NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

COMMERCIAL SOLUTIONS for CLASSIFIED (CSfC)

Campus Wireless Local Area Network (WLAN) Capability Package 3.2.0

Version 3.2.0
27 March 2026

CHANGE HISTORY

Title	Version	Date	Change Summary
Commercial Solutions for Classified (CSfC) Campus Wireless Local Area Network (WLAN) Capability Package	3.2.0	27 March 2026	• Objective CNSA 2.0 Algorithms for Wi-Fi and IPsec • Added Objective Software Signing Requirements • Clarified preference for separate WLAN Access Systems for Multi-Classification use case
Commercial Solutions for Classified (CSfC) Campus Wireless Local Area Network (WLAN) Capability Package	3.1.0	28 January 2025	• Added Composed EUD Requirement. • Added Clarification on Gray Management and Gray Data Network Separation. • Removed duplicate rational for layered encryption title. • Aligned Two Factor Authentication to Multi-Factor Authentication requirements. • Added Dedicated Outer WLAN use case. • Added objective requirement for Beacon Protection and Operation Channel Validation. • Added SHA-512 support. • WLAN-WC-6 has been moved to objective. • Alternative made for WLAN-EU-29 to allow for administrator lock out instead of device wipe. • DTLS has been added to WLAN-WL-4. • Added allowance for EUD to be directly wired into Red Network in WLAN-EU-17.
Commercial Solutions for Classified (CSfC) Campus Wireless Local Area Network (WLAN) Capability Package	3.0	04 May 2022	• Updated to WPA3 standard for 802.11 encryption, deprecating WPA2 in this document. • Added Campus WLAN Tactical Appendix. • Added Objective Virtualization requirements. • Added Objective Two Factor requirements. • Rewrote sections for consistency with other CSfC CPs. • Added inner firewall requirement. • Increased EUD minimum password to 14 characters. • Added 802.11w requirement.

Title	Version	Date	Change Summary
Commercial Solutions for Classified (CSfC) Campus Wireless Local Area Network (WLAN) Capability Package	2.3	April 2021	• Relocated WIDS Requirements from the CP and created a separate WIDS/WIPS Annex. • Relocated Continuous Monitoring Requirements from the CP and created a separate Continuous Monitoring Annex. • Inner Encryption Component must function using Tunnel Requirement.
Commercial Solutions for Classified (CSfC) Campus Wireless Local Area Network (WLAN) Capability Package	2.2	June 26, 2018	• Relocated Key Management Requirements from the CP and created a separate Key Management Requirements Annex. • Updated requirements to use "must" instead of "shall." • Minor administrative changes were made in formatting. • Changed WLAN PS-12 to 'Objective.' • Changed WLAN PS-14 to 'Threshold=Objective.'
Commercial Solutions for Classified (CSfC) Campus Wireless Local Area Network (WLAN) Capability Package	2.1	February 2018	• Removed references to CNSS AM 02-15 as CNSSP-15 was updated and signed. • Removed references to Suite-B encryption algorithms. Updated to reference the Commercial National Security Algorithm (CNSA) Suite. • Changed WLAN-PS-9 to Objective. • Changed WLAN-EU-23 minimum password length. • Updated Continuous Monitoring section to be consistent with other DIT CPs. • Updated Testing Requirements and created a Testing Requirements Annex. • Updated template IAD -> IAC. • Added requirement WLAN-PS-6 for selecting a Certification Authority from the CSfC Components list. • Removed Threat section—in a separate document available on the CSfC webpage. • Modified Table 17 to change the Objective requirement for AES-256-GCMP to AES-256-CCMP; removed inaccurate RFC references. • Added wording (from the Mobile Access CP) at the end of Section 2 to address case-by-case approvals for TS systems.

Title	Version	Date	Change Summary
Commercial Solutions for Classified (CSfC) Campus Wireless Local Area Network (WLAN) Capability Package	2.0	March 18, 2016	• Added EUD requirement (WLAN-EU-40) to isolate the management and control of the EUD connection to the WLAN system from other EUD functions. • Added IDS requirements for the Gray Network.
Commercial Solutions for Classified (CSfC) Campus Wireless Local Area Network (WLAN) Capability Package	1.8	September 17, 2015	• Initial release of CSfC Campus WLAN guidance for use of a Shared Outer WPA2 layer and single Gray Network with networks of multiple security levels. • Improvements of Continuous Monitoring and revised content to be consistent with VPN CP version 3.2 and MA CP version 1.1. • Added new Cryptography standards in accordance with CNSSP 15. • Added Gray Firewall. • Added Continuous Monitoring Requirements • Updated requirement WLAN-PS-10
Commercial Solutions for Classified (CSfC) Campus IEEE 802.11 Wireless Local Area Network (WLAN) Capability Package	1.1	March 4, 2014	• Corrected minor errors. • Removed redundant requirements. • Added Solution testing section. • Added Appendix F to state summary of changes in requirements between the versions.
Commercial Solutions for Classified (CSfC) Campus IEEE 802.11 Wireless Local Area Network (WLAN) Capability Package	1.0	August 20, 2013	• Official release of CSfC Campus WLAN guidance. • Revised content to be consistent with VPN CP version 2.0. • Removed compound requirements for improved testability. • Merged sections to reduce duplicate requirements.

TABLE OF CONTENTS

Table of Figures

List of Tables

1 INTRODUCTION

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

The NSA delivers this CSfC Campus Wireless Local Area Network (WLAN) CP to meet the demand for commercial End User Devices (EUD) (tablets, smartphones, and laptop computers) to access secure enterprise services over a campus wireless network. Cryptographic algorithms, known as Commercial National Security Algorithms (CNSA), are used to protect classified data using layers of COTS products.

While CSfC encourages industry innovation, trustworthiness of the components is paramount. Customers and their Integrators are advised that modifying a National Information Assurance Partnership (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 to determine whether such a modification will affect the component's certification.

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

Wireless communication systems (e.g., Wi-Fi) are inherently risky. *The CSfC WLAN CP* was developed and approved by the National Manager as a commercial strategy suitable for protecting classified information and National Security Systems (NSS), provided the customer's implementation of the solution is configured, maintained, and monitored as required by the CP. The residual risks for this CP are documented in the WLAN CP *Version* 3.2.0 *Risk Assessment*. The National Manager is responsible for ensuring that the design documented in the CP is sufficiently robust to protect classified information and NSS. The Government Authorizing Official (AO) assumes the risk for implementing and deploying the solution in accordance with the requirements in the CP. The AO must consider the operational environment and provide appropriate usage guidance to End Users. End Users must understand the risks and adhere to handling requirements established by the AO for the fielded WLAN CP system. End Users must maintain positive physical control of the End User device. Further, End Users should consider their environment and ensure adequate physical and wireless protections are in place.

2 PURPOSE AND USE

This CP provides high-level reference architecture and corresponding configuration information that allows customers to select COTS products from the CSfC Components List, available on the CSfC web

page (https://www.nsa.gov/resources/commercial-solutions-for-classified-program), for their Campus WLAN 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 11, customers must ensure that the components selected from the CSfC Components List provide the necessary functionality for the selected capabilities. To successfully implement a solution based on this CP, all Threshold (T) Requirements, or the corresponding Objective (O) Requirements applicable to the selected capabilities, must be implemented, as described in Section 11.

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

This CP will be reviewed twice a year to ensure that the defined capabilities and other instructions still provide the security services and robustness required. Solutions designed according to this CP must be registered with the NSA. Once registered, a signed Deputy National Manager (DNM) Approval Letter will be sent validating that the WLAN solution is registered as a CSfC solution validated to meet the requirements of the latest WLAN CP and is approved to protect classified information. Any solution designed according to this CP may be used for one year and must then be revalidated against the most recently published version of this CP. Top Secret Solutions will be considered on a case-by-case basis. Customers are encouraged to engage their Client Advocate or the CSfC PMO team early in the process to ensure the solutions are properly scoped, vetted, and that the customers understand the risks and available mitigations. Please provide comments on usability, applicability, and/or shortcomings to your NSA Client Advocate and the WLAN CP Maintenance Team at Wi-Fi@nsa.gov. WLAN CP solutions must also comply with the Committee on National Security Systems (CNSS) Policies and Instructions. Any conflicts identified between this CP and the CNSS or local policy should be provided to the WLAN CP Maintenance Team.

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

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

Customers and integrators must adhere to all applicable data transfer policies for their organization when designing and implementing Cross Domain Solutions (CDS) capabilities within their CSfC solution architecture. For example, DoD customers must follow DoDI 8540.01, "Cross Domain (SD) Policy", when deploying a CDS within a CSfC solution. Any discrepancies found between the guidance in this document and DoDI 8540.01 should be reported to the CSfC PMO office at csfc@nsa.gov.

For any additional information on CDSs, contact the National Cross Domain Strategy Management Office (NCDSMO) at ncdsmo@nsa.gov.

3 LEGAL DISCLAIMER

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

The solution described within this CP is supported by the use of wireless devices to access sensitive data and enterprise services while minimizing the risk when connecting to existing Government enterprise networks. Government-managed campus-area wireless networks provide controlled connectivity between mobile users and the broader Government enterprise. The term "Campus" is used in this document to refer to any area that is physically protected to the highest classification level of the enterprise network where multiple enclaves are supported. This physical area includes secure facilities and tactical environments when the Authorizing Official (AO) deems the physical controls appropriate.

The Campus WLAN solution uses two layers of cryptography, Internet Protocol Security (IPsec) using AES 256 and WPA3 using AES 256, to protect the confidentiality and integrity of the data as it transits the untrusted network. The Virtual Private Network (VPN) Client and WLAN Client running on an EUD generate the two layers protecting data flow. Figure 1 shows at a high level the basic segments of the Campus WLAN architecture. A customer implementing a WLAN solution that uses two layers of IPsec encryption has the option of complying and registering with the latest *Mobile Access CP* instead of this

CP.

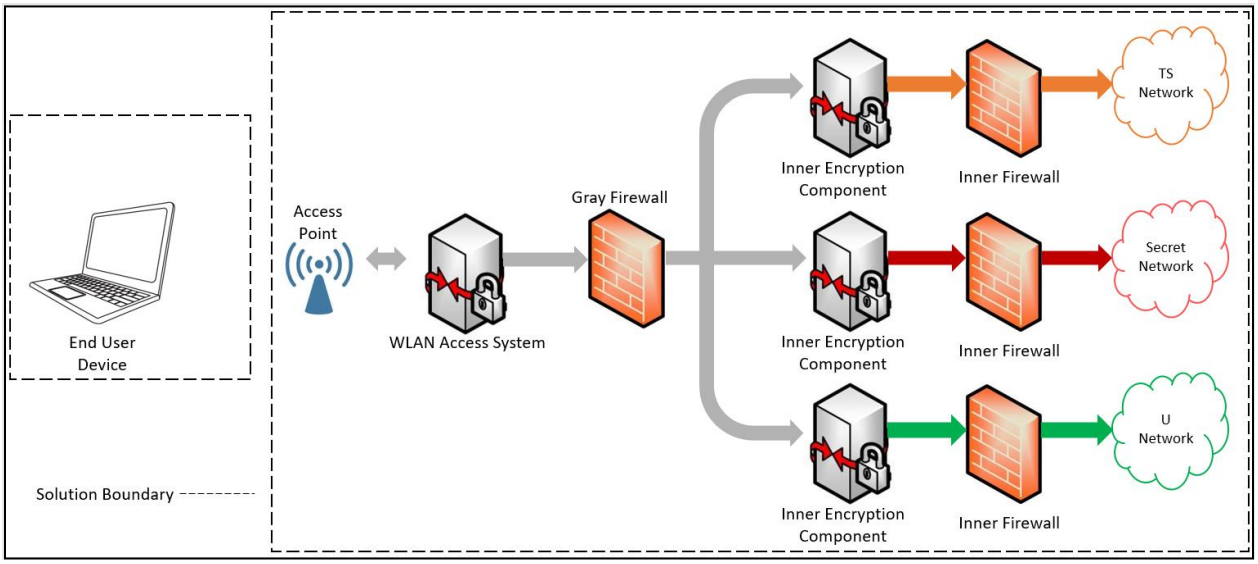

Figure 1. Overview of Campus WLAN CP

Campus WLAN solutions are composed, layered, and built using products from the CSfC Components List. Customers who are concerned that their desired products are not yet on the CSfC Components List are encouraged to contact the vendors and urge them to sign a Memorandum of Agreement (MOA) with NSA and start the National Information Assurance Partnership (NIAP) evaluation process, which enables them to be listed on the CSfC Components List. Products listed on the CSfC Components List are not guaranteed to be interoperable with all other products on the Components List. Customers and Integrators should perform interoperability testing to ensure the components selected for their Campus WLAN solution are interoperable. Customers needing assistance obtaining vendor POC information should email csfc_components@nsa.gov.

4.1 Rationale for Layered Encryption

A single layer of CNSA encryption, properly implemented, is sufficient to protect classified data in transit. However, a CSfC Campus WLAN solution uses two layers of CNSA encryption to mitigate the risk of a failure in one of the cryptographic components. Accidental misconfiguration, operator error, or malicious exploitation of a vulnerability, could result in the exposure of classified information if a single layer is used. The use of multiple layers, implemented with components meeting the CSfC vendor diversity requirements, reduces the likelihood that a single vulnerability can be exploited to reveal protected information.

Diversity of implementation is needed between the components in each layer of the solution in order to reduce the likelihood that both layers share a common vulnerability. The CSfC Program recognizes two ways to achieve this diversity. The first is to implement each layer using components produced by different manufacturers. The second is to use components from the same manufacturer, where the manufacturer has provided NSA with sufficient evidence that the implementations of the two components are independent of one another. The CSfC web page (https://www.nsa.gov/resources/commercial-solutions-for-classified-program) contains details on how a manufacturer submits this evidence to NSA and what documentation must be provided. Customers

that wish to use products from the same manufacturer in both layers must contact their NSA Client Advocate to confirm that NSA has accepted the manufacturer's claims before implementing their solution.

4.2 NETWORKS

This CP uses the following terminology to describe the various networks that comprise a Campus WLAN 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.

4.2.1 RED NETWORK

Red data consists of unencrypted classified data and a Red Network contains only Red data. Red Networks are under the control of the solution owner or a trusted third party.

The Red Network begins at the internal interface(s) of Inner Encryption Components located between the Gray Firewall and Inner Firewall. EUDs access the Red Network through the two layers of nested encryption described in this CP. For example, an Inner VPN Gateway located between the Gray Firewall and Inner Firewall terminates the Inner layer of IPsec encryption from a VPN EUD. Once a successful IPsec connection is established, the EUD is given access to classified services such as web, email, Virtual Desktop Infrastructure (VDI), voice, etc.

Red Networks may only communicate with an EUD through the WLAN solution if both operate at the same security level.

4.2.2 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 data on a Gray Network is classified, perhaps by determining the Internet Protocol (IP) addresses are classified at some level, then the WLAN solution described in this CP cannot be implemented, as it is not designed to provide two layers of protection for any data/traffic on the Gray Network.

Gray Network components consist of the WLAN Access System, Gray Firewall, and Gray Management Services. All Gray Network components are physically protected at the same level as the Red Network components of the WLAN infrastructure. Gray Management Services are physically connected to the Gray Firewall and include, at a minimum, an administration workstation. The Gray Management Services also include a Security Information and Event Management (SIEM) unless the SIEM is implemented in the Red Network in conjunction with a CDS. See the *Continuous Monitoring Annex* for more information. The WLAN 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 WLAN Access System, Gray Firewall, or Gray Management Services. Additionally, the Gray administration workstation is prohibited from managing Inner Encryption Components. These Inner Encryption Components must be managed from a Red Administration Workstation.

The Gray Network may be extended and shared through different sites using the *Enterprise Gray Implementation Requirements Annex*. This Annex allows for Gray Management Services to be shared between different CSfC deployments. For more information see the *Enterprise Gray Implementation Requirements Annex*.

4.2.3 BLACK NETWORK

A Black Network contains classified data that has been encrypted twice. The wireless network between the EUD and the WLAN Access System in which data is protected with two layers of encryption (the IPsec and the WPA3 layers) is a Black Network. Depending on which vendor product is chosen from the CSfC Components List, the WPA3 layer can terminate on either the Access Point(s) (AP) or Wireless controller. For WPA3 tunnels terminating at the AP, encryption standards such as IPsec, Secure Shell version 2 (SSHv2), Transport Layer Security (TLS), or TLS/Hypertext Transfer Protocol Secure (HTTPS) must be used to encrypt data between the AP and the wireless controller.

4.2.4 DATA, MANAGEMENT, AND CONTROL PLANE TRAFFIC

Data plane traffic is encrypted or unencrypted classified information that is being passed through the Campus WLAN solution. The Campus WLAN solution exists to encrypt and decrypt data plane traffic. All data plane traffic within the Black Network must be encapsulated within the Encapsulating Security Payload (ESP) protocol and WPA3 Enterprise.

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 log server, SIEM or similar repository. Management plane traffic on Red and Gray Networks must be encapsulated within the SSHv2, ESP, or TLS protocol.

