disabled.	T=O	
MSC-SR-21	Automatic remote boot-time configuration services shall be disabled (e.g., automatic configuration via Trivial File Transfer Protocol (TFTP) on boot).	T=O	

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

11.2 VPN GATEWAY REQUIREMENTS

This section addresses requirements for VPN Gateways. Table 6 identifies the algorithms approved for IPsec encryption. Table 7 provides requirements for VPN Gateways.

Table 6. IPsec Encryption (Approved Algorithms for Classified)

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

Table 7. VPN Gateway (VG) Requirements

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-VG-1	The proposals offered by VPN Gateways in the course of establishing the Internet Key Exchange (IKE) Security Association (SA) and the ESP SA for inner and outer tunnels shall be configured to offer algorithm suite(s) containing only CNSA Suite algorithms (see Table 6).	T=O	
MSC-VG-2	Default, self-signed or proprietary device certificates, which are frequently preinstalled by the vendor, for any VPN Gateway shall 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 shall be removed.	O	MSC-VG-2

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-VG-4	A unique device certificate shall 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 shall not be accessible through an interface.	T=O	
MSC-VG-6	A device certificate shall be used for VPN Gateway authentication during IKE.	T=O	
MSC-VG-7	VPN Gateway authentication shall 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 shall include a check that certificates are not expired.	T=O	
MSC-VG-9	All VPN Gateways shall use IKEv2 (IETF RFC 7296) key exchange.	T=O	
MSC-VG-10	All VPN Gateways shall use Cipher Block Chaining for IKE encryption.	T=O	
MSC-VG-11	All VPN Gateways shall use Cipher Block Chaining for ESP encryption with a Host-based Message Authentication Code (HMAC) for integrity.	T	MSC-VG-12
MSC-VG-12	All VPN Gateways shall use Galois Counter Mode for ESP encryption.	O	MSC-VG-11
MSC-VG-13	All VPN Gateways shall set the IKE SA lifetime to at most 24 hours.	T=O	
MSC-VG-14	All VPN Gateways shall set the ESP SA lifetime to at most 8 hours.	T=O	
MSC-VG-15	Inner VPN Gateways shall 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 shall 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 shall only allow the VPN Gateway to access the private key of the VPN Gateway.	O	None

11.3 MACSEC DEVICE REQUIREMENTS

This section addresses requirements for MACsec Devices. Table 8 identifies the algorithms approved for MACsec encryption. Table 9 provides requirements for MACsec Devices.

Table 8. MACsec Encryption (Approved Algorithms for Classified)

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

Table 9. MACsec Device (MD) Requirements

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-MD-1	MACsec Devices shall use AES Key Wrap for key distribution with a cryptographic key sizes of 256 bits.	T=O	
MSC-MD-2	MACsec Devices shall use AES GCM for MACsec with a cryptographic key sizes of 256 bits.	T=O	
MSC-MD-3	MACsec Devices shall authenticate using Pre-Shared Keys (PSKs), known as Connectivity Association Keys (CAKs).	T=O	
MSC-MD-4	CAKs shall be AES 256 bits and generated using an NSA-approved KGS.	T=O	
MSC-MD-5	MACsec Devices shall have the length of the CKN set to a minimum of 16 bytes (128 bits) and generate the CKN using an NSA-approved KGS.	T=O	
MSC-MD-6	For each pair of MACsec Devices establishing an encryption tunnel, one of the two shall be configured to be the Key Server by setting its Key Server value to 0 (zero). The other MACsec Device shall have its Key Server value set to 1. If a Central Management Site is part of the MSC Solution, it shall be the Key Server.	T=O	
MSC-MD-7	MACsec Devices shall enable data delay protection for MACsec Key Agreement (MKA).	T=O	
MSC-MD-8	MACsec Devices shall have an MKA Lifetime Timeout limit set to 6.0 seconds and Hello Timeout limit set to 2.0 seconds.	T=O	

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-MD-9	MACsec Devices shall 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 shall 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, shall be physically protected to the highest classification of the MACsec Device's CAK.	T=O	
MSC-MD-12	MACsec Devices shall 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 shall be considered a Solution Component when satisfying requirements in Section 11.1.	T=O	

11.4 Additional Requirements for Inner Encryption Components

Additional requirements for Inner Encryption Components are identified in Table 10.

Table 10. Additional Requirements for Inner Encryption Components (IR)

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-IR-1	The Inner VPN Gateway shall use ESP Tunnel mode IPsec, or ESP Transport mode IPsec using an associated IP tunneling protocol (e.g., Transport Mode IPsec with GRE).	T=O	
MSC-IR-2	Sizes for packets or frames leaving the external interface of the Inner Encryption Component shall be configured to reduce fragmentation and impact performance. This requires proper configuration of the Maximum Transmission Unit (MTU) (for IPv4 or MACsec) or Path MTU (PMTU) (for IPv6) and should consider Black network and Outer Encryption Component MTU/PMTU values to achieve this.	O	None
MSC-IR-3	The Inner Encryption Component shall not allow any packets received on an interface connected to a Red network to bypass encryption and be forwarded out through an interface connected to a Gray network.	T	MSC-IR-4

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-IR-4	The Inner Encryption Component shall use Mandatory Access Control policy to not allow any packets received on an interface connected to a Red network to bypass encryption and be forwarded out through an interface connected to a Gray network.	O	MSC-IR-3
MSC-IR-5	The Inner Encryption Component shall not allow any packets received on an interface connected to a Gray network to bypass decryption and be forwarded out through an interface connected to a Red network.	T	MSC-IR-6
MSC-IR-6	The Inner Encryption Component shall use Mandatory Access Control policy to not allow any packets received on an interface connected to a Gray network to bypass decryption and be forwarded out through an interface connected to a Red network.	O	MSC-IR-5
MSC-IR-7	The Inner Encryption Component shall not permit split-tunneling.	T=O	

11.5 Additional Requirements for Outer Encryption Components

Additional requirements for Outer Encryption Components are identified Table 11.

Table 11. Additional Requirements for Outer Encryption Components (OR)

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-OR-1	Outer VPN Gateways shall use ESP Tunnel mode IPsec.	T=O	
MSC-OR-2	Outer Encryption Components shall not allow any packets received on an interface connected to a Gray network to bypass encryption and be forwarded out through an interface connected to a Black network.	T	MSC-OR-3
MSC-OR-3	Outer Encryption Components shall use Mandatory Access Control policy to not allow any packets received on an interface connected to a Gray network to bypass encryption and be forwarded out through an interface connected to a Black network.	O	MSC-OR-2
MSC-OR-4	All traffic received by Outer Encryption Components on an interface connected to a Gray network, with the exception of control plane traffic, shall have already been encrypted once.	T=O	
MSC-OR-5	Outer Encryption Components shall not allow any packets received on an interface connected to a Black network to bypass decryption.	T	MSC-OR-6

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-OR-6	Outer Encryption Components shall 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 shall not permit split-tunneling.	T=O	
MSC-OR-8	Outer Encryption Components shall not use routing protocols (e.g., OSPF, BGP).	T=O	

11.6 PORT FILTERING REQUIREMENTS FOR SOLUTION COMPONENTS

Requirements for port filtering for Solution Components are identified in Table 12.