Control plane traffic consists of standard protocols necessary for the network to function. Control plane traffic is typically not initiated directly on behalf of a user (unlike data traffic) or a system administrator (unlike management traffic). Many, but not all, control plane protocols operate at Layer 2 or Layer 3 of the Open Systems Interconnection (OSI) model. Examples of control plane traffic include, but are not limited to, the following:

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

In general, this CP does not impose detailed requirements on control plane traffic, although control plane protocols may be used in order to implement certain requirements. For example, requirements WLAN-SR-2 and WLAN-SR-3 (see Section 12.1), 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. This CP provides detailed requirements in those cases due to the impact on the security of the solution. Unless otherwise specified in this CP, the usage of specific control plane protocols is left to the Solution Owner to approve, but any control plane protocols not approved by the solution owner should be disabled.

Data plane and management plane traffic is required to be separated from one another using physical, logically (at the Gray Firewall), 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 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. The Gray Management network is separated from the Gray Data network via the Gray Firewall and no other component, such as a switch or router, can conduct this separation unless it is a firewall chosen from the CSfC Components list. The Gray Firewall uses an Access Control List (ACL) to ensure that only appropriate Gray Management Services (i.e., administration workstation, SIEM or Network Time Server) can communicate with the WLAN Access System. The Gray Firewall is also responsible for ensuring that Gray Management Services are only capable of flowing in the appropriate direction. For example, SSH traffic is permitted to initiate from an administration workstation to the WLAN Access System, but not from the WLAN Access System to any Gray Management Services. Conversely, system log data is permitted from the WLAN Access System to the Gray collection server, but is not permitted from the Gray Management Services to the WLAN Access System. 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.

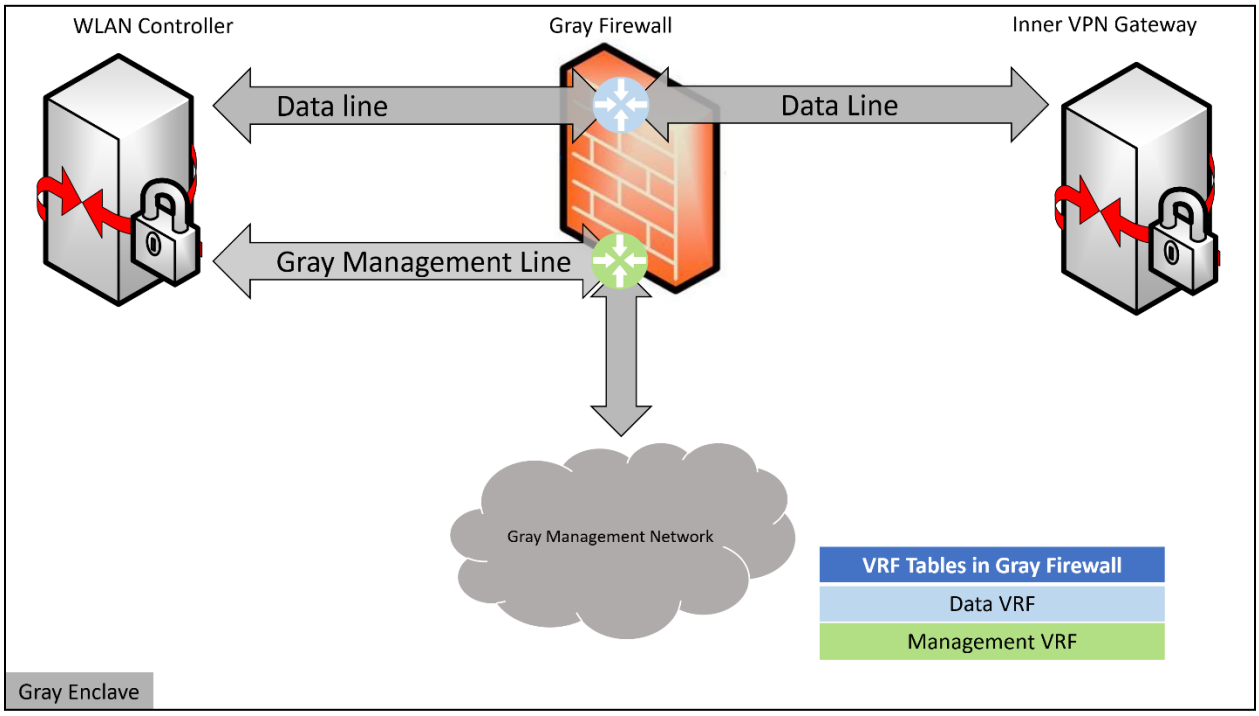

Figure 2. Gray Data and Management VRF Separation

Data and management traffic may be separated using Virtual Routing and Forwarding (VRF) on the Gray Firewall to enhance network security beyond firewall ACL filtering. VRFs are not required but can greatly increase the security posture within traditional static routing networks. Each interface will be assigned to a VRF that is specifically allowed to interact with its respective network plane (Data Plane or Management Plane). In some cases, the implementer may need to import or export routes to establish a VPN tunnel on an interface outside of its respective VRF. The primary use case of importing and exporting routes between VRFs is for the importing of the routes destined for the Inner Encryption Component to travel over its encrypted tunnel. A separate VRF should be used for the local Gray Management Network allowing for separation and for connecting the Gray Firewall to the local Gray Management Network.

4.3 HIGH-LEVEL DESIGN

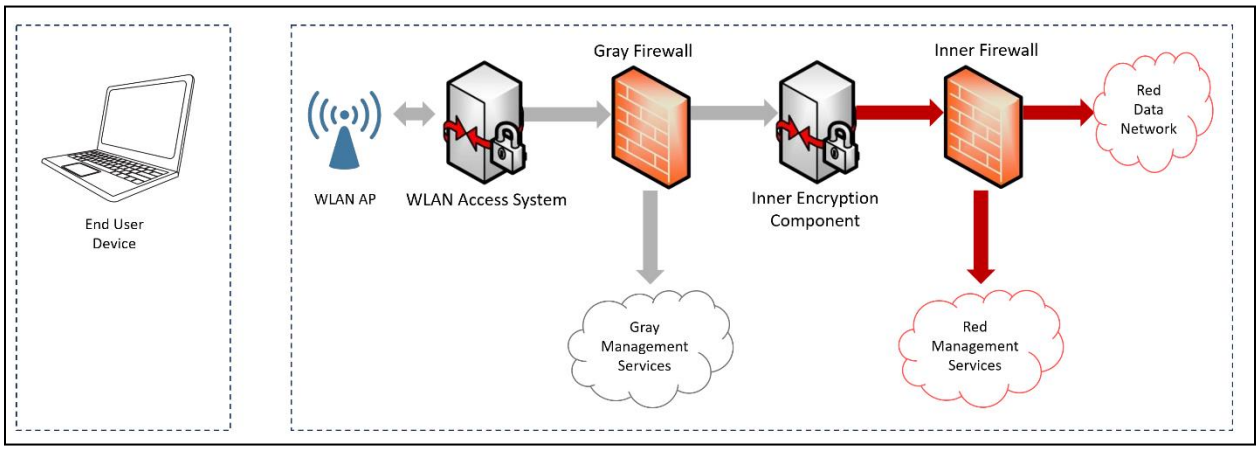

Figure 3. Campus WLAN Single Classification Implementation

Depending on the needs of the customer implementing the solution, the Campus WLAN CSfC solution is adaptable to support multiple capabilities. If a customer does not have to support multiple classified networks, then those elements do not need be included as part of the implementation as seen in Figure 3. The Black/Gray boundary in Figure 3 can be at the Access Point(s) or Controller, depending on the vendor. Similarly, a customer may choose to implement a solution where classified information is protected as it travels over-the-air between a WLAN-enabled EUD and a WLAN infrastructure attached to a wired network of the same classification level. However, any implementation of the Campus WLAN solution must satisfy all of the applicable requirements specified in this CP.

4.3.1 END USER DEVICES

This CP uses the concept of an EUD, which is either a single Computing Device, such as a smart phone, laptop, or tablet, or the combination of a Computing Device and a Dedicated Outer WLAN. The EUD provides two layers of protection for data in transit to access classified data on the Red Network. EUDs are dedicated to a single classification level and can only be used to access a Red Network of the same classification. EUDs must either be selected from the CSfC Components list or be comprised of selected sub-components listed on the CSfC Components list. For more information see section 6.1.

The two options for selecting an EUD within Campus WLAN from the CSfC Components list are:

1) be listed as an MDF EUD on the CSfC Components list;

2) select sub-components listed on the CSfC Components list to compose an EUDs.

The customer and/or Trusted Integrator is responsible for selecting and composing these sub-components into a functioning EUD. The CSfC Program does not guarantee the interoperability of the different sub-components. The sub-components that makeup a composed EUD include the following:

- General Purpose Operating Systems
- Client Virtualization Systems
- WLAN Clients

- General Purpose Compute Platform
- Dedicated Security Component (Optional)
- Hardware Full Drive Encryption or
- Software Full Drive Encryption

The Campus WLAN CP allows three different deployment options pertaining to the use and handling of an EUD while powered off:

- **EUD with DAR:** To implement Data-at-Rest (DAR) protection on an EUD, the DAR solution must be approved by NSA, either as a tailored solution or compliant with NSA's *Data-at-Rest CP.* Specification of such a DAR solution is outside the scope of this CP, but can be found in the DAR CP. The NSA requires implementing organizations to define the circumstances in which an EUD is to be considered outside of the continuous physical control of authorized users (i.e., "lost"). AOs will define "continuous physical control" and that definition should align with the intended mission and threat environment for which the solution will be deployed. Organizations must also define the circumstances in which an EUD that is a part of that organization's solution is to be considered recovered back into the continuous physical control of authorized users (i.e., "found").
- **Classified EUD:** The EUD can be used exclusively with physical security measures approved by the AO. EUDs are not subject to special physical handling restrictions beyond those applicable for classified devices since they can rely on the environment they are in for physical protection. If this design option is selected, the EUDs must be treated as classified devices at all times. The EUD must have a single layer of CSfC approved DAR protection to protect the private keys stored on it from disclosure and to increase the difficulty of tampering with the software and configuration. Continuous physical control of the EUD must be maintained at all times.
- **Thin EUD:** The EUD can be designed to prevent any classified information except for the private keys from being saved to any persistent storage media on the EUD. Possible techniques for implementing this include, but are not limited to: using Virtual Desktop Infrastructure (VDI) configured to not allow data from the associated Red Network to be saved on the EUD, restricting the user to a non-persistent virtual machine on the EUD, and/or configuring the EUD's operating system to prevent the user from saving data locally. Since the EUD does not provide secure local storage for classified data, its user is also prohibited by policy from saving classified data to it. The EUD must have a single layer of CSfC approved DAR protection to protect the private keys stored on it from disclosure, and to increase the difficulty of tampering with the software and configuration. Continuous physical control of the EUD must be maintained at all times.

The intent of a continuous physical control requirement for the WLAN CP is to prevent potential attacks via brief, undetected physical access of an EUD by any adversary. When used and stored within a

protected campus environment, the inherent security controls are sufficient to meet this requirement. When a WLAN EUD is transported or stored outside of the protected campus, a user must maintain continuous physical control of the EUD such that an adversary cannot obtain brief, undetected physical access.

While powered on, an EUD is classified at the same level of the Red Network that it accesses through the Campus WLAN solution, since classified data may be present in volatile memory and/or displayed on screen. With the addition of the DAR CP to a solution an EUD may be treated as unclassified when fully powered off. To mitigate the risk of accidental disclosure of classified information to unauthorized personnel while the EUD is in use, the customer must define and implement an EUD user agreement that specifies the rules of use for the system. The customer must only grant a user access to an EUD after they complete the user agreement and receive training on the use and protection of the EUD.

4.3.2 MULTIPLE SECURITY LEVELS

A single implementation of the WLAN solution may support multiple Red Networks of different security levels. The WLAN solution provides secure connectivity between EUDs and the Red Network of the same security level while preventing EUDs from accessing Red Networks of different security levels. This enables a customer to use the same physical infrastructure to carry traffic from multiple networks. EUDs operating as part of a Multiple Security Level solution are still dedicated to a single classification level. Although each Red Network still requires its own Inner Encryption Component(s), a site may use a single WLAN Access System in the infrastructure to encrypt and transport traffic that has been encrypted by Inner Encryption Components of varying security levels. As shown in Figure 4, a SECRET Coalition EUD is only capable of communicating with and authenticating to the Inner Encryption Components for the – SECRET Coalition network. This EUD does not have any connectivity to the Inner Encryption Components of the TS or Unclassified networks.

There is no limit to the number of different security levels that a WLAN solution may support.

In all cases, separate CAs and management devices are needed to manage the Inner Encryption Components and Inner Firewall at each security level. For example, Figure 5 shows an independent site with multiple security levels. Network 1, Network 2, and Network 3 each have their own CA and management devices which prevent EUDs from being able to authenticate with the incorrect network.

In addition to separate Inner Encryption Components and CAs, an authentication server must be used to allow the use of a single Outer Virtual Private Network (VPN) Gateway for multiple security levels. The authentication server resides within the Gray Management network and validates that Outer Tunnel certificates are signed by the Outer Tunnel CA, are still within their validity period, and have not been revoked. The authentication server also parses the certificate for information assigned to a specific inner network (e.g., Organizational Unit (OU) field or policy Object Identifiers (OIDs)) to determine which inner network the EUD is authorized to connect. After successful authentication, the authentication server provides an accept message to the WLAN Access System along with a Vendor-Specific Attribute (VSA). The WLAN Access System uses the VSA to assign the proper network and firewall rules such that an EUD can only reach the appropriate Inner Encryption Components.

4.3.2.1 Networks Operating at the Same Classification Level

When Red Networks operate at the same classification level but at different security levels, the cryptographic separation provided by the Inner VPN Gateways is sufficient to protect against unintended data flows between security levels. Two Inner VPN Gateways for networks of different security levels will be unable to mutually authenticate with each other because they trust different CAs which do not have a trust relationship with one another. This prevents the establishment of an IPsec tunnel between the two components.

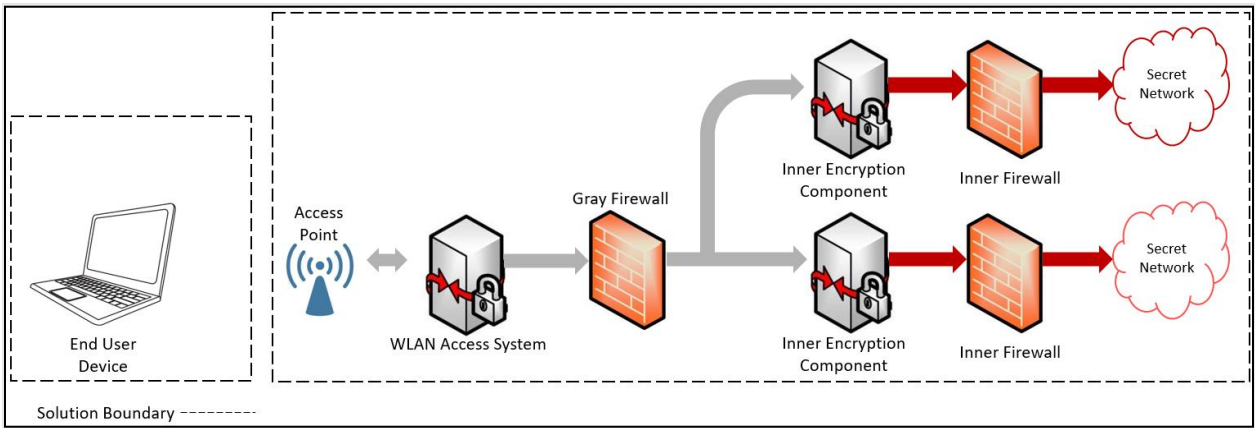

Figure 4. Campus WLAN Solution for Two Networks of the Same Classification Level

4.3.2.2 Networks Operating at Different Classification Levels

For Red Networks of different classification levels, the cryptographic separation of their traffic on a Gray Network (as described in Section 4.3.2.1) is still present. However, because the consequences of an unintended data flow between different classification levels are more severe than one with a single classification level, an additional mechanism is necessary to further guard against such a flow from occurring.