Table 12. Port Filtering (PF) Requirements for Solution Components

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-PF-1	All Solution Components shall have all network interfaces restricted to the smallest address ranges, ports, and protocols possible.	T=O	
MSC-PF-2	All Solution Components shall 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 shall be applied to both inbound and outbound traffic, such that only IKE, ESP, and control plane protocols (as defined in this CP) approved by organization-defined policy are allowed.	T=O	
MSC-PF-4	For all Outer MACsec Device interfaces connected to a Black network, traffic filtering rules shall be applied to both inbound and outbound traffic, such that only MACsec Protocol Data Units (MPDUs) and control plane protocols (as defined in this CP) approved by organization-defined policy are allowed.	T=O	
MSC-PF-5	For all Inner Encryption Component interfaces connected to a Gray network, traffic filtering rules shall 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) shall be blocked.	T	MSC-PF-7

Req. #	Requirement Description	Threshold / Objective	Alternative
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) shall be disabled.	O	MSC-PF-6
MSC-PF-8	Management plane traffic shall only be initiated from the Gray Administration Workstation with the exception of logging or authentication traffic that may be initiated from Outer Encryption Components.	T=O	
MSC-PF-9	Multicast messages received on external interfaces of Outer Encryption Components shall be dropped.	T=O	
MSC-PF-10	For solutions using IPv4, Outer VPN Gateways using IPsec shall drop all packets that use IP options.	O	
MSC-PF-11	For solutions using IPv4, each VPN Gateway shall 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 shall 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 shall allow IKE and IPsec, or MKA and MACsec traffic, as appropriate, that is between two Inner Encryption Components protecting networks of the same security level or that is being used for management of the Gray network.	T=O	
MSC-PF-14	The Gray network interfaces of Outer VPN Gateways shall allow HTTP traffic between Inner VPN Gateways and Inner CDPs/OCSP Responders.	T	MSC-PF-15 and MSC-PF-16
MSC-PF-15	The Gray network interfaces of Outer VPN Gateways shall allow HTTP GET and OCSP requests from Inner VPN Gateways to Inner CDPs and OCSP Responders, respectively, for the Uniform Resource Locator (URL) of the CRL or OCSP response needed by the Inner VPN Gateway, and block all other HTTP requests.	O	MSC-PF-14
MSC-PF-16	The Gray network interfaces of Outer VPN Gateways shall allow HTTP responses from Inner CDPs/OCSP Responders to Inner VPN Gateways that contain a well-formed CRL per IETF RFC 5280 or a well-formed OCSP response per IETF RFC 6960, and block all other HTTP responses.	O	MSC-PF-14

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-PF-17	The Gray network interfaces of Outer Encryption Components shall 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 shall 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 shall 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 shall deny all traffic that is not explicitly allowed by requirements MSC-PF-8, MSC-PF- 13, MSC-PF-14, MSC-PF-15, MSC-PF-16, or MSC-PF-19.	T=O	
MSC-PF-21	CDPs/OCSP Responders shall only allow inbound and outbound HTTP traffic per requirements MSC-PF-14, MSC-PF-15, and MSC-PF-16.	T=O	
MSC-PF-22	If an Outer Firewall is required, for all Outer Firewall interfaces, traffic filtering rules shall be applied to both inbound and outbound traffic, such that only IKE, ESP, MKA, MACsec and control plane protocols (as defined in this CP) approved by organization-defined policy are allowed.	T=O	
MSC-PF-23	If a Gray Firewall is required, the Gray Firewall shall permit IKE, IPsec, MKA and MACsec traffic between two Inner Encryption Components protecting networks of the same security level.	T=O	
MSC-PF-24	If a Gray Firewall is required, the Gray Firewall shall allow HTTP traffic between Inner VPN Gateways and Inner CDP/OCSP Responder.	T	MSC-PF-25 and MSC-PF-26
MSC-PF-25	If a Gray Firewall is required, the Gray Firewall shall allow HTTP GET and OCSP requests from Inner VPN Gateways to Inner CDPs/OCSP Responders for the URL of the CRL or OCSP response needed by the Inner VPN Gateway, and block all other HTTP requests.	O	MSC-PF-24

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-PF-26	If a Gray Firewall is required, the Gray Firewalls shall allow HTTP responses from Inner CDPs/OCSP Responders to Inner VPN Gateways that contain a well-formed CRL per IETF RFC 5280 or well-formed OCSP response per IETF RFC 6960, and block all other HTTP responses.	O	MSC-PF-24
MSC-PF-27	If a Gray Firewall is required, the Gray Firewall shall 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 shall 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 shall 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 shall allow control plane traffic (e.g., NTP, DHCP, and DNS).	T=O	
MSC-PF-31	If a Gray Firewall is required, the Gray Firewall shall deny all traffic that is not explicitly allowed by requirements MSC-PF-23, MSC-PF- 24, MSC-PF-25, MSC-PF-26, MSC-PF-27 or MSC-PF-30.	T=O	

11.7 Configuration Change Detection Requirements

Table 13 defines the requirements for Configuration Change Detection.

Table 13. Configuration Change Detection (CM) Requirements

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

11.8 Device Management Requirements

Table 14 defines the requirements for Device Management.

Table 14. Device Management (DM) Requirements

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-DM-1	Administration Workstations shall be dedicated for the purposes given in this CP and shall be physically separated from workstations used to manage non-CSfC solutions.	T=O	
MSC-DM-2	Administration Workstations shall physically reside within a protected facility where CSfC solution(s) are managed.	T=O	
MSC-DM-3	Administration Workstations shall connect from an internal port. Specifically, the Inner Encryption Component shall be managed from the Red network, and the Outer Encryption Component and Gray Firewall, if present, shall be managed from the Gray network.	T=O	
MSC-DM-4	A separate LAN or VLAN on the Red network shall 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 shall 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 shall 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 shall 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 shall be performed from an Administration Workstation remotely using an NSA-approved solution (e.g., CP or Type 1 encryptor), or by managing the Solution Components locally.	T=O	
MSC-DM-9	Security Administrators shall authenticate to Solution Components before performing administrative functions.	T	MSC-DM-10

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-DM-10	Security Administrators shall authenticate to Solution Components with CNSA Suite compliant certificates before performing administrative functions remotely.	O	MSC-DM-9
MSC-DM-11	The MSC Solution Owner shall identify the authorized Security Administrators to initiate certificate requests.	T=O	
MSC-DM-12	Authorized Security Administrators shall 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 shall be enforced by either procedural or technical means.	O	None
MSC-DM-14	Administration Workstations that interact with the Certificate Authority for the Outer VPN Gateways must be located on the Gray network.	T=O	
MSC-DM-15	VPN Gateways shall obtain certificates through the use of Public Key Cryptographic Standard (PKCS) #10 and PKCS#7 requests.	T=O	
MSC-DM-16	Devices shall use EST as detailed in IETF RFC 7030 for certificate management.	O	None
MSC-DM-17	The same Administration Workstation shall not be used to manage Inner Encryption Components and Outer Encryption Components.	T=O	
MSC-DM-18	If SIEMs are used in the solution, Outer Encryption Components and Solution Components within the Gray network shall forward log entries to a SIEM on the Gray management network (or SIEM in the Red network if using a CDS) within 10 minutes of the event's occurrence.	T=O	
MSC-DM-19	If SIEMS are used in the solution, Inner Encryption Components and Solution Components within the Red network shall forward log entries to a SIEM on the Red management network within 10 minutes of the event's occurrence.	T=O	
MSC-DM-20	If SIEMS are used in the solution, all logs forwarded to a SIEM on the Gray management network shall be encrypted using SSHv2, IPsec, MACsec, or TLS 1.2 or later.	O	None
MSC-DM-21	If SIEMS are used in the solution, all logs forwarded to a SIEM on a Red management network shall be encrypted using SSHv2, IPsec, MACsec, or TLS 1.2 or later.	O	None

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-DM-22	Outer Encryption Components shall only be managed by Security Administrators cleared to at least the highest level of classification of each Red network supported by the Outer Encryption Component at the physical site the Outer Encryption Component is located.	T=O	

11.9 CONTINUOUS MONITORING REQUIREMENTS

Continuous monitoring requirements are identified in Table 15.

Table 15. Requirements for Continuous Monitoring (MR)

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

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-MR-5	If the Black transport network is the Public Internet, an IPS shall be deployed in at least two of the following locations: • Between the Outer Firewall and the Outer Encryption Component (M1). • Between the Outer Encryption Component and Gray Firewall, if present, or the Inner Encryption Component (M2). • Between the Inner Encryption Component and Inner Firewall, if present, or the Red network (M3).	O	MSC-MR-3 MSC-MR-4 MSC-MR-6
MSC-MR-6	If the Black transport network is the Public Internet, an IPS shall be deployed in all of the following locations: • Between the Outer Firewall and the Outer Encryption Component (M1). • Between the Outer Encryption Component and Gray Firewall, if present, or the Inner Encryption Component (M2). • Between the Inner Encryption Component and Inner Firewall, if present, or the Red network (M3).	O	MSC-MR-3 MSC-MR-4 MSC-MR-5
MSC-MR-7	If IDSs are part of the solution, each IDS shall be configured to provide a dashboard or send alerts to the Security Administrator.	T	MSC-MR-8
MSC-MR-8	If IPSs are part of the solution, each IPS shall be configured to block malicious traffic flows and alert the Security Administrator.	O	MSC-MR-7
MSC-MR-9	If IDSs are part of the solution, each IDS shall be configured with rules that generate alerts upon detection of any unauthorized destination IP addresses.	T	MSC-MR-10
MSC-MR-10	If IPSs are part of the solution, each IPS shall be configured with rules that block and generate alerts upon detection of any unauthorized destination IP addresses.	O	MSC-MR-9
MSC-MR-11	If IDSs are part of the solution, each IDS shall be configured with rules that generate alerts upon detection of any unauthorized source IP addresses.	T	MSC-MR-12
MSC-MR-12	If IPSs are part of the solution, each IPS shall be configured with rules that block and generate alerts upon detection of any unauthorized source IP addresses.	O	MSC-MR-11

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-MR-13	If SIEMs are part of the solution, a SIEM component shall be placed within the Gray network unless devices are configured to push events to a Red network SIEM through an approved CDS.	T=O	
MSC-MR-14	If SIEMs are part of the solution, the SIEM shall be configured to send alerts to the Security Administrator when anomalous behavior is detected (e.g., blocked packets from the Outer Encryption Component or Gray Firewall).	T=O	
MSC-MR-15	If a Gray SIEM is part of the solution, the Gray SIEM shall collect logs from the Outer Encryption Component, Gray Firewall, and any components located within the Gray Management Services.	T=O	
MSC-MR-16	If a Gray SIEM is part of the solution, the Gray SIEM shall maintain an up-to-date table of Certificate Common Name and assigned IP address used for the Outer VPN Gateway.	T=O	
MSC-MR-17	If a Gray SIEM is part of the solution, the Gray SIEM shall provide a dashboard or alert for sites attempting to establish a connection with the Outer Encryption Component using misconfigured settings.	T=O	
MSC-MR-18	If a Gray SIEM is part of the solution, the Gray SIEM shall provide an alert or dashboard for three or more invalid login attempts in a 24-hour period to the Outer Encryption Component and Gray Firewall, if present.	T=O	
MSC-MR-19	If a Gray SIEM is part of the solution, the Gray SIEM shall provide an alert or dashboard of privilege escalations on the Outer Encryption Component and Gray Firewall, if present.	T=O	
MSC-MR-20	If a Gray SIEM is part of the solution, the Gray SIEM shall provide an alert or dashboard of configuration changes to the Outer Encryption Component and Gray Firewall, if present.	T=O	
MSC-MR-21	If a Gray SIEM is part of the solution, the Gray SIEM shall provide an alert or dashboard of new accounts created on the Outer Encryption Component and Gray Firewall, if present.	T=O	
MSC-MR-22	If a Gray SIEM is part of the solution, the Gray SIEM shall provide an alert or dashboard for attempted connections to the Outer Encryption Component that use invalid certificates or keys.	T=O	

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

11.10 AUDITING REQUIREMENTS

Auditing requirements for the MSC Solution are identified in Table 16.

Table 16. Auditing (AU) Requirements

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-AU-1	Encryption Components shall log establishment of an encryption tunnel.	T=O	
MSC-AU-2	Encryption Components shall log termination of an encryption tunnel.	T=O	
MSC-AU-3	Solution Components shall log all actions performed on the audit log (e.g., off-loading, deletion).	T=O	
MSC-AU-4	Solution Components shall log all actions involving identification and authentication.	T=O	

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-AU-5	Solution Components shall log attempts to perform an unauthorized action (e.g., read, write, execute, delete) on an object.	T=O	
MSC-AU-6	Solution Components shall log all actions performed by a user with super-user or administrator privileges.	T=O	
MSC-AU-7	Solution Components shall log escalation of user privileges.	T=O	
MSC-AU-8	Solution Components shall log generation, loading, and revocation of certificates.	T=O	
MSC-AU-9	Solution Components shall log changes to time.	T=O	
MSC-AU-10	Solution Components shall log when packets received on Gray network interfaces are dropped or blocked.	T=O	
MSC-AU-11	Solution Components shall log the results of built-in self-tests.	T=O	
MSC-AU-12	MACsec Devices shall log the installation of a CAK into the MACsec Device, including all subsequent installations of new CAKs (i.e., CAK rekey).	T=O	
MSC-AU-13	MACsec Devices shall log creation and updates of SAKs.	T=O	
MSC-AU-14	MACsec Devices shall log administrator lockout due to excessive authentication failures.	T=O	
MSC-AU-15	MACsec Devices shall log detected replay attempts.	T=O	
MSC-AU-16	Each log entry shall record the date and time of the event.	T=O	
MSC-AU-17	Each log entry shall include the identifier of the event.	T=O	
MSC-AU-18	Each log entry shall record the type of event.	T=O	
MSC-AU-19	Each log entry shall record the success or failure of the event to include failure code, when available.	T=O	
MSC-AU-20	Each log entry shall record the subject identity.	T=O	
MSC-AU-21	Each log entry shall record the source address for network-based events.	T=O	
MSC-AU-22	Each log entry shall record the user and, for role-based events, role identity, where applicable.	T=O	
MSC-AU-23	VPN Gateways shall log the failure to download the CRL from a CDP.	T=O	
MSC-AU-24	VPN Gateways shall log if the version of the CRL downloaded from a CDP is older than the current cached CRL.	T=O	
MSC-AU-25	VPN Gateways shall log if signature validation of the CRL downloaded from a CDP fails.	T=O	
MSC-AU-26	Auditors shall compare and analyze collected network flow data against the established baseline on at least a daily basis.	T=O	