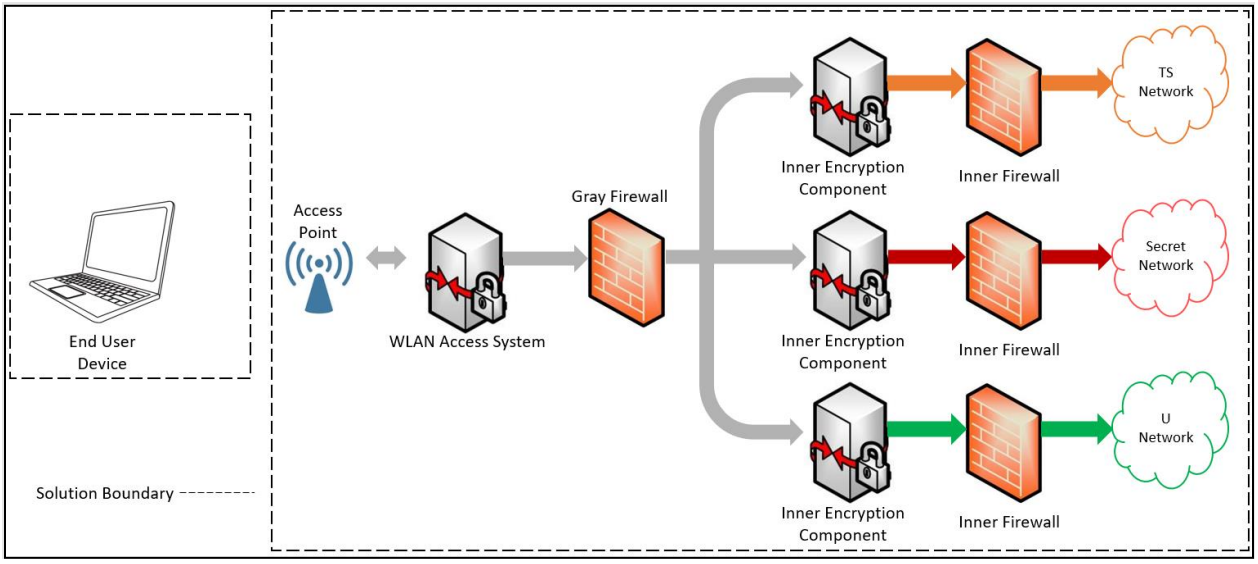

Figure 5. Campus WLAN Solution for Networks Operating at Different Classification Levels

In this scenario packet filtering is required within Gray Networks as an additional mechanism to prevent data flows between networks of different classification levels. Any physical path through a Gray Network between multiple Inner VPN Gateways supporting Red Networks of different classification 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. Packets are passed only if the source and destination components are intended to communicate with one another and are dropped otherwise.

When multiple classification levels are used, it is critical to enforce proper IP address assignment and firewall rule sets. The IP address assigned must be unique to that classification level such that the EUD is only able to send and receive traffic to and from their respective VPN Gateway. Proper assignment of IP address and firewall rule sets is done at both the Authentication Server (AS) and WLAN access system based on either an allowlist or X.509 Certificate.

Additionally, in the cases of WLAN solutions supporting multiple security classification such as unclassified red network existing in conjunction with a classified network. Multiple WLAN Access Systems should be used with the centralized cryptography model where the APs are “thin” and feed into separate controllers for encryption. See section 5.1 for more details.

4.4 AUTHENTICATION

The WLAN solution provides mutual device authentication between WLAN Access System and between Inner Encryption Components via public key certificates. This CP requires that all authentication certificates issued to WLAN Access System and Inner Encryption Components be Non-Person Entity (NPE) certificates. In addition, NPE certificates issued to WLAN Access Systems may need to assert the IP address of the WLAN Access System in either the Common Name field of the certificate Distinguished Name, or in the Subject Alternative Name certificate extension. The EUD may be required to check the

IP address asserted in the WLAN Access System certificate and ensure it is the same IP address registered in the EUD.

4.4.1 Traditional Authentication

Following the two layers of device authentication, EUDs require the user to authenticate to the network before gaining access to any classified data (e.g., username/password, user certificate). When a device certificate is used, the user must also authenticate to the Red Network before gaining access to any classified data in the same manner as a EUD (e.g., username/password, user certificate). In this latter case, it is recommended that additional access controls, such as allowlists, be implemented in conjunction with the user certificate to control access to Red Network services.

In addition to authentication for the Outer and Inner layer of encryption, the WLAN CP requires user-to-device authentication. This authentication occurs between the user and the Computing Device (which processes Red data) of an EUD. The WLAN CP requires EUD components use a minimum of a 14-character, case-sensitive, alphanumeric password to authenticate to the device. This password can be used both for decrypting the platform encryption as well as for unlocking the screen. EUD components, which are selected from the Mobile Platform section of the CSfC Components List, are able to use a relatively short authentication factor since they use a hardware-based root encryption key which is evaluated during the NIAP certification.

4.4.2 Multi-Factor Authentication

Within this CP a form of multi-factor authentication should be used for a user to access classified data. The current multi-factor authentication options are, 'something you know' and 'something you have.' There are three forms of multi-factor authentication:

- User to EUD
- User to VPN
- User to Virtual Desktop Interface (VDI)

4.5 Other Protocols

Throughout this document, when IP traffic is discussed, it can refer to either IPv4 or IPv6 traffic, unless otherwise specified, as the WLAN solution is agnostic to most named data handling protocols.

Public standards conformant Layer 2 control protocols, are allowed as necessary to ensure the operational usability of the network. This CP is agnostic with respect to Layer 2; specifically, it does not require Ethernet. Public standards conformant Layer 3 control protocols, may be allowed based on local 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.

It is expected that the WLAN solution can be implemented in such a way as to take advantage of standards-based routing protocols that are already being used in the Red Network. For example, networks that currently use Generic Routing Encapsulation (GRE) or Open Shortest Path First (OSPF)

protocols can continue to use these in conjunction with the Inner Firewall solution to provide routing as long as the AO approves their use.

Future iterations of this CP will discuss using different wireless standards other than 802.11 Wi-Fi if the standard still implements the WPA3 standard.

4.6 AVAILABILITY

The high-level designs described in Section 4.3 are not designed to automatically provide high availability. Supporting solution implementations for which high availability is important is not a goal of this version of the CP. However, this CP does not prohibit adding redundant components in parallel to allow for component failover or to increase the throughput of the WLAN solution, as long as each redundant component adheres to the requirements of this CP. The CP does not limit the number of WLAN Access Systems or Inner Encryption Components that can be implemented for high availability in a WLAN Solution.

An AO may additionally desire to have a wired Red Transport option for the EUDs if the WLAN access systems service is degraded, not available or unusable given the existing environment. In these cases, the AO may allow an Ethernet interface on the EUD to be activated to allow for direct connection to the CSfC Solutions Red Network. The EUD must only be used to connect to the CSfC Solution and not any other network.

4.7 IMPLEMENTING CSFC IN A HIGH ASSURANCE GOTS ENVIRONMENT

Customers have the option to use a blended solution that combines a CSfC solution with a High Assurance GOTS solution. While CSfC uses two layers of encryption, this is not required with High Assurance GOTS, where a single layer of encryption is sufficient. For example, a CSfC Campus WLAN solution can be employed in an infrastructure where network High Assurance Internet Protocol Encryptors (HAIPE) are also being used. The WLAN solution is segmented, and its protection is provided by CSfC, while the protection of the network that the information transits is provided by a High Assurance GOTS solution. For additional details or questions about this process, please contact the CSfC PMO office at csfc@nsa.gov.

5 INFRASTRUCTURE COMPONENTS

In the high-level design discussed in the previous section, at least two layers of encryption, implemented using WPA3 and an Inner layer of IPsec encryption, protect all communications flowing across a Black Network. Mandatory aspects of the solution infrastructure also include administration workstations, IDS/IPS, SIEM, firewalls, and CAs for key management using PKI.

Each infrastructure 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 and configured per NIAP configuration guidance in accordance with the Product Selection requirements of this CP (see Section 11).

Section 11 also provides details on additional components that can be added to the solution to help reduce the overall risk. Where indicated in the text, these are not considered mandatory components for the security of the solution; therefore, this CP does not place configuration requirements on those optional components.

5.1 WLAN ACCESS SYSTEM

In the context of this solution, the AP and the WLAN Controller compose the "WLAN Access System." These components are grouped together in this document to maintain vendor neutrality; there are a variety of WLAN Access System implementations across the vendor community. The WLAN Access System must be configured to use WPA3 Enterprise 192-bit mode, using AES 256, for CNSA 1.0 compliance. Objectively, the WLAN Access System should use CNSA 2.0 compliant algorithms in WPA Enterprise mode as part of the EAP-TLS connection with ML-KEM 1024 for Key Establishment and ML-DSA 87 for digital signatures as vendors enable support for these algorithms.

An AP is the media converter providing a link between the WLAN Client and the WLAN Controller. The level of functionality contained within the APs is vendor-dependent. Some solutions use "smart" or "thick" APs that incorporate a significant amount of functionality, including cryptographic operations. In this case, the APs would be considered part of the Gray Network. Other solutions implement "thin" APs that merely perform the wireless/wired media conversion and push all cryptographic functionality to the WLAN Controller. In this case, the APs would be considered part of the Black Network. If the access point is in the Black Network it has to be physically protected and access to the console port may need to be limited (e.g., tamper tape), or the port deactivated. Some vendors may produce both solutions. If WPA3 terminates on APs rather than on the WLAN Controller, then the connection between the APs and the WLAN Controller must be encrypted in a manner leveraging IPsec, SSHv2, TLS, DTLS, or TLS/HTTPS. If WPA3 terminates on the WLAN Controller, then the WPA3 encryption is used to protect the connection between the APs and the WLAN Controller. Additionally, in the cases of solutions supporting multiple security classification such as unclassified Red Network existing in conjunction with a classified network. Multiple WLAN Access Systems should be used with the centralized cryptography model where the APs are "thin" APs and feed into separate controllers for encryption.

The WLAN Access System must be capable of initiating and terminating multiple cryptographic tunnels to and from numerous Wireless Clients. It must also be capable of translating EAP-TLS over 802.1X messages to EAP-TLS over Remote Authentication Dial in User Service (RADIUS) messages to pass authentication information between the WLAN Client and WLAN Authentication Server. This exchange involves a Pairwise-Master Key (PMK) that is negotiated between the WLAN Client and the WLAN Authentication Server. The WLAN Authentication Server passes the PMK to the WLAN Access System over an IPsec tunnel, DTLS or TLS/RADsec tunnel. The Wireless Controller and the WLAN Client use the PMK to negotiate a session key to protect the subsequent user traffic exchanged between the WLAN Client and the WLAN Access System.

As mentioned above, the WLAN Access System should operate on its own separate hardware and/or virtual device(s), depending on the vendor implementation. This separation may include isolating the switches and wiring between the APs and the controller from any existing network. At the very least, the WLAN Access System and the VPN Gateway must operate on separate hardware. Since the WLAN Access System is deployed between the Black Network and the Gray Network, it is essential to

implement port filtering on the WLAN Access System's Gray Network interface to prevent unauthorized traffic. Traffic should be restricted using configuration requirements stated in Section 12.7.

5.2 GRAY FIREWALL

The Gray Firewall is located between the WLAN Access System and Inner Encryption Components. In addition to filtering EUD traffic, the Gray Firewall also provides packet filtering for the Gray Management Services.

The external interface of the Gray Firewall should only accept packets with a source address of the WLAN Access System's IP pool assigned to EUDs. The internal interface of the Gray Firewall should only accept packets with a source address of the Inner VPN Gateway as part of an established communication session. When supporting multiple security levels, the Gray Firewall must also ensure that only EUDs and Inner Encryption Components of the same security level are able to communicate. Once successfully authenticated, the Authentication Server then passes the attribute information associated with the EUD's enclave to the WLAN Access System as part of the EAP-success packet. The WLAN Controller uses the attribute information received from the Authentication Server to ensure they are placed on the proper Gray Network for their enclave and receive the correct Firewall ACL rules.

In addition to EUD data traffic, the Gray Firewall adjudicates traffic related to both the management of the Gray boundary and EUD control plane traffic. As shown in Figure 6, the Gray Firewall, selected from the CSfC Components List, must be physically separate from the WLAN Access System and Inner Encryption Components.

5.3 INNER FIREWALL

The Inner Firewall is located between the Inner Encryption Components and the Red Network. The external interface of the Inner Firewall should only accept inbound traffic with a source address of the Inner VPN Component. The internal interface of the Inner Firewall should only allow outbound traffic from the Red enclave to the Inner VPN Component.

The Inner Firewall, selected from the CSfC Components List, must be physically separate from the Inner Encryption Components.

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. The Gray Management Services are composed of multiple components that provide distinct security to the solution. The WLAN CP allows flexibility in the placement of some Gray Management Services. All components within the Gray Management Services are either directly or indirectly connected to the Gray Firewall (i.e., multiple Gray Management Services connected to a switch which is connected to the Gray Firewall). The Gray Management Services are physically protected as classified devices.

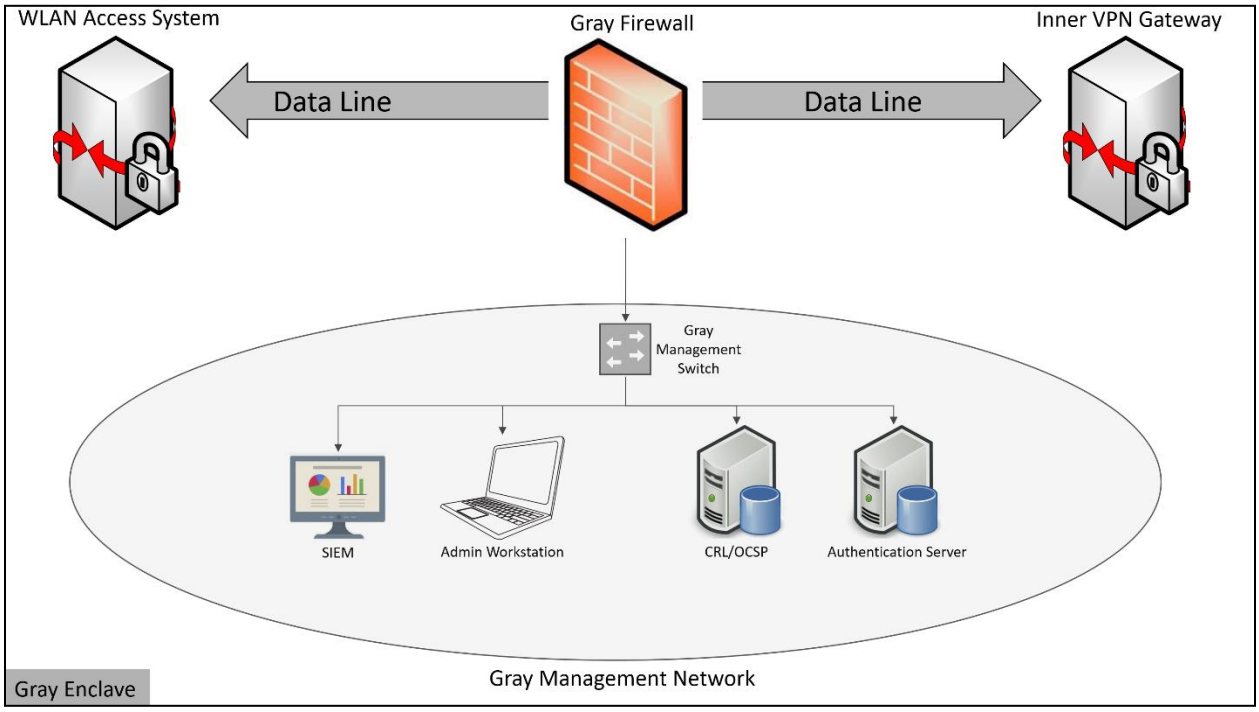

Figure 6. Overview of Gray Management Services

Figure 6 shows the infrastructure components of the Gray Management Services in the WLAN Solution. Within the Gray Network, which is between the WLAN Access System and Inner Encryption Components, there is an Administration workstation, SIEM, Authentication Server, OCSP/CRL Server and DNS. Components within the Gray Network are further described below.

5.4.1 GRAY ADMINISTRATION WORKSTATION

Gray administration workstations maintain, monitor, and control all security functions for the WLAN Access System, Gray Firewall, and all Gray Management service components. These workstations are not permitted to maintain, monitor, or control Inner Encryption Components or Red Management Services. All WLAN solutions will have at least one Gray administration workstation. Section 8 provides more detail on management of WLAN solution components.

The WLAN Access System, WLAN Authentication Server, and the WLAN Client must have an administration workstation on the Gray Management network to maintain, monitor, and control all security functionality for those devices. The administration workstations for the VPN are located on the Red Network. These administration workstations must also allow for logging and configuration management, as well as reviewing audit logs. Given the architecture of the solution, there are distinct administration networks for the WLAN Access System and VPN Gateway devices. Layer 3 routing between management and data networks must be prohibited to maintain strict separation between management and data traffic.

Administration Workstations must be dedicated for the purposes given in the CP, and must not be used to manage any non-CSfC solutions. As such, a dedicated virtual machine on an administration device used for non-CSfC solutions cannot be used to manage CSfC solutions.

5.4.2 GRAY SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

The Gray SIEM collects and analyzes log data from the WLAN Access System, Gray Firewall, and other Gray Management Service components. Log data may be encrypted between the originating component and the Gray SIEM with SSHv2, TLS, or IPsec to maintain confidentiality and integrity of the log data. The SIEM is configured to provide alerts for specific events including if the WLAN Access System or Gray Firewall receives and drops any unexpected traffic which could indicate a compromise of the WLAN Access System. These functions can also be performed on a Red SIEM if a CDS is used as described in the *CSfC Continuous Monitoring Annex*.