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-AU-27	Locally-run CAs shall comply with the audit and archival requirements defined in IETF RFC 3647 Sections 4.5.4 and 4.5.5, respectively.	T=O	
MSC-AU-28	Locally-run CAs shall comply with periodic audit and assessment requirements defined in IETF RFC 3647 Section 4.8.	T=O	
MSC-AU-29	Audits and assessments for a CA shall be performed by personnel who are knowledgeable in the CA's operations, as well as the CA's Certificate Policy and CPS requirements and processes, respectively.	T=O	
MSC-AU-30	KGSs that deliver CAK Management Services for MSC Solutions are to comply with audit and assessment requirements defined by the customer's operational security doctrine and enterprise KGS (if applicable).	T=O	
MSC-AU-31	Audits and assessments for a KGS are to be performed by personnel who are knowledgeable in the KGS's operations, as well as the KGS's audit requirements and processes, respectively.	T=O	

11.11 Key Management Requirements

This section details key management requirements for the MSC Solution. General requirements are identified, followed by requirements specific to certificates and CAKs.

11.11.1 General Requirements

General key management requirements are identified in Table 17.

Table 17. General Key Management (KM) Requirements

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-1	Certificate Management Services for the inner tunnel shall be provided through the Red network.	T=O	
MSC-KM-2	Certificate Management Services for the outer tunnel shall be provided through either the Gray network or Red network.	T=O	
MSC-KM-3	CAK management services (enterprise or locally-owned) shall be provided through the local Red network.	T=O	

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-4	If the Certificate and CAK Management Services operate at the same security level as a Red network, a non-CDS Controlled Interface shall be used to control information flow between the Certificate and CAK Management Services and the Red network.	T=O	
MSC-KM-5	If the Certificate and CAK Management Services operate at a different security level than a Red network or Gray network, a Controlled Interface that is also a CDS shall be used to control information flow between the Certificate and CAK Management Services and the Red network or Gray network.	T=O	
MSC-KM-6	If multiple Red enclaves exist in the MSC Solution and the Outer CA resides in the Red network, the Outer CA must reside in the Red network with the highest security level.	T=O	
MSC-KM-7	All device certificates issued by the Outer and Inner CAs, and their corresponding private keys, shall be treated as CUI (or higher as determined by the AO).	T=O	
MSC-KM-8	All certificates issued by the Outer and Inner CAs for the MSC Solution shall be NPE certificates.	T=O	
MSC-KM-9	Authentication certificates issued by the Outer and Inner CAs for the MSC Solution shall be X.509 v3 certificates as defined in IETF RFC 5280.	T=O	
MSC-KM-10	CAKs issued to Outer Encryption Components are CUI, but they are physically protected as if they were classified to the level of the Red network.	T=O	
MSC-KM-11	CAKs issued to Inner Encryption Components are classified to the level of the Red network.	T=O	
MSC-KM-12	Enterprise Certificate and CAK Management Services shall be used to the greatest extent possible.	O	None
MSC-KM-13	The key sizes and algorithms for CA certificates and authentication certificates issued to VPN Gateways and Administrative Device Components shall be as illustrated in Table 6.	T=O	
MSC-KM-14	All public/private key pairs and certificates for VPN Gateways shall be used for authentication only.	T=O	
MSC-KM-15	All CAKs generated by or issued to an Encryption Component are to be used in strict accordance with approved protocols identified in this CP.	T=O	
MSC-KM-16	CAs shall not escrow private keys.	T=O	
MSC-KM-17	Outer and Inner CAs shall not have access to private keys used in the Solution Components.	T=O	

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-18	A locally-run CA supporting an Inner VPN Gateway shall be physically separated from a locally-run CA supporting an Outer VPN Gateway.	T=O	
MSC-KM-19	The Outer and Inner CAs shall each operate in compliance with a Certificate Policy and CPS that are formatted in accordance with IETF RFC 3647.	T=O	
MSC-KM-20	KGSs and the MSC Solution being supported shall operate in compliance with an NSA-approved KMP.	T=O	
MSC-KM-21	MSC Solutions using CAKs are to obtain an IAD MD-110 waiver if the CAKs exist in red form during any part of the CAK life-cycle management process.	T=O	
MSC-KM-22	CAs shall run anti-virus software.	T=O	
MSC-KM-23	Authentication certificate profiles for the Outer and Inner CAs for the MSC Solution shall comply with IETF RFC 5280.	T=O	
MSC-KM-24	Private keys of on-line, locally-run Outer and Inner CAs shall be protected from tampering and unauthorized use by a FIPS 140-2 Level 2 validated cryptographic module (e.g., Hardware Security Module). On-line means the CA is powered on and network accessible.	T=O	
MSC-KM-25	Copies of CA private keys shall only be made using AO-approved procedures to support CA continuity of operations and disaster recovery (e.g., backups of private keys).	T=O	

11.11.2 CERTIFICATE ISSUANCE REQUIREMENTS

Requirements for issuing certificates are provided in Table 18.

Table 18. Certificate Issuance Requirements

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-26	Gray and Red Management Services Components shall be initially keyed and loaded with certificates within a physical environment certified to protect the highest classification of the MSC Solution.	T=O	
MSC-KM-27	Outer and Inner CAs shall use PKCS#10 and PKCS#7 to issue authentication certificates to VPN Gateways, and Gray and Red Management Services Components.	T	MSC-KM-28
MSC-KM-28	Outer and Inner CAs shall use IETF RFC 7030 EST to issue authentication certificates to VPN Gateways, and Gray and Red Management Services Components.	O	MSC-KM-27

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-29	Certificate signing requests shall be submitted to the CA by an authorized Registration Authority (RA) and in accordance with the CA's Certificate Policy and CPS. The MSC Solution Owner shall identify the authorized Registration Authorities.	T=O	
MSC-KM-30	Authentication of RAs shall be enforced by technical means (e.g., enterprise authentication tokens).	O	None
MSC-KM-31	Outer and Inner CAs shall issue certificates in accordance with their Certificate Policies and CPSs.	T=O	
MSC-KM-32	Certificate Policies and CPSs for non-Enterprise, locally run CAs shall ensure the CAs issue certificates within a defined and limited name space and assert: • Unique Distinguished Names (DNs) • Appropriate key usages • A registered policy OID	T=O	
MSC-KM-33	If a CDP is used in the MSC Solution, the Outer and/or Inner CAs shall assert at least one CDP URL in certificates issued to VPN Gateways, and Gray and/or Red Management Services Components. The CDP URL specifies the location of the CA's CRLs.	T=O	
MSC-KM-34	The key validity period for certificates issued by non-Enterprise, locally-run CAs to MSC Solution Components shall not exceed 36 months.	T=O	
MSC-KM-35	Inner CAs shall only issue certificates to Inner VPN Gateways and Red Network Components of MSC Solutions.	T=O	
MSC-KM-36	Outer CAs shall only issue certificates to Outer VPN Gateways and Gray Network Components of MSC Solutions.	T=O	
MSC-KM-37	The Inner VPN Gateway shall only trust the Inner CA used for its network.	T=O	
MSC-KM-38	The Outer VPN Gateway shall only trust the Outer CA used within the solution.	T=O	
MSC-KM-39	New certificates shall be issued as needed in accordance with local policy.	T=O	

11.11.3 CERTIFICATE RENEWAL AND REKEY REQUIREMENTS

Requirements for renewing and rekeying certificates are provided in Table 19.