5.4.3 GRAY AUTHENTICATION SERVER

The Authentication Server is used to authenticate EUDs attempting to gain access to a Campus WLAN solution. The WLAN Authentication Server performs device authentication during the 802.1X exchange. The Wireless Client and WLAN Authentication Server perform an EAP-TLS over RADIUS exchange using the 802.1X protocol, with the WLAN Access System acting as a pass-through. As part of this exchange, a PMK is negotiated between the WLAN Client and the WLAN Authentication Server. The WLAN Authentication Server passes this key to the WLAN Access System in accordance with Wireless Infrastructure Authentication requirements (WLAN-IA-1 and WLAN-IA-2) to protect the subsequent user traffic exchanged between the WLAN Client and the WLAN Access System. The WLAN Authentication Server must operate on a separate hardware device from the WLAN Access System.

Campus WLAN solutions that support more than one enclave include additional requirements on the Authentication Server to ensure that EUDs are only permitted access to the correct network that directs the traffic to the appropriate Inner VPN Gateway. There are two acceptable approaches to ensure that EUDs are only permitted access to their assigned domain. The first is to maintain an allowlist of devices and the enclave for which each device is provisioned. This allowlist can be saved in a database on the Authentication Server or can be retrieved from a separate server that resides in the Gray Network. The second approach is to use information in the certificate of each EUD to make the access decision. Specifically, customers can use fields in the Distinguished Name of the Certificate (e.g., Organizational Unit Field) or use registered Policy Object Identifiers to assign EUDs to the appropriate domain. Use of Policy Object Identifiers (OIDs) is the preferred approach if supported by the Authentication Server and PKI.

The Gray Authentication Server is only required for solutions supporting multiple security levels. The authentication server is responsible for performing mutual authentication with EUDs using the WLAN Access System as an EAP pass-through. In addition to verifying that certificates are signed by the correct CA, are within their validity period, and are not revoked, the authentication server parses the certificate for information (e.g., OU field or Policy OID) that is associated with the Red Network with which the EUD is permitted to establish an Inner IPsec connection. Upon successful authentication of the EUD, the authentication server sends an Access-Accept packet to WLAN Access System. The Access-Accept packet includes an attribute derived from the OU or policy OID which the WLAN Access System uses to apply ACLs and route the EUDs traffic to the proper Inner Encryption Component.

5.5 INNER ENCRYPTION COMPONENTS

The WLAN CP allows for the use of one type of Inner Encryption Component: Inner VPN Gateway. Inner VPN Gateways are always located between the Gray Firewall and Inner Firewall. An Inner VPN Gateway will always have at least two interfaces, one external interface connected to the Gray Firewall and one internal interface connected to the Inner Firewall.

If implemented with a single data plane interface, then that interface establishes the Inner layer of encryption and provides the classified data to the EUD. Inner VPN Gateways must be managed from the Red Management Services. The management interface of the Inner VPN Gateway can either be connected to the Inner Firewall or run directly to a standalone Red Management Services enclave.

Multiple Inner Encryption Components are acceptable, provided they comply with the requirements of this CP.

5.5.1 INNER VPN GATEWAY

The Inner VPN Gateway provides authentication of peer VPN Components, cryptographic protection of data in transit, and configuration and enforcement of network packet handling rules. The Inner VPN Gateway is located between the Gray Firewall and the Inner Firewall. The Inner VPN Gateway is required to be implemented if supporting VPN EUDs.

The external interface of the Inner VPN Gateway is connected to the internal interface of the Gray Firewall. The VPN Gateway establishes an IPsec tunnel with peer Inner VPN Components. The external interface of the Inner VPN Gateway only permits the egress of IPsec traffic and AO-approved control plane traffic. The internal interface of the Inner VPN Gateway is configured to only permit traffic with an IP address and port associated with Red Network services.

The Inner VPN Gateway cannot directly 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 and routed through an IPsec VPN tunnel that is configured according to this CP. The Inner VPN Gateway, selected from the CSfC Components List, must be physically separate from the Gray Firewall and Inner Firewall.

5.5.2 CNSA 2.0 IPSEC

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

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

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

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

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

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

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

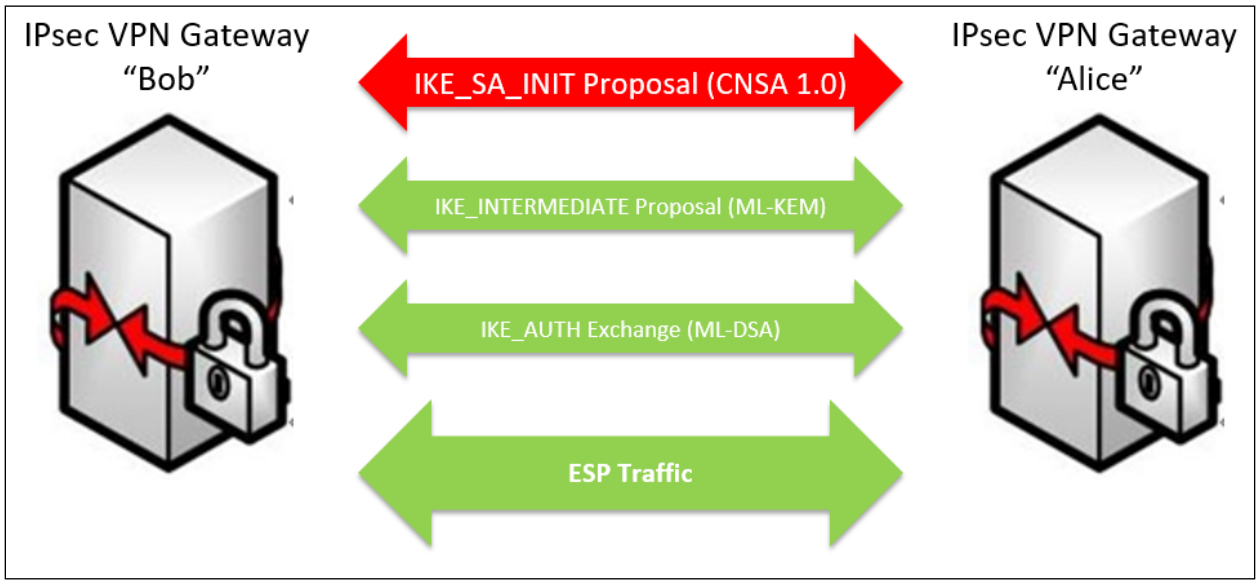

Figure 7. CNSA 2.0 IKEv2 Exchanges

As detailed in Figure 7, RFC 9370 enables peers to perform multiple key exchanges. The key-establishment algorithm used in the Initial IKE SA (IKE_SA_INIT) exchange must be constrained enough in size as to not induce IP fragmentation. The ML-KEM-1024 public key and ciphertext sizes are too large for this initial exchange and thus the IKE_SA_INIT exchange must use a CNSA 1.0-compliant key establishment algorithm. A subsequent Intermediate IKE (IKE_INTERMEDIATE) exchange (as specified in RFC 9242) is then used to perform an ML-KEM key establishment. This second exchange, encrypted using keys established by IKE_SA_INIT, can leverage the IKEv2-level fragmentation mechanism specified in RFC 7383.

5.6 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. The WLAN CP allows flexibility in the placement of some Red Management Services as described below.

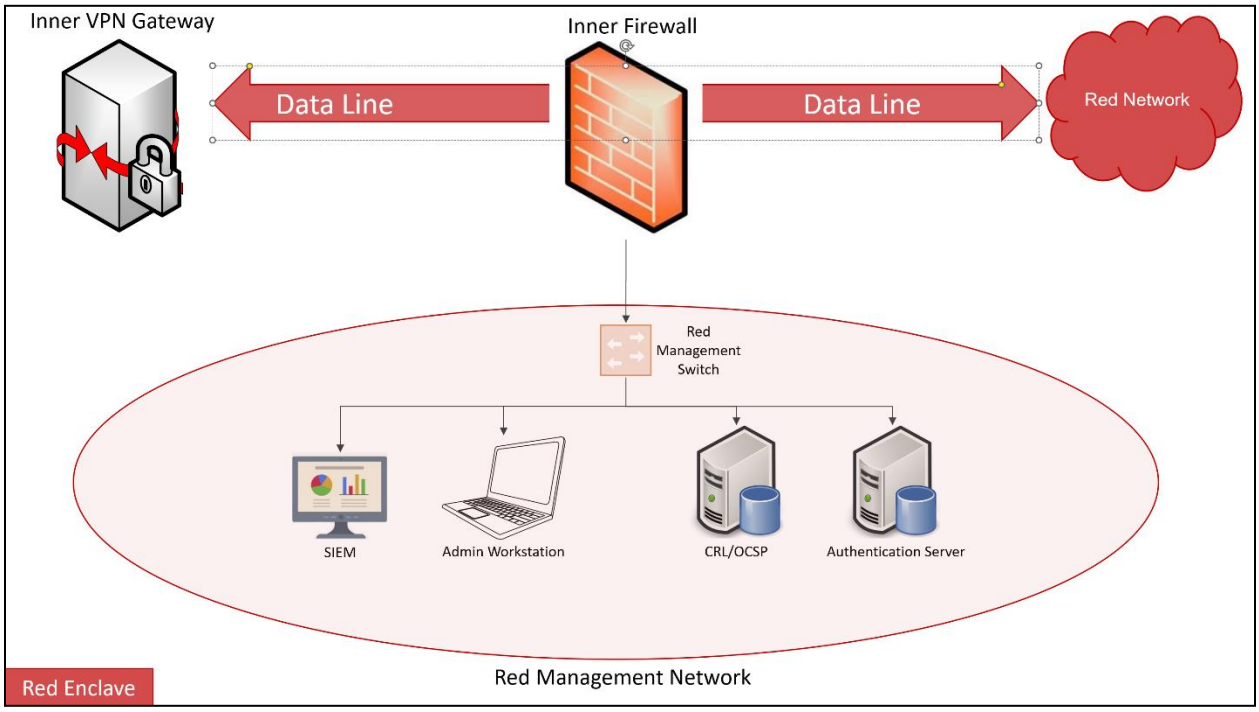

Figure 8. Overview of Red Management Services

Figure 8 shows the infrastructure components of the Red Management Services in the WLAN Solution. The Red Network, located beyond the Inner Encryption Components, has management services components. Each of the management services components are described below.

5.6.1 RED ADMINISTRATION WORKSTATIONS

The Red administration workstation maintains, monitors, and controls all security functionality for the Inner Encryption Components, Inner Firewall, and all Red Management service components. The Red administration workstations are not permitted to maintain, monitor, or control Outer Encryption Components or Gray Management Services. All WLAN solutions will have at least one Red administration workstation. Section 8 provides more detail on management of WLAN solution components.

5.6.2 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 may be encrypted between the originating component and the Red SIEM with SSHv2, TLS, or IPsec to ensure confidentiality and integrity. The SIEM is configured to provide alerts for specific events. Customers are encouraged to leverage existing Enterprise SIEM capabilities to monitor log data from Inner Encryption Components, the Inner Firewall, and Red Management Services. 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 the *CSfC Continuous Monitoring Annex*.

5.7 PUBLIC KEY INFRASTRUCTURE COMPONENTS

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

5.8 SOFTWARE AND FIRMWARE SIGNINGS

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

There are three acceptable algorithms for software and firmware digital signatures, which are all included as part of the CNSA 2.0 cipher suites. These algorithms are enumerated within Table 1 and only one of the algorithms will be required to meet this requirement.

Table 1. CNSA 2.0 Algorithms for Software and Firmware Signing

Algorithm	Function	Specification	Parameters
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels. SHA-256/192 recommended.
Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels
ML-DSA	Asymmetric algorithm for digital signatures	FIPS 204	Category 5 parameter, ML-DSA87

6 END USER DEVICE COMPONENTS

This section covers the components that make up an EUD and different permutations of these components to create a more secure EUD. There are two broad categories for EUDs within Campus WLAN:

1) an MDF EUD which is an EUD listed on the *Mobile Platform* section of the CSfC Components List
2) a Composed EUD, which is an EUD made up of multiple sub-components from the CSfC Components List. The responsibility of selecting and composing these sub-components into a functioning EUDs is up to the customer and/or trusted integrator.

The CSfC Program does not guarantee the interoperability of the different sub-components. The sub-components that makeup a composed EUD include the following:

- General Purpose Operating Systems or

- Client Virtualization Systems;
- WLAN Clients;
- General Purpose Compute Platform;
- Dedicated Security Component (Optional);
- Hardware Full Drive Encryption or
- Software Full Drive Encryption.

A Composed EUD and MDF EUDs can be configured in multiple ways depending on the technology being used to implement the EUD. The following table summarizes these options:

Table 2. EUD Type Summarization

EUD Configuration	Description	Benefit
Base EUD	An EUD built to function within the constraints of a typical OS or MDF platform	Minimum Standard for EUDs within CSfC
Software Separated EUD	An EUD built around a standard OS with a virtualization functionality, containerization engine or kernel separation running to abstract out critical function	Offers more usability but no difference in security than base EUD (Individual deployments may be more secure)
Virtualized EUD: Type 1 Hypervisor with Hardware Abstraction	An EUD built around a Type 1 Hypervisor with hardware abstraction capabilities to separate the critical functions into separate virtual instances	Offers more usability and increases the security of an WLAN EUD with abstraction of the Wi-Fi driver and hardware
Hardware Separated EUD	An EUD with critical functions such as transport, encryption and Red Compute into separate dedicated hardware components	High risk functions are physically separated into separate hardware such as the Dedicated Outer WLAN use case

See Appendix E for a more detailed version of this table.

6.1 EUD HARDWARE PLATFORM

For a Composed EUD, the EUD Hardware Platform is the physical hardware that the other sub-components of the EUD operates on. All Composed EUDs must have an EUD Hardware Platform that is listed on the CSfC Components List as an EUD Hardware Platform. The platform typically is a traditional laptop, computer, tablet, smartphone or other such end user form factor but may be a server or other computing form factor.

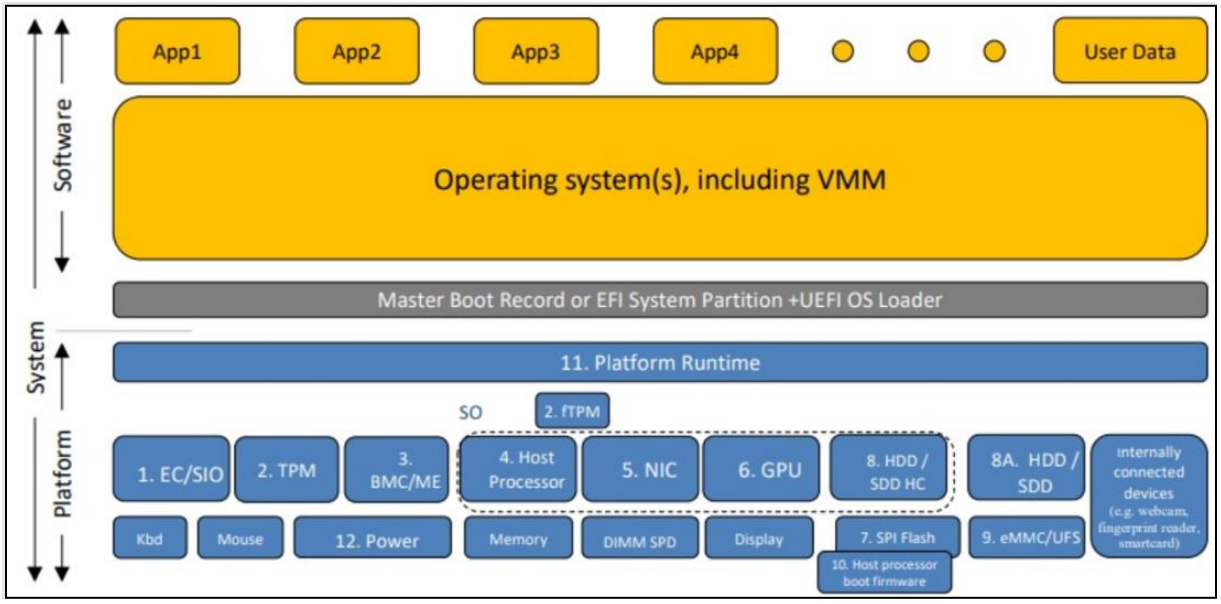

Figure 9. General Purpose Computing Platform

6.2 DEDICATED SECURITY COMPONENT

The Dedicated Security Component (DSC) is a combination of a hardware component and its controlling firmware that provides a secure execution environment, key storage and/or other security related functionality to the composed EUD. Currently, a DSC is not required but is an optional sub-component that will further enhance the security of all EUDs. These dedicated security components should take the form of Secure Elements (SE), Trusted Platform Modules (TPM), Hardware Security Modules (HSM), Trusted Execution Environments (TEE), and Secure Enclave Processors (SEP). The firmware of these should provide the encompassing platform with services for the provisioning, protection, and use of Security Data Objects (SDOs), which include keys, identities, attributes, and other types of Security Data Elements (SDEs).