Table 19. Certificate Renewal and Rekey Requirements

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-40	Certificate renewal or rekey shall occur prior to a certificate expiring.	T=O	
MSC-KM-41	If rekeying of the VPN Gateways is not completed prior to expiration of keys, they shall be rekeyed through the same process as initial keying.	T=O	
MSC-KM-42	Certificate renewal or rekey shall be performed in accordance with the CA's Certificate Policy and CPS.	T=O	
MSC-KM-43	Outer and Inner CAs shall issue renewed/rekeyed authentication certificates to Solution Components using PKCS#10 and PKCS#7.	T	MSC-KM-44
MSC-KM-44	Outer and Inner CAs shall issue renewed/rekeyed authentication certificates to Solution Components using EST (IETF RFC 7030).	O	MSC-KM-43

11.11.4 CERTIFICATE REVOCATION REQUIREMENTS

Requirements for revoking certificates are provided in Table 20.

Table 20. Certificate Revocation Requirements

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-45	CRL profiles shall comply with IETF RFC 5280.	T=O	
MSC-KM-46	Outer and Inner CAs shall revoke a certificate issued to Solution Components when the binding between the subject information and public key within the certificate issued is no longer considered valid.	T=O	
MSC-KM-47	Outer and Inner CAs shall make certificate revocation information available in the form of CRLs signed by the CAs.	T=O	
MSC-KM-48	Procedures for requesting certificate revocation shall comply with the CA's Certificate Policy and CPS.	T=O	

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-49	Certificate Policies and CPSs for non-Enterprise, locally-run CAs shall ensure revocation procedures address the following: • Removal of a revoked infrastructure device (e.g., VPN Gateway) from the network. • Re-establishment of a Solution Component whose certificate was revoked. • Revocation of an authentication certificate if simultaneous use of the certificate is detected from different IP addresses.	T=O	
MSC-KM-50	Enterprise CAs shall create and publish CRLs in accordance with the Enterprise CAs' Certificate Policies and CPSs.	T=O	
MSC-KM-51	Non-enterprise, locally-run CAs shall publish new CRLs at least once every 28 days.	T=O	
MSC-KM-52	Non-enterprise, locally-run CAs shall create a new CRL within one hour of a certificate being revoked.	T=O	
MSC-KM-53	Solution Components shall have access to new certificate revocation information within 24 hours of the CA creating a new CRL.	T=O	
MSC-KM-54	CRLs shall expire no later than 31 days after their issue date.	T=O	
MSC-KM-55	Non-enterprise, locally-run CAs shall ensure that newly created CRLs are published at least 7 days prior to the expiration of the current CRLs.	T=O	
MSC-KM-56	The MSC Solution shall provide certificate revocation status information via an OCSP Responder on the Red and Gray network that is compliant with IETF RFC 6960.	O	None
MSC-KM-57	Certificate revocation status messages delivered by an Outer/Inner OCSP Responder shall be digitally signed and compliant with IETF RFC 6960. The OCSP Responder generates the digitally-signed OCSP response using a private key that corresponds to a device certificate issued by the Outer/Inner CA.	O	None
MSC-KM-58	If OCSP Responders are used in the MSC Solution, Inner CAs shall assert the Authority Information Access certificate extension and include the list of URLs identifying the Inner OCSP Responders from which Inner VPN Gateways can request and receive OCSP revocation status responses.	T=O	

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-59	If OCSP Responders are used in the MSC Solution, Outer CAs shall assert the Authority Information Access certificate extension and include the list of URLs identifying the Outer OCSP Responders from which Outer VPN Gateways can request and receive OCSP revocation status responses.	T=O	
MSC-KM-60	Outer and Inner CAs shall make CRLs available to authorized CDPs, so that the CRLs can be accessed by Solution Components.	T=O	
MSC-KM-61	CRLs hosted by CDPs shall be compliant with IETF RFC 5280.	T=O	
MSC-KM-62	CRLs hosted on Inner CDPs shall be signed by the associated Inner CA.	T=O	
MSC-KM-63	CRLs hosted on Outer CDPs shall be signed by the associated Outer CA.	T=O	
MSC-KM-64	CDPs and OCSP Responders shall only issue CRLs and OCSP responses, respectively, over port 80 (HTTP).	T=O	
MSC-KM-65	CRLs shall be transferred via an AO-approved one-way transfer mechanism from Inner CAs to associated Inner CDP servers and Inner OCSP Responders.	T=O	
MSC-KM-66	CRLs shall be transferred via an AO-approved one-way transfer mechanism from Outer CAs to associated Outer CDP servers and OCSP Responders.	T=O	
MSC-KM-67	Newly issued CRLs shall be transferred to CDP servers and OCSP Responders at least 4 days prior to the expiration of the current CRLs.	T=O	
MSC-KM-68	VPN Gateways shall attempt to download the latest CRL from a CDP at least once every 24 hours.	T=O	
MSC-KM-69	If whitelists are used for authentication, the whitelist shall be validated against the latest CRL at least once every 24 hours.	T=O	
MSC-KM-70	CDPs and OCSP Responders shall only accept traffic on port 80 and ports used for remote management traffic.	T=O	
MSC-KM-71	CDPs and OCSP Responders shall only accept connections from known VPN Gateway or Administration Workstation addresses or address ranges.	T=O	
MSC-KM-72	If an integrity check of a CRL or OCSP response received from a CDP or OCSP response fails, then VPN Gateways shall use the current cached CRL or OCSP response.	T=O	

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-73	If a CDP or OCSP Responder is offline or contains an invalid CRL or OCSP response, then Inner and Outer VPN Gateway CRLs and OCSP responses shall be manually updated prior to the expiration of the current cached CRLs or OCSP responses.	T=O	
MSC-KM-74	Inner CAs shall set the CDP extension of the certificates it generates for the MSC Solution to the list of URLs hosted by Inner CDPs from which Inner VPN Gateways can download the CRL.	T=O	
MSC-KM-75	Outer CAs shall set the CDP extension of the certificates it generates for the MSC Solution to the list of URLs hosted by Outer CDPs from which Outer VPN Gateways can download the CRL.	T=O	

11.11.5 CAK Generation and Distribution Requirements

Requirements for generating and distributing CAKs are provided in Table 21.

Table 21. CAK Generation and Distribution Requirements

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-76	Generation of CAKs and their associated CKNs shall be performed by an NSA-approved KGS. NSA-approved means: a) a component from the CSfC Approved Products List; or b) a component approved for the CSfC solution by the Deputy National Manager for National Security Systems; or c) an already approved enterprise service.	T=O	
MSC-KM-77	Centralized generation, distribution and management of CAKs and their associated CKNs for Outer and Inner MACsec Devices shall be performed by a dedicated KGS located in, or accessed through, the Red network.	T=O	
MSC-KM-78	CAKs issued to Outer MACsec Devices shall be transferred from the Red network to the Gray network using an AO-approved transfer method.	T=O	
MSC-KM-79	CAKs shall be 256 bits.	T=O	
MSC-KM-80	CAKs shall not be exposed in plaintext form until they are ready to be installed on MACsec Devices. Installation of CAKs and their associated CKNs may be performed via file transfer or text input.	T=O	

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-81	CAKs shall be protected from unauthorized disclosure when they are distributed outside a controlled boundary or over unprotected communications channels through appropriate two-person control manual distribution procedures and methods, as defined in the KMP.	T	MSC-KM-82
MSC-KM-82	CAKs shall be protected from unauthorized disclosure when they are distributed outside a controlled boundary or over unprotected communications channels through the use of pre-placed symmetric CEK or an approved key distribution protocol.	O	MSC-KM-81
MSC-KM-83	CEKs shall be 256 bits.	T=O	
MSC-KM-84	The classification of pre-placed CEKs shall be the same as the classification of the CAKs that are encrypted with the pre-placed CEKs.	T=O	

11.11.6 CAK USAGE REQUIREMENTS

Requirements for using CAKs are provided in Table 22.

Table 22. CAK Usage Requirements

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-85	CAKs are to only be used with the MACsec protocol.	T=O	
MSC-KM-86	CAKs and CEKs are to be stored within an approved cryptographic boundary within a Solution Component.	T=O	
MSC-KM-87	CAKs and CEKs exported from a Solution Component are to be protected from unauthorized disclosure through two-person control manual procedure protection methods.	T	MSC-KM-88
MSC-KM-88	CAKs and CEKs exported from a Solution Component are to be protected from unauthorized disclosure through encryption.	O	MSC-KM-87
MSC-KM-89	A compromised CAK/CEK is to never be used in the MSC Solution.	T=O	

11.11.7 CAK UPDATE (REKEY) REQUIREMENTS

Requirements for updating (rekeying) CAKs are provided in Table 23.

Table 23. CAK Update (Rekey) Requirements

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-90	The same CAK shall be used in only one pair of MACsec Devices that are establishing an encryption tunnel.	T=O	
MSC-KM-91	CAKs and their associated CKNs shall be updated (rekeyed) every 30 days, or as defined by the KMP.	T=O	
MSC-KM-92	CEKs are to be updated (rekeyed) every 90 days, or as defined by the KMP.	T=O	

11.11.8 CAK COMPROMISE RECOVERY REQUIREMENTS

Requirements for recovering from compromised CAKs are provided in Table 24.

Table 24. CAK Compromise Recovery Requirements

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-93	The KMP shall document the CAK/CEK compromise recovery process, to include: • Removal of a compromised infrastructure device (e.g., MACsec Devices) from the network, and • Re-establishing a MACsec Device after its CAK is compromised.	T=O	
MSC-KM-94	Accounting procedures need to support CAK and CEK compromise recovery to ensure all copies of compromised CAKs and CEKs are identified and updated (rekeyed).	T=O	
MSC-KM-95	CAKs/CEKs are to be updated (rekeyed) immediately if they are considered compromised.	T=O	
MSC-KM-96	If a CAK/CEK is considered compromised, a compromise notification shall be submitted to the KGS along with a request to update (rekey) the CAK/CEK.	T=O	
MSC-KM-97	If a CAK/CEK is compromised, the procedures for CAK/CEK compromise reporting, as defined by the applicable KMP, shall be followed.	T=O	
MSC-KM-98	If a compromised device is to be reused, that device must go through the initial CAK issuance process.	T=O	

12 REQUIREMENTS FOR SOLUTION OPERATION, MAINTENANCE, AND HANDLING

12.1 REQUIREMENTS FOR THE USE AND HANDLING OF SOLUTIONS

The requirements in Table 25 shall be followed regarding the use and handling of the solution.

Table 25. Requirements for the Use and Handling of Solutions

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-GD-1	All Solution Components, with the exception of the Outer Firewall (if present), shall 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 shall have physical access to the Solution Components.	T=O	
MSC-GD-3	All components of the solution shall be disposed of as classified devices, unless declassified using AO-approved procedures.	T=O	
MSC-GD-4	Acquisition and procurement documentation shall 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 shall allow, and fully cooperate with, NSA or its authorized agent to perform an Information Assurance (IA) compliance audit (including, but not limited to, inspection, testing, observation, and interviewing) of the solution implementation to ensure it meets the latest version of this CP.	T=O	
MSC-GD-6	The AO will ensure that a compliance audit shall 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 shall be provided to and reviewed by the AO.	T=O	
MSC-GD-8	Customers interested in registering their solution against this CP shall register with NSA and receive approval prior to operating the solution.	T=O	
MSC-GD-9	The implementing organization shall complete and submit an MSC CP requirements compliance matrix to their respective AO.	T=O	

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-GD-10	Registration and re-registration against this CP shall include submission of CP registration forms and compliance matrix to NSA.	T=O	
MSC-GD-11	When a new approved version of the MSC CP is published by NSA, the AO shall ensure compliance against this new CP within 6 months.	T=O	
MSC-GD-12	Solution implementation information that was provided to NSA during solution registration shall 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 shall be maintained for a minimum of 1 year.	T=O	
MSC-GD-14	The amount of storage remaining for audit events shall 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 shall be off-loaded to a backup storage medium at least once a week.	T=O	
MSC-GD-16	The implementing organization shall 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 shall 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 shall 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 shall 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 shall 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 shall be used that comply with the requirements of the AO.	T=O	

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

12.2 Requirements for Incident Reporting

Table 26 lists requirements for reporting security incidents to NSA to be followed in the event that a Solution Owner identifies a security incident that affects the solution. These reporting requirements are intended to augment, not replace, any incident reporting procedures already in use within the Solution Owner's organization. It is critical that Security Administrators, Certification Authority Administrators (CAAs), KGSAs, and Auditors are familiar with maintaining the solution in accordance with this CP. Based on familiarity with the known-good configuration of the solution, personnel responsible for the operations and maintenance of the solution will be better equipped to identify reportable incidents.

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

Table 26 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 26. Incident Reporting Requirements (RP)

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-RP-1	Solution Owners shall report confirmed incidents meeting the criteria in MSC-RP-3 through MSC-RP-14 within 24 hours of detection via the Joint Incident Management System (JIMS) or contacting NSA as specified in the CSfC Registration Letter issued for the solution.	T=O	

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-RP-2	At a minimum, the organization shall provide the following information when reporting security incidents: • CSfC Registration Number • Primary POC name, phone, email • Alternate POC name, phone, email • Security level of affected solution • Name of affected network(s) • Affected component(s) manufacturer/ vendor • Affected component(s) model number • Affected component(s) version number • Date and time of incident • Description of incident • Description of remediation activities • Is Technical Support from NSA requested? (Yes/No)	T=O	
MSC-RP-3	Solution Owners shall report a security failure in any of the CSfC Solution Components.	T=O	
MSC-RP-4	Solution Owners shall 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 shall report any malicious inbound and outbound traffic.	T=O	
MSC-RP-6	Solution Owners shall report any evidence of an unauthorized device/user gaining access to the classified network via the solution.	T=O	
MSC-RP-7	Solution Owners shall report if a Solution Component sends traffic with an unauthorized destination address.	T=O	
MSC-RP-8	Solution Owners shall report any malicious configuration changes to the components.	T=O	
MSC-RP-9	Solution Owners shall report any unauthorized escalation of privileges to any of the CSfC Solution Components.	T=O	
MSC-RP-10	Solution Owners shall 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 shall report any evidence of malicious physical tampering with Solution Components.	T=O	
MSC-RP-12	Solution Owners shall report any evidence that one or both layers of the solution failed to protect the data.	T=O	

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-RP-13	Solution Owners shall 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 shall report malicious discrepancies in the number of connections established by the Outer Encryption Component.	T=O	
MSC-RP-15	Solution Owners shall 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 shall be responsible for maintaining, monitoring, and controlling 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) Ensuring that the latest security-critical software patches and updates (such as Information Assurance Vulnerability Alerts (IAVAs)) are applied to each product.