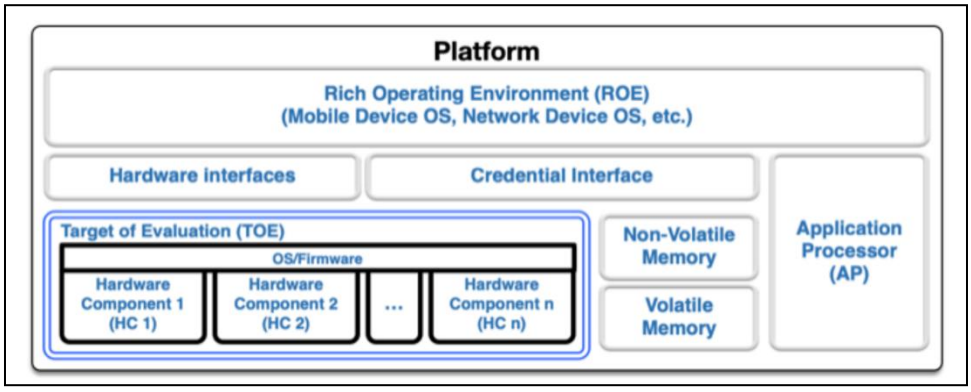

Figure 10 . Dedicated Security Component

It is expected that the DSC will be integrated into the EUD Hardware Platform or have an already tested DSC integrated into it the EUD separately. MDF EUDs can additionally leverage the DSC to provide the

same functionality as the composed EUDs. Currently, a DSC is an objective design feature for all EUDs but is intended to become threshold in the future.

6.3 Operating System

For Composed EUDs the OS is software that manages computer hardware and software resources for EUDs and provides common services for application programs. The hardware it manages may be physical or virtual. The OS encompasses the OS kernel and its drivers, shared software libraries, and some application software included with the OS. Applications included are those that provide essential security services, many of which run with elevated privileges.

6.4 WLAN Client

The WLAN Client is a software application running on the EUD that provides management and control of the wireless connection. The WLAN Client is a sub-component of the OS and should be paired with the given OS or MDF Platform. The products chosen to implement the WLAN Client services must provide a base level of protection and should be able to interoperate with products from other vendors. The products must also provide cryptographic and functional services that meet or exceed the requirements listed in Section 12 for the WLAN Client. The WLAN Client automatically establishes the WPA3 tunnel between the EUD and the WLAN Access System using EAP-TLS over 802.1X to pass Public Key device certificates for mutual authentication between the WLAN Client and WLAN Authentication Server.

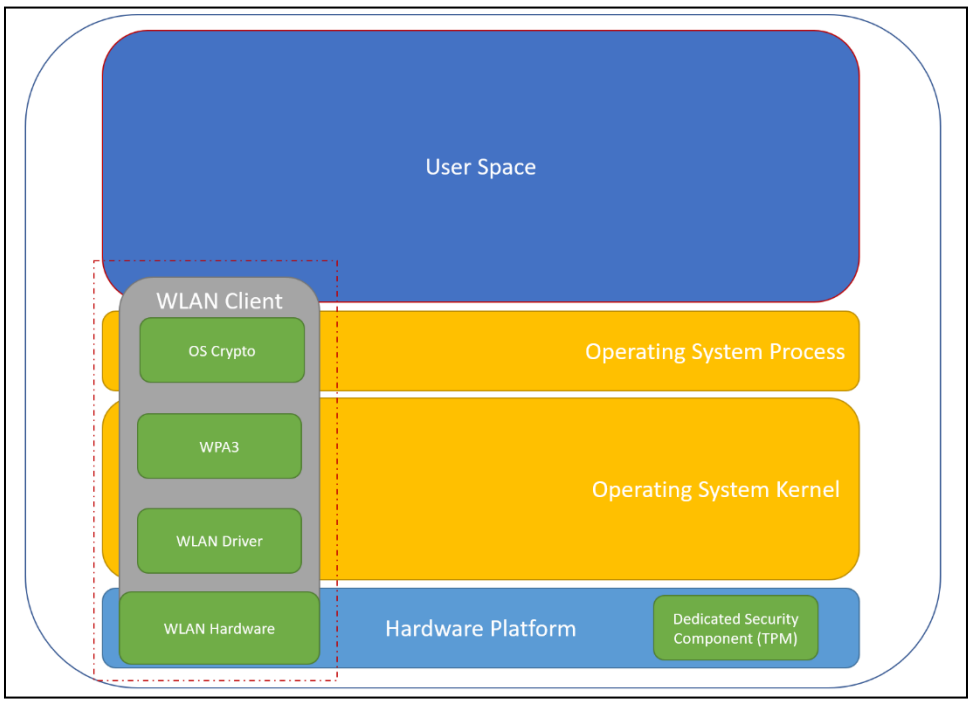

Figure 11. EUD WLAN Client

6.5 DEDICATED OUTER WLAN

A Dedicated Outer WLAN can be used as the WLAN Client for EUDs. Using a physically separate Outer Encryption Component as part of the EUD improves security by providing physical separation between the Computing Device and the Outer layer of encryption. When using a Dedicated Outer WLAN, the Dedicated Outer and Computing Device are collectively referred to as the EUD.

The Dedicated Outer WLAN included as part of the EUD must be physically connected to the computing platform using an Ethernet cable. The Dedicated Outer WLAN is selected from either the WLAN Access System section or the WLAN Client section of the CSfC Components List.

When a Dedicated Outer WLAN is included as part of an EUD, it provides configuration and enforcement of network packet handling rules for the Outer layer of encryption. The configuration settings of the Dedicated Outer WLAN may need to be updated when entering new environments (e.g., updating the Default Gateway). Dedicated Outer WLANs are dedicated to a single security level and can only provide the Outer layer of WPA3 encryption for clients connecting to a Red Network of the same security level.

6.6 VPN CLIENT

The VPN Client is a software application running on the EUD. The products chosen to implement the VPN services must provide cryptographic and functional services that meet or exceed the requirements listed in Section 12 for the VPN Client.

The VPN Client establishes an IPsec tunnel to the VPN Gateway. The VPN Client first performs an Internet Key Exchange (IKE) with the VPN Gateway to authenticate both parties and exchange session keys for the IPsec tunnel. Authentication is performed via mutual authentication of Public Key device certificates. When IKE completes, the IPsec tunnel is secured using the ESP. The Inner VPN Tunnel must use Tunnel Mode IPsec or Transport Mode IPsec using an associated IP tunneling protocol (e.g., Transport Mode IPsec with GRE).

For information on the objective requirements and implementation notes on the VPN Client performing authentication using CNSA 2.0 compliant algorithms see section 5.5.2.

6.7 HYPERVISOR

The Hypervisor, also referred to as the Client Virtualization, is a virtualization engine that runs on the EUD hardware in place of an OS and its Kernel. It runs additional guest operating systems and their guest kernels. The Hypervisor used is considered to be a Type One Hypervisor where the virtualization engine directly runs on the hardware platform instead of running on a separate OS. The Type One Hypervisor has a great deal of high-level separation that includes kernel separation and limited hardware separation. One of these Hypervisors is expected to implement the following features to isolate the VM handling the Wi-Fi Driver from the rest of the virtual machines (VM) and Hypervisors:

- PCIe Passthrough Technology where the Wi-Fi card is passed through to the Wi-Fi VM for it to run the driver instead of the Hypervisor or other guest VMs
- Memory Isolation where each VM can be allocated its own separate memory space to ensure separation between the VMs memories
- Processor Pinning where the individual processors of a system can be dedicated to processing a single VM

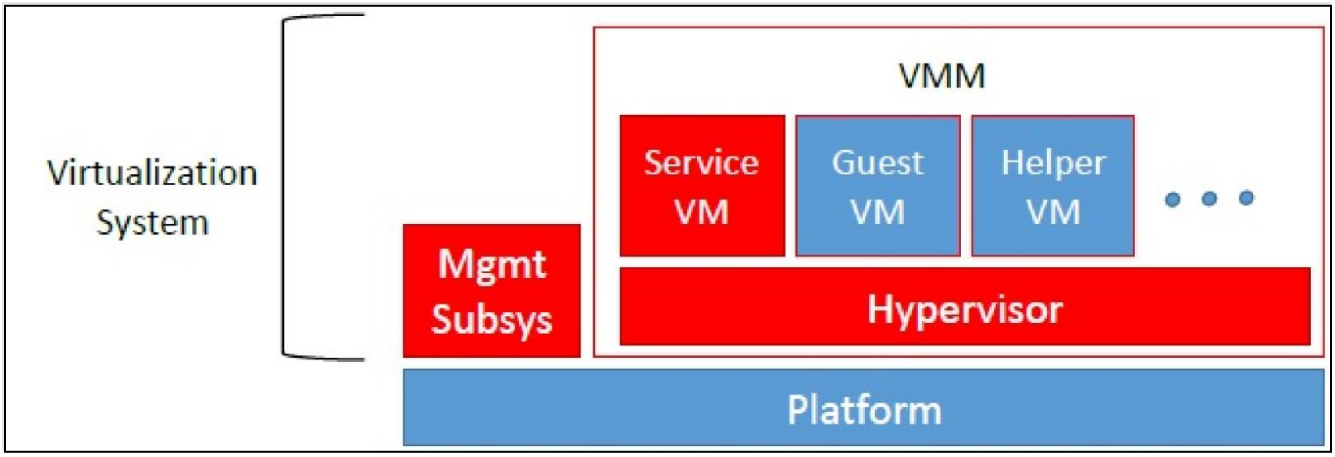

Figure 12. Virtualization Client

6.8 END USER DEVICES FULL DISK ENCRYPTION

A Composed EUD is required to have a single layer of Full Drive Encryption (FDE) enabled to act as a base level of protection to the EUD protecting it from unauthorized modification and data recovery efforts. MDFs EUDS already have a single layer of Platform Encryption already part of the architecture and it is required for this to be enabled for these EUDs as well. For more information on how encryption relates to device handling, see section 7.2.

6.9 MDF END USER DEVICE

The MDF EUD is a commercial tablet, smartphone, or similar computing device that supports Wi-Fi connectivity options.

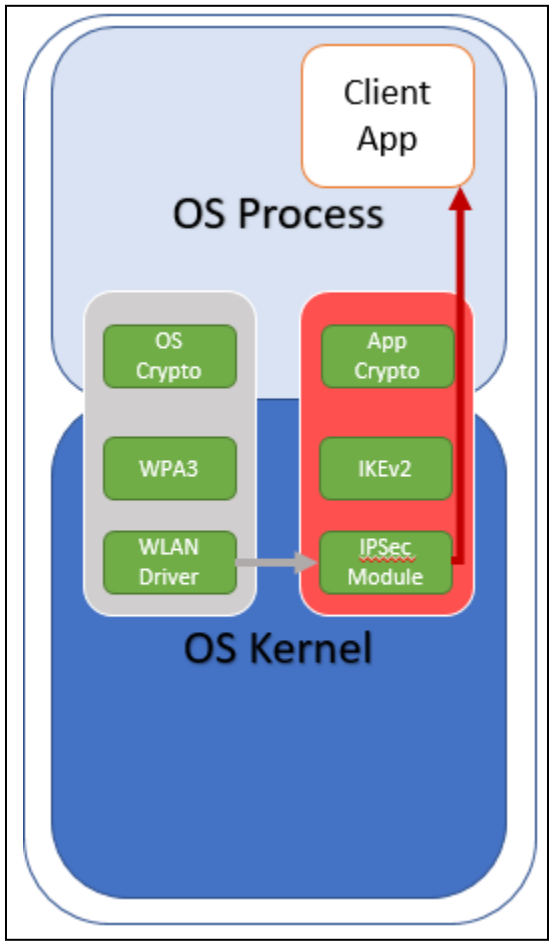

Figure 13. Campus WLAN MDF EUD Architecture

Figure 13 shows the software architecture of a typical Mobile Device Fundamentals (MDF) EUD. The VPN Client and WLAN Client run as operating system processes and exist to perform authentication and key establishment for the IPsec module and WPA3 driver respectively.

EUDs use WPA3 using a WLAN Client (also known as WPA supplicant) to provide the Outer layer of encryption. The WLAN Client establishes an encrypted connection to the WLAN Access System. The connection can be configured to automatically be established as part of the EUD's power-on process. Once connected to the WLAN Access system, the EUD can establish the Inner IPsec tunnel. The private keys and certificates used for the authentication of the WLAN Access System are considered Controlled Unclassified Information (CUI) and must be, at a minimum, protected by enabling the native platform DAR protection.

For MDF EUDs, the *Mobile Platform* section of the CSfC Components List already includes the required sub-components but, does not include the DSC as it currently is an objective design feature of the EUD.

A VPN Client must be used as the Inner VPN Component for EUDs. The Inner VPN Client establishes an IPsec tunnel to the Inner VPN Gateway of the WLAN Solution Infrastructure. The tunnel can be configured to automatically be established as part of the EUD's power-on process. A combination of the VPN Client and the Operating System on which it is installed, provides configuration and enforcement of

network packet handling rules for the Inner layer of encryption. The Inner VPN Client is selected from the *IPsec VPN Client* section of the CSfC Components list. The VPN Client is installed on the Computing Device selected from the *Mobile Platform* section of the CSfC Components List. The private keys must be classified as determined by the AO and compliant with CNSSI 4005 and certificates used for the authentication of the Inner VPN Gateway are considered CUI and must be, at a minimum, protected by enabling the native platform DAR protection.

When using virtualization, a WLAN Client and Inner VPN Client both reside on the same Computing Device but are operating in two virtual instances to ensure that two separate IP stacks are used. The EUD is to be used exclusively within physically secure environments, such as facilities and tactical environments with physical controls considered appropriate by the AO.

6.10 Composed End User Device Components

The Composed EUD is a commercial tablet, laptop computer, or similar computing device that supports Wi-Fi connectivity options.

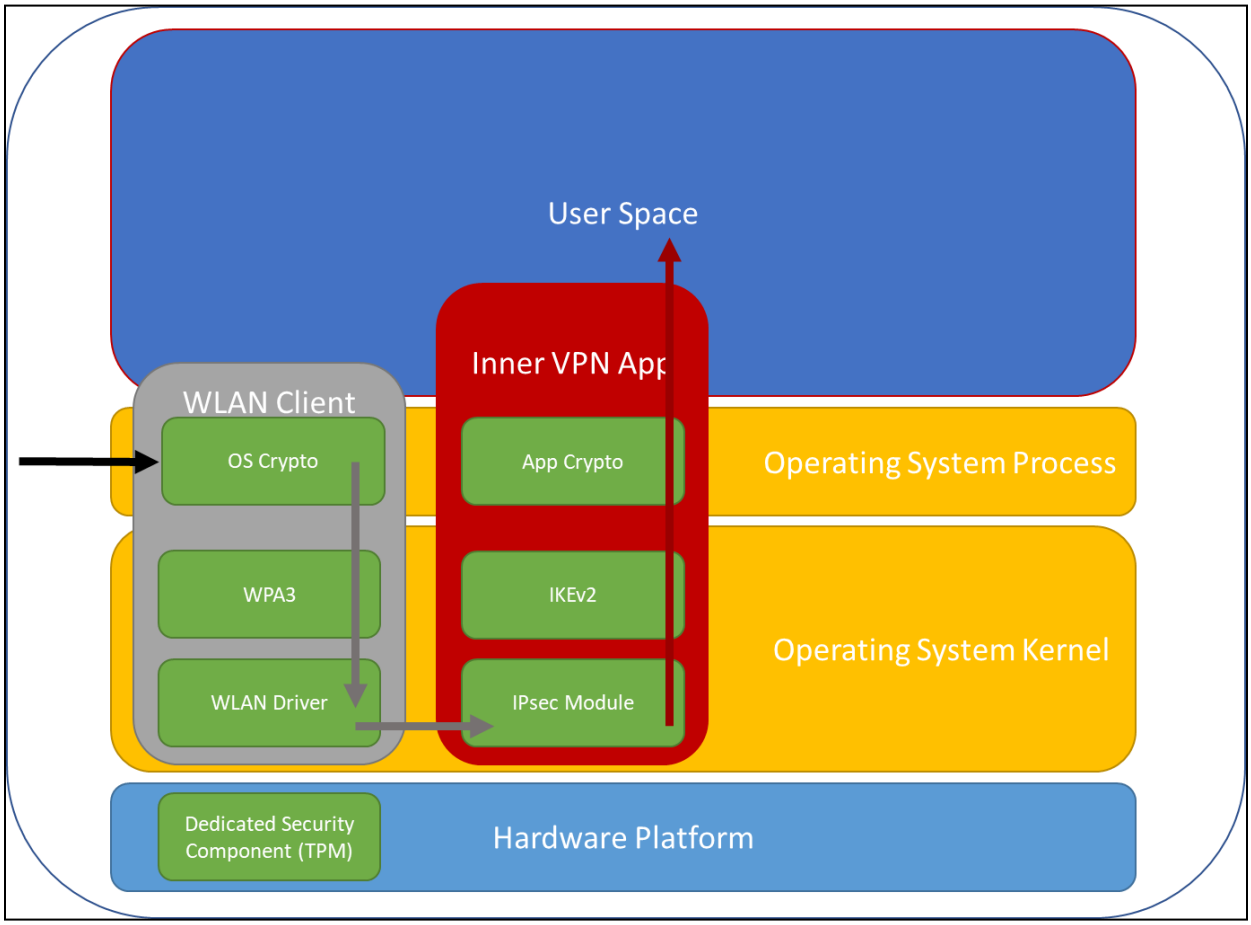

Figure 14. Campus WLAN Composed EUD Architecture

Figure 14 shows the software architecture of a typical Composed EUD, also referred to as a base EUD. This section additionally applies to Software Separated EUDs as the component selection is the same.