2) Documenting and reporting security-related incidents to the appropriate authorities.

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

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

5) Ensuring 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 shall be responsible for maintaining, monitoring, and controlling all security functions for the CA products. CAA duties include, but are not limited to:

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

2) Maintaining and updating the CRL.

3) Provisioning and maintaining certificates in accordance with this CP for implementations that use them.

Key Generation Solution Administrator (KGSA) – The KGSA shall be responsible for maintaining, monitoring, and controlling all security functions for the KGS products. KGSA duties include, but are not limited to:

1) Administering the KGS, including authentication of all components requesting CAKs and CEKs.

2) Maintaining and updating the CAK and CEK revocation lists.

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

Auditor – The Auditor shall be responsible for reviewing 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) Reviewing, managing, controlling, and maintaining security audit log data.

2) Documenting and reporting 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) Acquiring the products that compose the solution.

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

3) Documenting, testing, and maintaining the solution.

4) Responding to incidents affecting the solution.

Additional policies related to the personnel that perform these roles in a MSC Solution are identified in Table 27.

Table 27. Role-Based Personnel Requirements

Req. #	Requirement Description	Threshold / Objective	Alternative
MSC-RB-1	The Security Administrators, CAAs, KGSAs, Auditors, and Integrators shall 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 shall be performed by different people.	T=O	
MSC-RB-3	All Security Administrators, CAAs, KGSAs, and Auditors shall meet local IA training requirements.	T=O	
MSC-RB-4	The CAA(s) for the inner tunnel shall 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 shall 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 shall periodically inspect the physical attributes of infrastructure hardware for signs of tampering or other unauthorized changes.	T=O	
MSC-RB-7	The Auditor shall review all logs specified in this CP at least once a day.	T=O	
MSC-RB-8	Security Administrators shall 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 shall be performed by individuals who were not involved in the development of the Certificate Policy and CPS, or integration of the MSC Solution.	T=O	
MSC-RB-10	Auditing of the KGS operations shall be performed by individuals who were not involved in the development of the KMP, or integration of the MSC Solution.	T=O	
MSC-RB-11	Mandatory Access Control policy shall 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 has a testing team develop a test plan and perform 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 for ensuring that all requirements from this CP have been properly implemented in accordance with this CP.
- The customer registers the solution with 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 will ensure that a compliance audit shall be conducted every year against the latest version of the MSC CP, and the results shall be provided to the AO.
- The AO will ensure 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 will ensure 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 will report 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 shall 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 shall 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 shall 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 shall be documented.

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

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

Table 28. Test (TR) Requirements

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

14.2 Risk Assessment

The Risk Assessment of the MSC Solution presented in this CP focuses on the types of attacks that are feasible against this solution and the mitigations that can be employed. Customers should contact their NSA External Engagement Representative to request this document, or visit the Secret Internet Protocol Router Network (SIPRNet) CSfC site for information. The process for obtaining the Risk Assessment is available on the SIPRNet CSfC website. The AO shall 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 shall register their solution with NSA prior to operational use. This registration will allow NSA to track where MSC Solutions are instantiated and to provide the AOs at those sites with appropriate information, including any significant vulnerabilities that may be discovered in components or high-level designs approved for these solutions. The CSfC solution registration process is available on the CSfC web page under the "Solution Registration" tab (https://www.nsa.gov/resources/everyone/csfc).

Solution registrations are valid for one year from the date the solution registration is approved, at which time customers are required to re-register their solution to continue using it. Approved CPs will be reviewed twice a year, or as events warrant. Registered users of this CP will be notified when an updated version is published. When a new version of this NSA-approved CP is published, customers will have six months 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.

Authorization (To Operate) – The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (NIST SP 800-37)

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)

Authorizing Official Designated Representative – An organizational official acting on behalf of an AO in carrying out and coordinating the required activities associated with security authorization. (NIST SP 800-37)

Authorization Package – A security package of documents consisting of the security control assessment that provides the AO with essential information needed to make a risk-based decision on whether to authorize operation of an information system or a designated set of common controls.

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 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]

Committee on National Security Systems Policy No. 15 (CNSSP-15) – Policy specifies which public standards may be used for cryptographic protocol and algorithm interoperability to protect NSS.

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.

Control Plane Protocol – A routing, signaling, or similar protocol whose endpoints are network infrastructure devices such as VPN Gateways or routers. Control plane protocols carry neither user data nor management traffic.

Controlled Unclassified Information (CUI) – Information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended. [CNSSI 4009]

CRL Distribution Point (CDP) – A web server that hosts a copy of a CRL issued by a CA for VPN Gateways to download.

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]

Data Plane Protocol – A protocol that carries the data being transferred through the solution.

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.

Management Plane Protocol – A protocol that carries either traffic between a system administrator and a component being managed, or log messages from a Solution Component to a log server or similar repository.

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.

APPENDIX B. ACRONYMS

Acronym	Definition
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
CSfC	Commercial Solutions for Classified
CUI	Controlled Unclassified Information
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DM	Device Management
DN	Distinguished Name
DNS	Domain Name System
DoS	Denial of Service
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EoMPLS	Ethernet over Multiprotocol Label Switching
ESP	Encapsulating Security Payload
EST	Enrollment Over Secure Transport
FIPS	Federal Information Processing Standards
GCM	Galois Counter Mode
GOTS	Government Off-the-Shelf
GRE	Generic Routing Encapsulation
HMAC	Host-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure

Acronym	Definition
IA	Information Assurance
IAD	Information Assurance Directorate
IAVA	Information Assurance Vulnerability Alerts
IC	Intelligence Community
ICMP	Internet Control Message Protocol
ID	Identification
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IS-IS	Intermediate System to Intermediate System
JIMS	Joint Incident Management System
KGS	Key Generation Solution
KGSA	Key Generation Solution Administrator
KM	Key Management
KMI	Key Management Infrastructure
KMP	Key Management Plan
L2TPv3	Layer 2 Tunneling Protocol Version 3
MACsec	Media Access Control Security
MGC	Management Client
MKA	MACsec Key Agreement
MLD	Multicast Listener Discovery
MoA	Memorandum of Agreement
MPDU	MACsec Protocol Data Unit
MPLS	Multiprotocol Label Switching
MSC	Multi-Site Connectivity
MTU	Maximum Transmission Unit
NDP	Neighbor Discovery Protocol
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
NSA	National Security Agency
NSS	National Security Systems
NTP	Network Time Protocol
O	Objective
OCSP	Online Certificate Status Protocol

Acronym	Definition
OEM	Original Equipment Manufacturer
OID	Object Identifier
OS	Operating System
OSPF	Open Shortest Path First
PKCS	Public Key Cryptographic Standard
PKI	Public Key Infrastructure
PMTU	Path Maximum Transmission Unit
PSK	Pre-Shared Key
PTP	Precision Time Protocol
QoS	Quality of Service
RA	Registration Authority
RFC	Request for Comments
RIP	Routing Information Protocol
RSA	Rivest Shamir Adelman algorithm
SA	Security Association
SAK	Secure Association Key
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
TFFW	Traffic Filtering Firewall
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
XPN	eXtended Packet Number

APPENDIX C. REFERENCES

CNSSD 505	*CNSS Directive (CNSSD) Number 505, Supply Chain Risk Management (SCRM)*	March 2012
CNSSI 1253	*CNSS Instruction (CNSSI) 1253, Security Categorization and Control Selection for National Security Systems*	March 2014
CNSSI 1300	*CNSS Instruction (CNSSI) 1300, National Security Systems Public Key Infrastructure X.509 Certificate Policy*	December 2014
CNSSI 4009	*CNSS Instruction (CNSSI) 4009, Committee on National Security Systems Glossary*	April 2015
CNSSP 11	*CNSS Policy (CNSSP) Number 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products*	June 2013
CNSSP 15	*CNSS Policy (CNSSP) Number 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems Committee for National Security Systems*	October 2016
FIPS 140-2	*Federal Information Processing Standard 140, Security Requirements For Cryptographic Modules.* National Institute for Standards and Technology (NIST).	May 2001
FIPS 180-4	*Federal Information Processing Standard 180-4, Secure Hash Standard (SHS).* NIST.	August 2015
FIPS 186-4	*Federal Information Processing Standard 186-4, Digital Signature Standard (DSS).* NIST.	July 2013
FIPS 197	*Federal Information Processing Standard 197, Advanced Encryption Standard (AES).* NIST.	November 2001
IAD MD-110	*Information Assurance Directorate Management Directive No. 110, Cryptographic Key Protection*	July 2011
IEEE 802.1AE-2006	*IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security*	August 2006
IEEE 802.1AEbn-2011	*IEEE Standard for Local and Metropolitan Area Networks--Media Access Control (MAC) Security Amendment 1: Galois Counter Mode--Advanced Encryption Standard-- 256 (GCM-AES-256) Cipher Suite*	October 2011
IEEE 802.1 AEbw-2013	*IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Security Amendment 2: Extended Packet Numbering*	February 2013
IEEE 802.1AEcg-2016 (draft)	*IEEE Standard for Media Access Control (MAC) Security Amendment: Ethernet Data Encryption Devices, Draft, June 2016*	June 2016
RFC 3526	*IETF RFC 3526 More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE).* T. Kivinen and M. Kojo.	May 2003

RFC 3647	*IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.* S. Chokhani, et. al.	November 2003
RFC 4252	*IETF RFC 4252 The Secure Shell (SSH) Authentication Protocol*. T. Ylonen and C. Lonvick.	January 2006
RFC 4253	*IETF RFC 4253 The Secure Shell (SSH) Transport Layer Protocol*. T. Ylonen and C. Lonvick.	January 2006
RFC 4254	*IETF RFC 4254 The Secure Shell (SSH) Connection Protocol*. T. Ylonen and C. Lonvick.	January 2006
RFC 4256	*IETF RFC 4256 Generic Message Exchange Authentication for the Secure Shell Protocol (SSH)*. F. Cusack and M. Forssen.	January 2006
RFC 4302	*IETF RFC 4302 IP Authentication Header*. S. Kent.	December 2005
RFC 4303	*IETF RFC 4303 IP Encapsulating Security Payload*. S. Kent.	December 2005
RFC 4307	*IETF RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*. J. Schiller.	December 2005
RFC 4308	*IETF RFC 4308 Cryptographic Suites for IPsec*. P. Hoffman.	December 2005
RFC 4754	*IETF RFC 4754 IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)*. D. Fu and J. Solinas.	January 2007
RFC 5246	*IETF RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2*. T. Dierks and E. Rescorla.	August 2008
RFC 5280	*IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. D. Cooper, et. al.	May 2008
RFC 5746	*IETF RFC 5746 Transport Layer Security (TLS) Renegotiation Indication Extension.* E. Rescorla, et. al.	February 2010
RFC 5759	*IETF RFC 5759 Suite B Certificate and Certificate Revocation List (CRL) Profile*. J. Solinas and L. Zieglar.	January 2010
RFC 5878	*IETF RFC 5878 Transport Layer Security (TLS) Authorization Extensions.* M. Brown and R. Housley.	May 2010
RFC 5903	*IETF RFC 5903 Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2.* D. Fu and J. Solinas.	June 2010
RFC 6176	*IETF RFC 6176 Prohibiting Secure Sockets Layer (SSL) Version 2.0.* S. Turner and T. Polk.	March 2011
RFC 6379	*IETF RFC 6379 Suite B Cryptographic Suites for IPsec*. L. Law and J. Solinas.	October 2011
RFC 6380	*IETF RFC 6380 Suite B Profile for Internet Protocol Security (IPsec)*. K. Burgin and M. Peck.	October 2011
RFC 6668	*IETF RFC 6668 SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol. D. Bider and M. Baushke.*	July 2012

RFC 6818	*IETF RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. P. Yee.	January 2013
RFC 6960	*IETF RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.* S. Santerson, et. al.	June 2013
RFC 7030	*IETF RFC 7030 Enrollment over Secure Transport*. M. Pritikin, P. Yee, and D. Harkins.	October 2013
RFC 7296	*IETF RFC 7296 Internet Key Exchange Protocol Version 2 (IKEv2).* C. Kaufman, et. al.	October 2014
RFC 7427	*IETF RFC 7427 Signature Authentication in the Internet Key Exchange version 2 (IKEv2).* T. Kivinen and J. Snyder.	January 2015
RFC 7465	*IETF RFC 7465 Prohibiting RC4 Cipher Suites.* A. Popov.	February 2015
RFC 7507	*IETF RFC 7507 TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks.* B. Moeller and A. Langley.	April 2015
RFC 7568	*IETF RFC 7568 Deprecating Secure Sockets Layer Version 3.0.* R. Barnes, et. al.	June 2015
RFC 7627	*IETF RFC 7627 Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension.* K. Bhargavan, et. al.	September 2015
RFC 7670	*IETF RFC 7670 Generic Raw Public-Key Support for IKEv2.* T. Kivinen, P. Wouters, and H. Tschofenig.	January 2016
RFC 7685	*IETF RFC 7685 A Transport Layer Security (TLS) ClientHello Padding Extension.* A. Langley.	October 2015
RFC 7905	*IETF RFC 7905 ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS).* A. Langley, et. al.	June 2016
RFC 7919	*IETF RFC 7919 Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS).* D. Gillmor.	August 2016
SP 800-56A	*NIST Special Publication 800-56A Rev. 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*. E. Barker, et. al.	May 2013
SP 800-56B	*NIST Special Publication 800-56B Rev. 1, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*. E. Barker, et. al.	September 2014
SP 800-56C	*NIST Special Publication 800-56C, Recommendation for Key Derivation through Extraction-then-Expansion*. L. Chen.	November 2011
SP 800-57	*NIST Special Publication 800-57 Part 1 Rev 4, Recommendation for Key Management Part 1: General.* E. Barker.	January 2016
SP 800-131A	*NIST Special Publication 800-131A Rev. 1, Recommendation for Transitioning of Cryptographic Algorithms and Key Lengths*. E. Barker and A. Roginsky.	November 2015