The VPN Client and WLAN Client run as operating system processes and exist to perform authentication and key establishment for the IPsec module and WPA3 driver respectively.

EUDs use WPA3 using a WLAN Client (also known as WPA supplicant) to provide the Outer layer of encryption. The WLAN Client establishes an encrypted connection to the WLAN Access System. The connection can be configured to automatically be established as part of the EUD's power-on process. Once connected to the WLAN Access system, the EUD can establish the Inner IPsec tunnel. The private keys and certificates used for the authentication of the WLAN Access System are considered Controlled Unclassified Information (CUI) and must be, at a minimum, protected by enabling the native platform DAR protection.

The Composed EUD must be made from the sub-components described in Table 3.

Table 3. Composed EUD Sub-Components

Component	CSfC Component Category
EUD Hardware	General Purpose Computing Platform
EUD- Dedicated Security Component (Optional)	*Dedicated Security Component*
OS	General Purpose Operating Systems
WLAN Client	WLAN Client
Inner VPN Client	IPsec VPN Client
EUD DAR Encryption	Hardware Full Drive Encryption or Software Full Drive Encryption

The EUD consists of the hardware and software components (Operating System (OS), VPN client, WLAN Client, and applications) that provide a variety of security services. The Composed EUD itself is run on physical hardware selected from the CSfC Components list for General Purpose Computing Platform. The hardware may integrate a DSC that is chosen from the CSfC Components List for DSC. The EUD's OS must be chosen from the CSfC Components List for General Purpose Operating Systems. Composed EUDs may rely on virtualization instead of an OS for more information see section 6.10.1. The WLAN Client must be chosen from an OS that is listed on the CSfC Components List for WLAN. The VPN Client must be chosen from the CSfC Components List for VPN Client and be deployed on the tested EUD's OS. For encryption, the EUD must use an encryptor chosen from the CSfC Components List for Software, Hardware, or Platform encryptor. For DAR CP compliant devices refer to DAR CP for all requirements on selecting EUD encryption. A VPN Client must be used as the Inner VPN Component for EUDs. The Inner VPN Client establishes an IPsec tunnel to the Inner VPN Gateway of the WLAN Solution Infrastructure. The tunnel can be configured to automatically be established as part of the EUD's power-on process. A combination of the VPN Client and the Operating System on which it is installed, provides configuration and enforcement of network packet handling rules for the Inner layer of encryption. The Inner VPN Client is selected from the *IPsec VPN Client* section of the CSfC Components List. The VPN Client is installed on the Composed EUD. The private keys must be classified as determined by the AO in

accordance with CNSSI 4005 and certificates used for the authentication of the Inner VPN Gateway are considered CUI.

6.10.1 VIRTUALIZED EUD

In this CP, the EUD relies on a single operating system to connect to the WLAN Access System, the Inner Encryption Component and user space. To create an additional layer of security, this function of the EUD may be isolated on the EUD. This isolation is achieved through the use of hypervisor and virtual machine technologies on the EUD. Both a Composed EUD can leverage virtualization technologies to improve security, usability, or user experience.

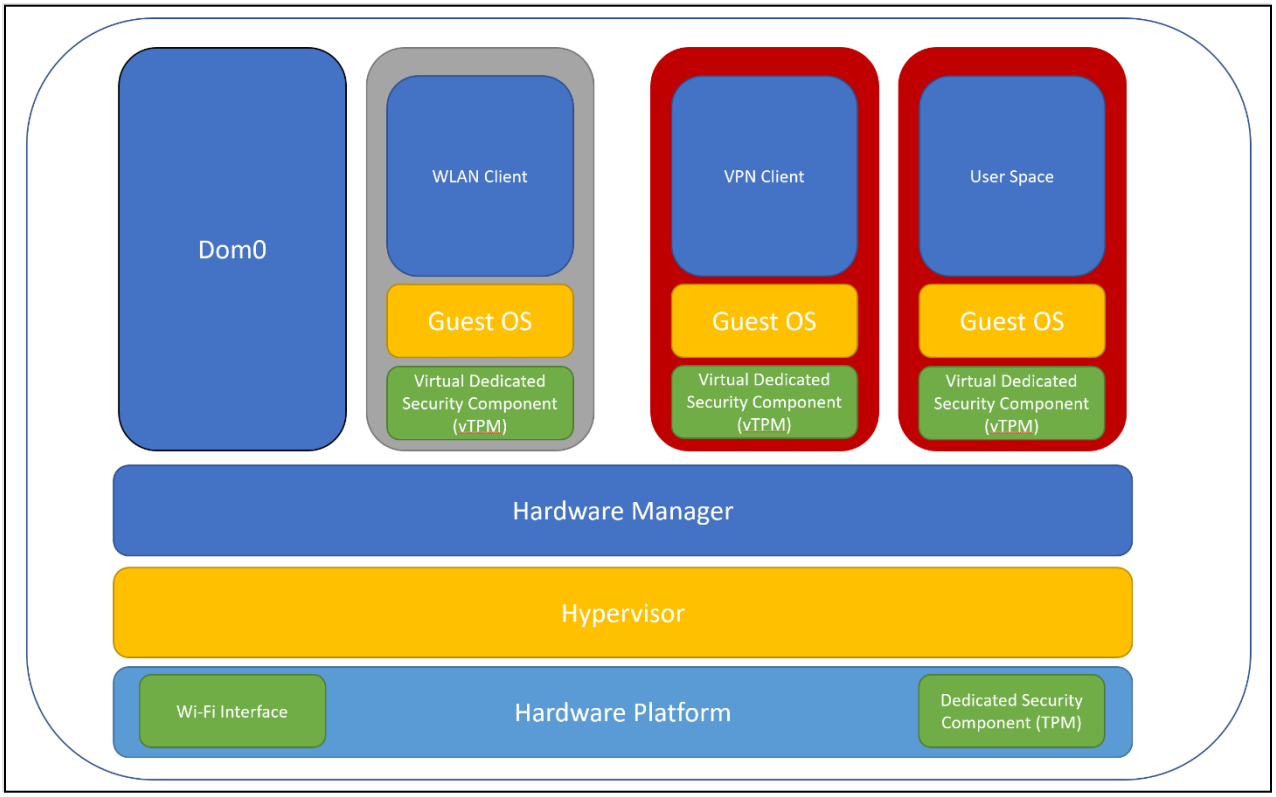

Figure 15. Enhanced Software Virtualization Architecture

Virtualized EUDs use a Type 1 Hypervisor running directly on the hardware to create multiple isolated and stand-alone domains on a single EUD. The most common form of one of these domains is a VM. The isolated domains allow multiple parts of a Campus WLAN EUD to be built securely into a single piece of hardware. They also ensure that separate IP stacks are used for each connection layer. The hypervisor also provides the virtual networks that are used by the domains for the internal network connections required for the dual layer WLAN connection.

The Hypervisor, also referred to as the Client Virtualization, is a virtualization engine that runs on the hardware of the EUD in place of an OS and its Kernel. It runs additional guest operating systems and their guest kernels. The Hypervisor being used is considered to be a Type One hypervisor where the virtualization engine directly runs on the hardware platform instead of running on a separate OS.- The Type One Hypervisor has a high level of separation that includes kernel separation and limited hardware separation. This hypervisor must be listed on the CSfC Components List for Client Virtualization as

described in section 6.7. If a virtualization, containerization, or other such software separation technology is used then it must be listed on the CSfC Components List for OS.

Table 4. Virtualized EUD Components

EUD Component	CSfC Components List
EUD Hardware	*General Purpose Computing Platform*
EUD- Dedicated Security Component (Optional)	*Dedicated Security Component*
Hypervisor	*Client Virtualization*
WLAN Guest Operating System	*General Purpose Operating Systems*
WLAN Client	*WLAN Network Client*
Inner VPN Client	*VPN Client*
EUD Encryption	*Hardware Full Drive Encryption or Software Full Drive Encryption*

Each isolated domain should include the following subdomains: 1) a user domain where the user can interact with the EUD, 2) a transport domain to connect the WLAN Access System and, 3) a transport domain to connect to the Inner VPN Gateway.

Virtualized EUD has a virtual OS dedicated to the WLAN Client and as this WLAN client is acting as the Outer Encryption layer this OS must be chosen from the CSfC Components List for WLAN Clients and OSs. End users should only be able to access end user domains. Other domains should be managed by an administrator. Additional domains/VMs can also be added for device management functions.

6.10.1.1 VM Architecture

Within the Composed Virtualized EUDs there are several methods and architectures that may be used to create an EUD that meets the requirements of a Virtualized EUD. This document will not prescribe any particular architectures but instead present concepts and best practices that should be used in implementation of the Composed Virtualized EUDs. These concepts include:

- VM Interconnectivity
- Limited VMs
- Read Only VMs

6.10.1.2 VM Interconnectivity

The separation that the Type 1 hypervisor adds between the VMs must be considered when doing the interconnection between the VM for the data to make its way from the Black untrusted network to the Red user space. All VMs should have their connection limited to what is necessary for the VMs to function for their given application. Most hypervisors have virtualized switching technology that can be used to allow routing between the VMs and even the hypervisor. These virtual switches should be

separated out by the data type handles such as black, gray, and red. For example, there should be a separate virtual switch that handles the Black data, Gray data, Red data, and a dedicated switch to pass data between the Black Network and the Black VM. Figure 16 depicts Virtual EUDs with separate virtual switches allowing for communication between the VMs with each switch dedicated to the type of data transiting the switch.

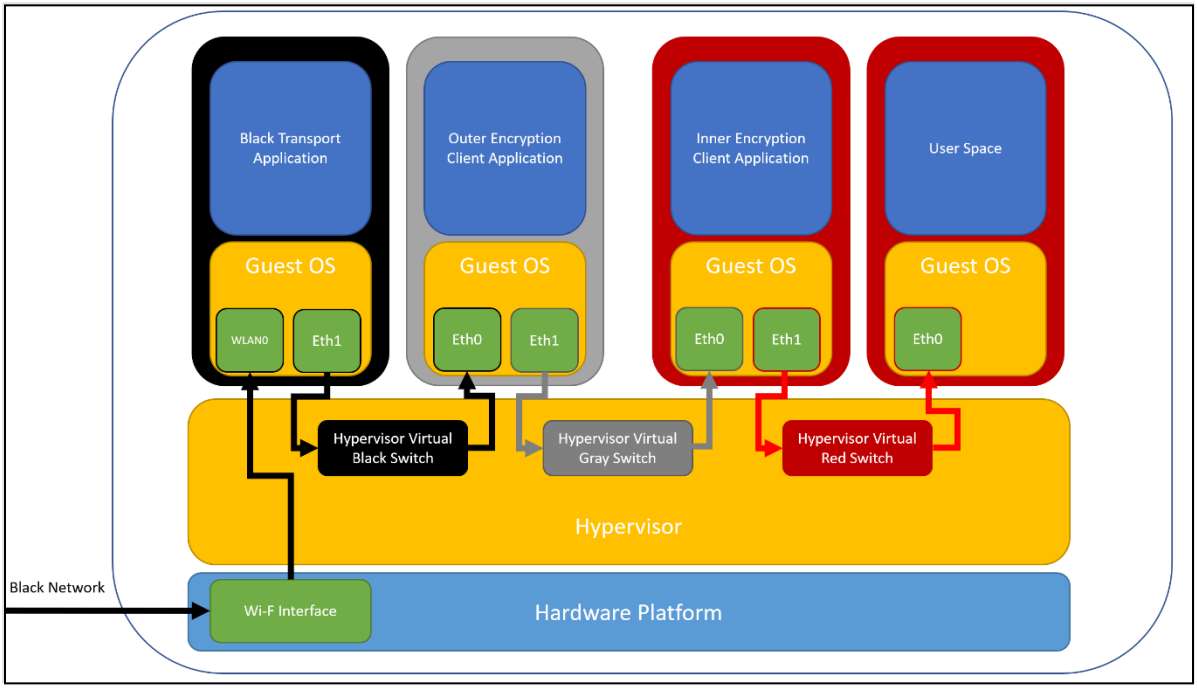

Figure 16. VM Interconnectivity

Another additional function that can be leveraged is for the VMs to run an independent firewall in each guest VM. This limits what the VM can send and receive on its own interfaces and adds an additional layer of network security to the EUD.

6.10.1.3 VM Interconnectivity

VM within a virtual EUD should be limited to only have the necessary core functions required for operation. All other additional functionality should be removed. An example of this is the Outer Encryption VM should only have the outer encryption client, network supplicants, firewall, and any additional supporting libraries and should have any non-essential functionality. Non-essential functionality can include user applications, text editors, and even user interfaces. These principals limited functionality should be applied to all VMs within a virtual EUD to further reduce the attack surface which each VM presents to the virtual EUD.

6.10.1.4 Read Only VMs

Within Virtualization technology is the concept of 'Read Only' VMs where the file system of the virtualized guest's OS is in a 'read only' state. In this state, no changes to the guest OS's file system are permanent nor are the changes to these OSs persistent through rebooting the VMs. This guarantees that the VMs will always boot into a known good state and any errors that occur within the VM are not

persistent on reboot. These traits are very beneficial for VMs that handles the network functionality of the EUD. Additionally, this prevents any modification to the file system and reduces persistence through reboots. Within CSfC, this technology is not required to be deployed within a Virtualized EUD, but it is recommended that the Integrator consider technologies such as this to reduce the risk of operating the solution and improve the usability of the EUDs.

6.11 Hardware Separated EUDs

This section expands upon the concept of multiple components making up a single EUD. This concept is exemplified by the Dedicated Outer WLANs that can be paired with a traditional EUD. This is done to pass along functionality that causes risk to a separate component other than the EUD handling red data or having the separate hardware perform a function that the EUD is incapable of performing. This concept can be expanded on to further enhance the security of an EUD or allow for EUDs that cannot meet the requirements placed on traditional EUDs such as a laptop, smartphone, tablet, or computer.

The concept of multiple EUD components will expand to include both a Dedicated Inner VPN and a Red Compute Hardware. This allows for EUDs that cannot operate the Inner Encryption to still be used with CSfC or to pass along the risk from the Red Compute to the other dedicated component. The Dedicated Outer, Inner and Red Compute Hardware are objective design features within a CSfC Solution and are not required to be implemented by the customer.

6.11.1 Dedicated Outer WLAN (Outer Wireless Access)

A Dedicated Outer WLAN can be used as the Outer WLAN Component for EUDs. Using a physically separate WLAN client as part of the EUD improves security by providing physical separation between the Computing Device and the Wi-Fi. When using a Dedicated Outer WLAN, the Outer WLAN and Computing Device are collectively referred to as the EUD.

The Dedicated Outer WLAN included as part of the EUD must be physically connected to the computing platform preferably using an Ethernet cable. The Dedicated Outer WLAN is selected from either the WLAN Access System section or the WLAN *client* section of the CSfC Components List.

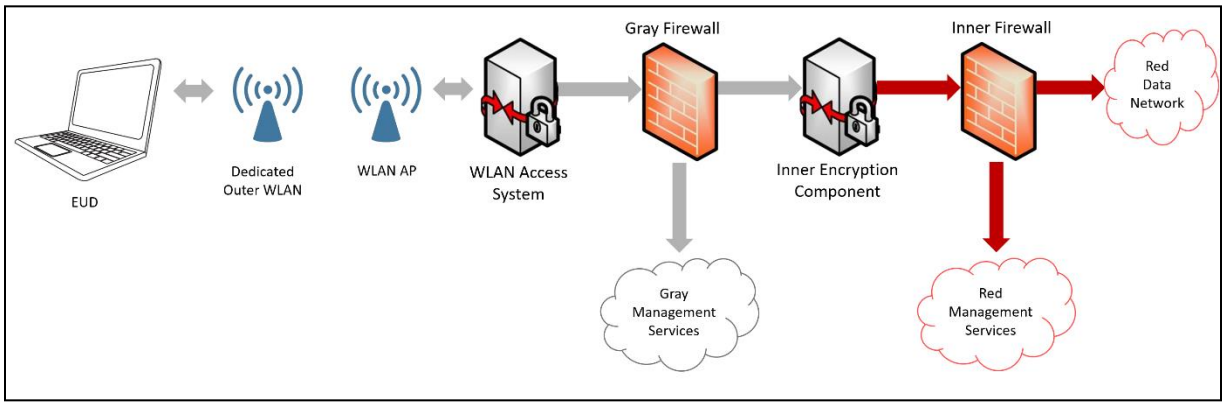

Figure 17. Dedicated Outer WLAN

When a Dedicated Outer WLAN is included as part of an EUD, it provides configuration and enforcement of network packet handling rules for the Wi-Fi. Dedicated Outer WLANs are dedicated to a single security level and can only provide the Wi-Fi for clients connecting to a Red Network of the same security level.

6.11.2 DEDICATED INNER VPN (INNER ENCRYPTION COMPONENT)

A Dedicated Inner VPN is a separate component that can be used as the Inner VPN for an EUD. Additionally, Dedicated Outer WLAN is required when a Dedicated Inner VPN is used. These Dedicated Inner VPNs normally are small travel routers or similar network gear. The Dedicated Inner VPN included as part of the EUD must be physically connected to the computing platform using a wired connection preferably an Ethernet cable. A Dedicated Outer and Dedicated Inner may be combined into the same hardware, though for this use case it is preferred to have these to be separate components.

For the first option with the Dedicated Inner VPN being a travel router or other similar component, the Dedicated Inner VPN is selected from either the *IPsec VPN Gateway* section or the *IPsec VPN Client* section of the CSfC Components List. When a Dedicated Inner VPN is included as part of an EUD, it provides configuration and enforcement of network packet handling rules for the Inner layer of encryption. The configuration settings of the Dedicated Inner VPN may need to be updated when entering new environments (i.e., updating the Default Gateway). Dedicated Inner VPNs are dedicated to a single security level and can only provide the Inner layer of IPsec for clients connecting to a Red Network of the same security level.

When the Dedicated Inner VPN is a composed EUD the OS is selected from the *OS* section of the CSfC Components List. The Dedicated Inner VPN hardware is selected from the *Hardware Platform* section of the CSfC Components List. The Dedicated Inner VPN hardware is selected from the *Hardware Platform* section of the CSfC Components List. Finally, the Dedicated Inner VPN's VPN is selected from the *IPsec* VPN Client section of the CSfC Components List. Dedicated Inner VPNs are dedicated to a single security level and can only provide the Inner layer of IPsec for clients connecting to a Red Network of the same security level.

6.11.3 RED COMPUTE HARDWARE

The Red Compute Hardware is a dedicated Red Component whose role is to only handle the classified information and not to handle any of the encryption required to connect to a CSfC Solution. This dedicated Red Compute is expected to be Smartphone, Tablet, Laptop, or other standard EUD but may additionally be a non-traditional compute platform that does not fit in the concept of EUDs. The Red Compute must be physically connected to the Dedicated Inner VPN using a wired connection preferably an Ethernet cable.

6.12 ACCESS CDS EUDS

Access Cross Domain Solutions (CDS) are a type of CDS that provides access to a computing platform, application, or data residing on different security domains from a single device without any transfer between the various domains. Access CDSs are used within CSfC solutions to fully replace a traditional EUD. Thus, the National Cross Domain Strategy Management Office (NCDSMO) and the CSfC Program have partnered together to provide this guidance. The specific CDS targeted here are Access CDSs that rely of virtualization technologies for separation of different domains. These Access CDS must go

through a validation process and then it may be listed on the CDS Baseline. For any additional information on CDS contact the NCDSMO at ncdsmo@nsa.gov or local CDS support element.

Reciprocity between the NCDSMO Baseline and the CSfC Components List allows the NCDSMO Baseline to be equivalent to the General-Purpose Compute Platform and Virtualization Client. All Access CDSs will not be automatically allowed to act as a CSfC EUD, they will only be allowed on a case-by-case basis based on input on the CSfC program and the NCDSMO. To allow for an Access CDS to be used within a CSfC Solution contact the CSfC Program Management Office (PMO), csfc@nsa.gov, to discuss the requirements and necessary information to allow for an Access CDS within CSfC Solutions.

Table 5. Access CDS EUD Components

EUD Component	CSfC Components List
EUD	CDS Baseline listed Access CDS
EUD--Dedicated Security Component (Optional)	Dedicated Security Component
Hypervisor	CDS Baseline listed Access CDS
WLAN Guest Operating System	*General Purpose Operating Systems*
WLAN Client	*Wireless Local Area Network Client*
Outer VPN Client	*VPN Client*
Inner VPN Client	*VPN Client*
EUD Encryption	*Hardware Full Drive Encryption or Software Full Drive Encryption*

The customer must ensure they are using a current NCDSMO baseline CDS and that it is maintained in accordance with NCDSMO requirements. The security related components of the CDS must be maintained as directed by the NCDSMO such as the Hypervisor and EUD Encryption. There are other components that in addition to NCDSMO requirements that must comply with CSfC Program requirements. These include VPN Client, TLS Client, SRTP Client and WLAN Client. The VPN Client, TLS Client, SRTP Client, WLAN Client and security relevant updates for the Guest Operating Systems are expected and required to be updated as part of the CSfC Components lifecycle and updating them will not affect the status of these devices on the CDS Baseline. For questions or conflicting guidance on this guidance contact the CSfC PMO at csfc@nsa.gov.

7 END USER DEVICE DEPLOYMENTS

Campus WLAN has a single option for Data-in-Transit (DiT) deployments and three separate deployment options for device handling. The DiT deployment option is WLAN-VPN EUDs where the EUD uses a WLAN Client to connect to an authorized WLAN Access Solution and a VPN Client to connect to the Inner VPN. The three options for device handling effect how and what data is stored on the EUD during operations and what data is exposed on the EUD when powered off. The most recommended option for device handling is to deploy an EUD with a *CSfC DAR Solution* ensuring that all data on the EUD is protected

when the EUD is powered off. The other two options revolve around whether the EUD stores classified data or not, Thick EUD and a Thin EUD models.

7.1 End User DiT Options

Campus WLAN has a single deployment option for DiT which is the WLAN-VPN model.

7.2 End User Device Handling Options

The Campus WLAN CP allows three different deployment options pertaining to the use and handling of an EUD while powered off:

- **EUD with DAR:** To implement Data-at-Rest (DAR) protection on an EUD, the DAR solution must be approved by NSA, either as a tailored solution or compliant with NSA's *Data-at-Rest CP.* Specification of such a DAR solution is outside the scope of this CP, but can be found in the DAR CP. The NSA requires implementing organizations to define the circumstances in which an EUD is to be considered outside of the continuous physical control of authorized users (i.e., "lost"). AOs will define "continuous physical control" and that definition should align with the intended mission and threat environment for which the solution will be deployed. Organizations must also define the circumstances in which an EUD that is a part of that organization's solution is to be considered recovered back into the continuous physical control of authorized users (i.e., "found").

- **Thin EUD:** The EUD can be designed to prevent any classified information except for the private keys from being saved to any persistent storage media on the EUD. This allows for the EUD to be treated as Unclassified, or at a high level as determined by the AO, when powered down. Possible techniques for implementing this include, but are not limited to: using Virtual Desktop Infrastructure (VDI) configured to not allow data from the associated Red Network to be saved on the EUD, restricting the user to a non-persistent virtual machine on the EUD, and/or configuring the EUD's operating system to prevent the user from saving data locally. Continuous physical control of the EUD must be maintained at all times.

- **Classified EUD:** The EUD can be used exclusively with physical security measures approved by the AO. EUDs are not subject to special physical handling restrictions beyond those applicable for classified devices since they can rely on the environment they are in for physical protection. If this design option is selected, the EUDs must be treated as classified devices at all times. The EUD in this case must enable the native platform DAR protection to protect the private keys stored on it from disclosure and to increase the difficulty of tampering with the software and configuration. Continuous physical control of the EUD must be maintained at all times.

7.2.1 MULTI-FACTOR AUTHENTICATION OPTIONS

Within this CP a form of multi-factor authentication should be used for a user to access classified data. The current multi-factor authentication options are, 'something you know' and 'something you have.' There are three forms of multi-factor authentication one of which should be used within WLAN CP. The three forms are 'User to EUD', in which the user authenticates to the EUD using an additional factor, 'User to Inner Encryption Component', in which the user authenticates to the Inner Encryption Component user an additional factor, and 'User to VDI' where a user authenticated to a VDI session to access a classified work environment. The authentication token and the EUD must be stored in a physically separate and independently securable storage containers when both devices are securely stored.

7.2.1.1 User to EUD

"User to EUD" is defined as using a second factor of authentication for login to the device in a user's possession. This could be accomplished using a smart card with an identity PKI cert (something you have) and a passphrase (something you know). This could also be accomplished with a passphrase (something you know) and the second factor will be a "something-you-have" factor manifesting as a physically separate token external from the VPN EUD supplying a one-time password for the user to enter. The passphrase should meet the complexity and length requirement specified in WLAN-EU-23. For future versions of the WLAN CP, transferring this one-time password via a short-range RF communication will be examined.

7.2.1.2 User to Inner Encryption Component

"User to Inner Encryption Component" is defined as using a second factor of authentication to the Inner VPN tunnel. This could be accomplished using a smart card with the Inner EUD PKI cert (something you have) and a passphrase (something you know). The second factor will be a "something-you-have" factor manifesting as a physically separate token from the EUD supplying a one-time password for the user to enter. Adding a second factor of authentication to the solution prevents continued access to a network if an EUD is compromised as a result of an attack. If a device has been compromised, it must be assumed that the certificates used to authenticate to the enterprise would be accessible to an adversary to be used on a legitimate device or they could be extracted and used on a different device masquerading as the user. If an adversary has managed to compromise the certificates on an EUD, adding a second authentication factor prevents persistent access to a network.

7.2.1.3 User to Virtual Desktop Infrastructure

This multi-factor use case applies to a Thin EUD and is defined as a second factor of authentication to log into a Virtual Desktop/Environment session to access Red data. This could be accomplished using a smart card with an identity PKI cert (something you have) and a passphrase (something you know). This could also be accomplished with a passphrase (something you know) and the second factor will be a "something-you-have" factor manifesting as a physically separate token external from the VPN EUD supplying a one-time password for the user to enter.

8 CAMPUS WLAN CONFIGURATION AND MANAGEMENT

The Campus WLAN CP includes design details for the provisioning and management of Solution Components. The CSfC solution owner must identify authorized Security Administrators (SAs) to perform configuration and management tasks. The following sections describe the design in detail and Section 13 articulates specific configuration requirements that must be met to comply with the WLAN CP.

8.1 SOLUTION INFRASTRUCTURE COMPONENT PROVISIONING

Provisioning is an out-of-band process performed in a physically secured area (e.g., Red Network), through which WLAN solution infrastructure components are configured and initialized before their first use. During the provisioning process, the SA configures the WLAN Access System, Gray Management Services, Inner Encryption Components, and Red Management Services in accordance with the requirements of this CP.

During provisioning, the WLAN Access System and Inner Encryption Components generate a public/private key pair and output the public key in a Certificate Signing Request (CSR). The SA delivers the WLAN Access System's CSR to the Outer CA and the Inner Encryption Components' CSR to the Inner CA. The appropriate CA processes the CSR for each encryption component and returns a signed X.509 certificate. The SA then installs the unique signed certificate and the certificate chain, which consists of the signing CA's certificate and the Trust Anchor certificate (e.g., Root CA certificate). The SA may also install an initial Certificate Revocation List (CRL).

8.2 EUD PROVISIONING

Initial provisioning of campus EUD will be performed using enrollment capabilities hosted in the Red Network and leveraging the Outer and Inner CAs. To support different device types, it may be necessary to support both wireless and wired connection capabilities to the EUD being provisioned. Since keying and secure applications needed to connect to the operational WLAN Access System have not yet been established, wireless provisioning connectivity must be performed on a separate WLAN Access System in a shielded enclosure. The provisioning process includes assigning identifiers to the devices, installing required applications, configuring the device's policy and settings (especially WPA3 and IPsec settings), and loading certificates and keying material. Prior to provisioning devices, configuration profiles are created and required device applications are obtained.

Initial provisioning (for all device types) should include the following, in no specific order:

- **Device registration**. Collect identifying information from the EUD, assign Government device identities for the Gray and Red domains, and update data stores (directory, inventory, and/or authorization) to include new EUD.

- **Settings configuration**. Load configuration (within the limitations of what is supported by each device type) that implement policies on allowed and disallowed services (such as Bluetooth) and user authentication parameters (such as password length and when to lock the device). Supply other settings such as network parameters.

- **Application installation**. Load required applications, including the VPN client and enterprise client applications (there is no current support for an online application store, so all applications should be loaded during initial provisioning). If possible, unneeded applications should be removed from the device.

- **Certificate request and issuance**. Using the assigned Government device identifiers, connect to the Gray Network, request certificates from the Outer CA, and load received material into the EUD. Disconnect the device from the Gray Network, connect to the Red Network, request certificates from the Inner CA, and load received material into the EUD. Note: It is possible for both CAs to reside on the Red Network.

Depending on the capabilities of the EUD, the device either connects and interacts with the CAs in order to be issued certificates, or the certificates are generated and loaded onto a device storage medium from a provisioning workstation for transfer to the EUD. There will also be differences based on whether the EUD generates and provides a private key for the certificate or is issued one from the CA (more secure handling and transfer is required for the latter case). Finally, some devices may require that certificate provisioning be performed using a wireless connection. In the event that a device can only support wireless certificate provisioning, the certificate provisioning must be performed in a shielded enclosure deemed appropriate by the AO.

Once the EUD is properly configured and certificates/keying material is in place, it is ready to be issued to a user with the final steps of establishing user login and associating the user with the device in the registration data. Once the device is connected to the Red Network, the device is classified.

8.3 Management of Campus WLAN Solution Components

Management of all Campus WLAN solution components is always encrypted to protect confidentiality and integrity, except in the case where components are locally managed through a direct physical connection (e.g., serial cable from the Gray Administration Workstation to the WLAN Controller). Management traffic must be encrypted with SSHv2, TLS, or IPsec.

The requirements for configuring the EUDs in Section 12.2 can be accomplished through a variety of mechanisms. First, the EUDs can be configured using Mobile Device Management (MDM) selected from the CSfC Components List. Alternatively, the EUD can be configured using a provisioning tool which enforces configuration policies during initial setup, and must be brought back to a Security Administrator to be updated. Customers can also configure the EUD using an existing Enterprise Policy enforcement mechanism. Finally, customers can choose to use a hybrid approach with more than one of the above options.

8.4 EUDs for Different Classification Domains

As specified in this CP, an EUD is only authorized to communicate with Red Networks operating at the same classification level. Implementation of the Multiple Security Levels design does not change the requirement for EUDs to be dedicated to a single classification level. However, the CP does not preclude the possibility that an approved CDS can be used within an infrastructure to provide cross domain transfer of data between EUDs operating at differing classification levels. It also does not preclude the

use of an EUD as an access CDS for multiple enclaves operating at different classification levels if approved through the appropriate CDS approval process.

The requirements for a CDS capable of providing separation between enclaves of two or more classification levels are outside the scope of this CP. If developing a WLAN solution with a CDS capability, the solution owner must register against this CP and use the appropriate CDS approval processes.

9 SUPPORTING DOCUMENTS

9.1 CONTINUOUS MONITORING

The Campus WLAN CP allows customers to use EUDs from physical environments residing within a government secure facility. Today's technology provides increased accessibility to various networks, which creates a need to continuously monitor network traffic and system log data within the solution infrastructure. This monitoring allows customers to detect, react to, and report any attacks that occur on or against their solution. This continuous monitoring also enables the detection of any configuration errors in solution infrastructure components.

Continuous Monitoring requirements have been relocated to the *CSfC Continuous Monitoring Annex*.

Figure 18 shows the monitoring points in the *CSfC Continuous Monitoring Annex* for Campus WLAN CP.

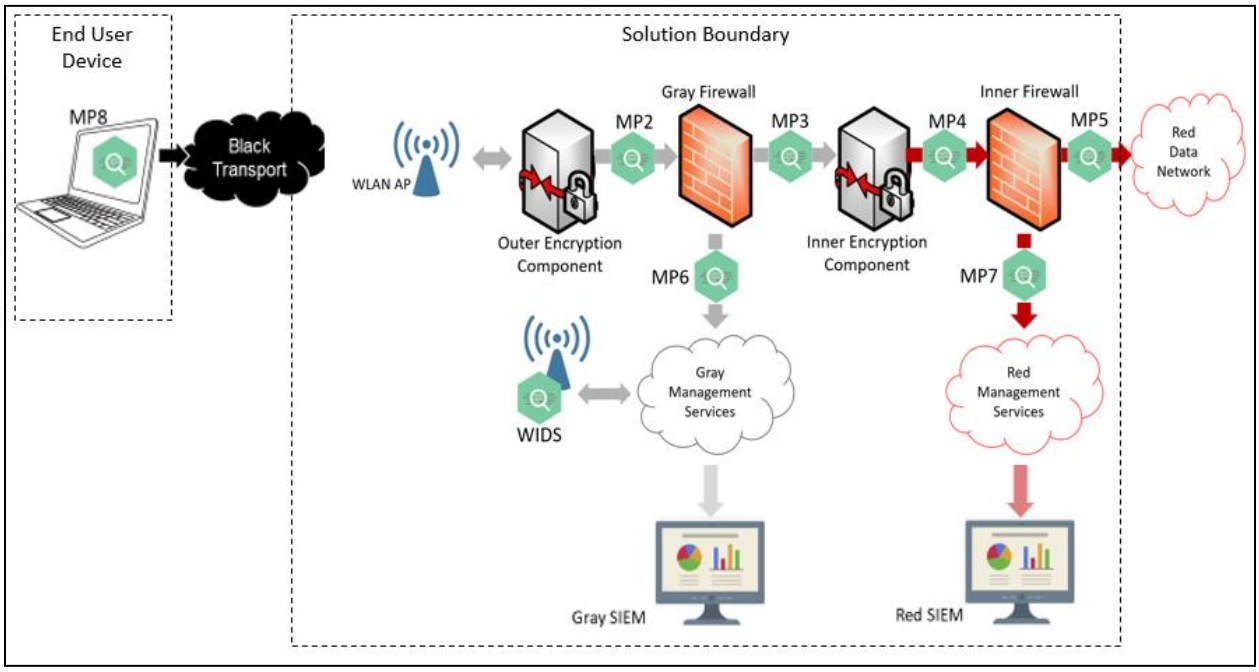

Figure 18. Campus WLAN Continuous Monitoring Points

9.2 KEY MANAGEMENT

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

The *CSfC Key Management Requirements Annex* provides requirements and guidance for implementing the secure use of public key certificates for component authentication to establish the Outer and Inner encryption tunnels of CSfC solutions. At least two Certification Authorities (CAs) are used to issue certificates. One CA (known as the Outer CA) issues certificates to Outer Encryption Components and the other CA (known as the Inner CA) is used to issue certificates to Inner Encryption Components. 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 to validate the Outer Tunnel and Inner Tunnel authentication certificates, respectively.

9.3 ENTERPRISE GRAY

The *CSfC Enterprise Gray (EG) Implementation Requirements Annex* is a supplemental document that enables the following capabilities within a CSfC solution:

- Enhanced scalability
- Centralized management
- Enhanced site survivability
- Ability to implement multiple CPs simultaneously

The Gray Encryption Components are allowed to share routes between each other to streamline the management of shared Gray Data and Gray Management planes in larger CSfC solutions. This dynamic sharing allows for better scaling for these networks and better resilience against network disruptions.

EG allows for interconnected CSfC sites or solutions to share a single Gray Management plane referred to as the Enterprise Gray Network and shared Gray Data plane. This shared Gray Data plane allows sites to access resources hosted at different sites such as Gray Data services and Inner Encryption Components only deployed on specific sites.

Greater interconnection and reliance between sites using the Enterprise Gray Network allows some sites to maintain functionality even if connections to other sites are lost or otherwise unusable. EG covers the utilities and services needed by a site to maintain a site solution while connection is restored.

EG allows for a single CSfC solution to incorporate multiple CPs into the same physical hardware. For example, an Outer Encryption Component being used as both the WLAN Access System as described in the *CSfC Campus WLAN CP* and the Outer VPN Gateway as allowed by the *CSfC Mobile Access CP*.

9.4 DATA AT REST

A Campus WLAN CP EUD using Data-at-Rest (DAR) requires the DAR solution be approved by the NSA. The documentation for tailoring a NSA approved DAR solution can be found in the *CSfC Data-at-Rest Capability Package*.

The *CSfC Data-at-Rest Capability Package* is a high-level reference design document that enables customers to select products from the CSfC Components List and then to properly configure those products to achieve a level of assurance sufficient for protecting classified data while at rest.

9.5 WIRELESS INTRUSION DETECTION SYSTEM (WIDS)

The Wireless Intrusion Detection System (WIDS) Requirements have been relocated to a separate *CSfC Wireless Intrusion Detection System (WIDS) Annex*.

The *CSfC Wireless Intrusion Detection System (WIDS) Annex* provides requirements and guidance for monitoring and protection of wireless 802.11 End User Devices (EUD) (e.g., tablets, smartphones, and laptop computers) accessing secure enterprise services over a campus wireless network or authorized wireless deployment. The WIDS Annex provides reference architecture and corresponding configuration information that allows customers to select COTS products from the CSfC Components List to develop a WIDS/WIPS solution and then properly configure those products to achieve a level of assurance sufficient for a solution used to protect classified Data-in-Transit (DIT).

10 19REQUIREMENTS OVERVIEW

The following five sections (Section 11 through Section 15, and the *CSfC Key Management Requirements Annex*) specify requirements for implementations of WLAN solutions compliant with this CP. However, not all requirements in the following sections will apply to each compliant solution.

10.1 THRESHOLD AND OBJECTIVE REQUIREMENTS

In some cases, multiple versions of a requirement may exist in this CP. Such alternative versions of a requirement are designated as being either a Threshold requirement or an Objective requirement:

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

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

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

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

10.2 REQUIREMENTS DESIGNATORS

Each requirement defined in this CP has a unique identifier consisting of the prefix "WLAN," a digraph that groups related requirements together (e.g., "KM"), and a sequence number (e.g., 11).

Table 6 lists the digraphs used to group together related requirements and identifies the sections in which those requirement groups can be found.

Table 6. Requirement Digraph

Digraph	Description	Section	Table
PS	Product Selection Requirements	Section 11	Table 7
SR	Overall Solution Requirements	Section 12.1	Table 8
EU	End User Device Requirements	Section 12.2	Table 10
VZ	Enhanced Virtualization Requirements	Section 12.3	Table 11
WC	WLAN Client Configuration Requirements	Section 12.4	Table 12
WO	Dedicate Outer WLAN Requirements	Section 12.4	Table 13
WL	Wireless Link Requirements	Section 12.4	Table 14
CR	VPN Components Configuration Requirements	Section 12.5	Table 19
WS	WLAN Access System Configuration Requirements	Section 12.6	Table 20
IA	Wireless Infrastructure Authentication Requirements	Section 12.6	Table 21
AA	Wireless Authentication and Authorization Requirements	Section 12.6	Table 22
WA	Wireless Authentication Server Requirements	Section 12.6	Table 23
PF	Solution Components Port Filtering Requirements	Section 12.7	Table 24
PR	End User Device Provisioning Requirements	Section 12.8	Table 25
WIDS	WIDS/WIPS Requirements	Section 12.9	Table 26
DM	Device Management Requirements	Section 12.11	Table 27
CM	Continuous Monitoring Requirements	Section 12.12	Table 28
KM	Key Management Requirements	Section 12.14	Table 29
FW	Gray Firewall Requirements	Section 12.15	Table 30
MFA	Multi-Factor Authentication Requirements	Section 12.16	Table 31
GD	Use and Handling of Solutions Requirements	Section 13.1	Table 32
RP	Incident Reporting Requirements	Section 13.2	Table 33
GD	Role-Based Personnel Requirements	Section 14	Table 34
TR	Test Requirement	Section 15.1	Table 35
KM	Key Management Requirements (See *Key Management Requirements Annex*)		
WIDS	Wireless Intrusion Detection System Requirements (See *WIDS/WIPS Requirements Annex)*		
CM	Continuous Monitoring Requirements (See *Continuous Monitoring Requirements Annex)*		

11 REQUIREMENTS FOR SELECTING COMPONENTS

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

Table 7. Production Selection Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-PS-1	The product used for the VPN Gateway(s) must be chosen from the list of IPsec VPN Gateways on the CSfC Components List.	T=O	
WLAN-PS-2	The products used for any WLAN Access System must be chosen from the list of WLAN Access Systems on the CSfC Components List.	T=O	
WLAN-PS-3	The products used for any WLAN Client must be chosen from the list of Mobile Platforms on the CSfC Components List or an Operating System which is listed on the CSfC Components List for WLAN Clients.	T=O	WLAN-PS-21
WLAN-PS-4	If using a MDF EUD, the EUDs must be chosen from the list of Mobile Platforms on the CSfC Components List.	T=O	**Composed EUD:** WLAN-PS-17 and WLAN-PS-18; or **Virtual EUD:** WLAN-PS-17 and WLAN-PS-19; or **CDS EUD:** WLAN-PS-22 and WLAN-PS-23
WLAN-PS-5	The products used for the Inner VPN Client must be chosen from the list of IPsec VPN Clients on the CSfC Components List.	T=O	
WLAN-PS-6	Requirement has been relocated to the *CSfC Key Management Requirements Annex*.		
WLAN-PS-7	Withdrawn		
WLAN-PS-8	Products used for the Gray Firewall and Inner Firewall must be chosen from the list of Stateful Traffic Filtering Firewalls (TFFW) on the CSfC Components List.	T=O	
WLAN-PS-9	Products used for the Authentication Server must be chosen from the list of Authentication Servers on the CSfC Components List.	T=O	
WLAN-PS-10	The Inner VPN Gateway and the WLAN Access System must either: • come from different manufacturers, where neither manufacturer is a subsidiary of the other; or, • be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence. Differences between Service Packs (SP) and version numbers for a particular vendor's OS do not provide adequate diversity.	T=O	
WLAN-PS-11	The WLAN Access System, Gray Firewall, Inner VPN Gateway and Inner Firewall must use physically separate	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
	components, such that no component is used for more than one function.		
WLAN-PS-12	Requirement has been relocated to the *CSfC Key Management Requirements Annex*.		
WLAN-PS-13	The EUD's VPN Client and WLAN Client must either: • come from different manufacturers, where neither manufacturer is a subsidiary of the other; or, • be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence.	T=O	
WLAN-PS-14	The cryptographic libraries used by the WLAN Access System and the Inner VPN Gateway must either: • come from different manufacturers, where neither manufacturer is a subsidiary of the other; or, • be different libraries from the same manufacturer, where NSA has determined that the libraries meet the CSfC criteria for implementation independence.	T=O	
WLAN-PS-15	Each component that is selected from the CSfC Components List must go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO-approved Product Supply Chain Threat Assessment process (see CNSSD 505 SCRM for additional guidance).	T=O	
WLAN-PS-16	Products selected from the CSfC Components List must be configured to use the NIAP-certified evaluated configuration.	T=O	
WLAN-PS-17	If using a composed EUD, the EUDs Hardware Platform must be chosen from the list of Hardware Platforms on the CSfC Components List.	T=O	**MDF EUD:** WLAN-PS-4; or **CDS EUD:** WLAN-PS-22
WLAN-PS-18	If using a composed EUD, the EUD's Operating System must be chosen from the list of Operating Systems on the CSfC Components List.	T=O	**MDF EUD:** WLAN-PS-4; or **Virtual EUD:** WLAN-PS-19; or **CDS EUD:** WLAN-PS-23
WLAN-PS-19	If using a virtualized EUD, the EUD's Hypervisor must be chosen from the list of Client Hypervisors on the CSfC Components List.	O	**MDF EUD:** WLAN-PS-4; or **Composed EUD:** WLAN-PS-18; or **CDS EUD:** WLAN-PS-22

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-PS-20	The EUD must have a Dedicated Security Component chosen from the list of Dedicated Security Components on the CSfC Components List.	O	Optional
WLAN-PS-21	If the solution uses a Dedicated Outer Wi-Fi as part of an EUD, it must be chosen from the list of WLAN Access Systems or WLAN Clients on the CSfC Components List.	T=O	WLAN-PS-3
WLAN-PS-22	If using an Access CDS EUD, the EUDs Hardware Platform must be validated as part of an Access CDS listed on the CDS Baseline.	T=O	**MDF EUD:** WLAN-PS-4; or **Composed/ Virtual EUD:** WLAN-PS-17
WLAN-PS-23	If using an Access CDS EUD, the EUD's Hypervisor used must be validated as part of an Access CDS listed on the CDS Baseline.	T=O	**MDF EUD:** WLAN-PS-4; or **Composed EUD:** WLAN-PS-18; or **Virtual EUD:** WLAN-PS-19
WLAN-PS-24	The products used for the SWFDE layer must be chosen from the list of SWFDEs on the CSfC Components List.	T=O	WLAN-PS-25
WLAN-PS-25	The products used for the HWFDE layer must be chosen from the list of HWFDEs on the CSfC Components List.	T=O	WLAN-PS-24

12 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 WLAN solution.

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

This section contains requirements applicable to the Campus WLAN solution components. In this section, a series of overarching architectural requirements are given for maximizing the independence between the components within the solution. This independence will increase the level of effort required to compromise this solution.

The products that are approved for use in this solution will be listed on the CSfC Components List on the CSfC website (https://www.nsa.gov/resources/commercial-solutions-for-classified-program). No single commercial product must be used to protect classified information. The only approved methods for using COTS products to protect classified information in transit on a Campus WLAN follow the requirements outlined in this CP.

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

12.1 Overall Solution Requirements

Table 8. Overall Solution Requirements (SR)

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-SR-1	Default accounts, passwords, community strings and other default access control mechanisms for all Campus WLAN components must be changed or removed.	T=O	
WLAN-SR-2	The time of day on Inner Encryption Endpoints, Inner Firewall, and Red Management Services must be synchronized to a time source located in the Red Network.	T=O	
WLAN-SR-3	The time of day on the WLAN Authentication Server, the WLAN Controller and Gray Network components must be synchronized to a time source located in the Gray Management network.	T=O	
WLAN-SR-4	All components must be properly configured in accordance with local policy and applicable U.S. Government guidance. In the event of conflict between the requirements in this CP and local policy, this CP takes precedence.	T=O	
WLAN-SR-5	Solution components must receive virus signature updates as required by the local agency policy and the AO.	T=O	
WLAN-SR-6	The only approved physical paths leaving the Red Network must be through a WLAN solution in accordance with this CP or via an AO-approved solution for protecting data in transit.	T=O	
WLAN-SR-7	All Infrastructure components must implement a password/authentication with entropy of at least 95 bits.	T	WLAN-SR-8
WLAN-SR-8	All infrastructure components must use an authentication service on their respective network/domain in order to access the infrastructure component of the respective network/domain.	O	WLAN-SR-7
WLAN-SR-9	When multiple Inner Encryption Components are placed between the Gray Firewall and Inner Firewall, they must be placed in parallel.	T=O	
WLAN-SR-10	Inner Encryption Components must not perform switching or routing for other Encryption Components.	T=O	
WLAN-SR-11	Infrastructure components must only be configured over an interface dedicated for management.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-SR-12	DNS lookup services on network devices must be disabled.	O	Optional
WLAN-SR-13	DNS server addresses on infrastructure devices must be specified or DNS services must be disabled.	T=O	
WLAN-SR-14	Automatic remote boot-time configuration services must be disabled (e.g., automatic configuration via Trivial File Transfer Protocol on boot).	T=O	
WLAN-SR-15	All solution components (Firewalls, WLAN Access Systems, VPN Gateways, Authentication Servers, and EUDs) must use software and firmware signing algorithms in Table 9	O	Optional

Table 9. CNSA 2.0 Algorithms for Software and Firmware Signing

Algorithm	Function	Specification	Parameters
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels. SHA-256/192 recommended.
Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels
ML-DSA (aka CRYSTALS-Dilithium)	Asymmetric algorithm for digital signatures	FIPS 204	Category 5 parameter, ML-DSA87

12.2 End User Device Requirements

Table 10. End User Device (EU) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-EU-1	The EUD must restrict configuration (Service Set Identifier (SSID) and authentication mechanism) of authorized WLANs to authorized administrators.	T=O	
WLAN-EU-2	The EUD must be configured with separate authentication and privileges for administrator and user roles.	T=O	
WLAN-EU-3	The EUD must be loaded with only AO-approved software.	T=O	
WLAN-EU-4	The EUD must restrict installation and removal of software to authorized administrators.	T=O	
WLAN-EU-5	The EUD must require a user to log in prior to granting access to any EUD functionality.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-EU-6	The EUD must be configured to limit the number of incorrect logins per an AO-approved period of time either by erasing the configuration and data stored on the device or by prohibiting login attempts for a AO-approved period of time.	T=O	
WLAN-EU-7	Rekeying of an EUD's certificates and associated private keys must be done through re-provisioning prior to expiration of keys.	T	WLAN-EU-8
WLAN-EU-8	Rekeying of an EUD's certificates and associated private keys must be done over the WLAN solution network prior to expiration of keys.	O	WLAN-EU-7
WLAN-EU-9	An EUD must be deauthorized from the network and submitted for forensic analysis if suspected of being compromised.	T=O	
WLAN-EU-10	An EUD should be destroyed only if it has been determined to be compromised through forensic analysis.	T=O	
WLAN-EU-11	Users of EUDs must successfully authenticate themselves to the services they access on their respective Red Network using an AO-approved method.	T=O	
WLAN-EU-12	Red Network services must not transmit any classified data to EUDs until user authentication succeeds.	T=O	
WLAN-EU-13	The EUD must lock the screen and require user re-authentication after an AO-approved period of inactivity.	T=O	
WLAN-EU-14	All EUD users must sign an organization-defined user agreement before being authorized to use an EUD.	T=O	
WLAN-EU-15	All EUD users must receive an organization-developed training course for operating an EUD prior to use.	T=O	
WLAN-EU-16	At a minimum, the organization-defined user agreement must include each of the following: Consent to monitoring Operations Security (OPSEC) guidance • Required physical protections to employ when operating and storing the EUD • Restrictions for when, where, and under what conditions the EUD may be used • Responsibility for reporting security incidents • Verification of IA Training • Verification of appropriate clearance • Justification for Access • Requester information and organization • Account Expiration Date • User Responsibilities	T=O	
WLAN-EU-17	EUDs must be dedicated for use solely in the CSfC WLAN solution, and not used to access any resources on networks other than the Red Network it communicates with through the two layers of encryption or other AO approved direct wired connection to the Red Network.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-EU-18	The EUD must disable all transmitted Global Positioning System (GPS) and location services except Enhanced 9-1-1 (E911) or those authorized by the AO.	T=O	
WLAN-EU-19	If the EUD has cellular capability then cellular service must be disabled.	T=O	
WLAN-EU-20	The EUD must have all network and wireless interfaces disabled except for 802.11 while in operation.	T=O	WLAN-EU-49
WLAN-EU-21	Withdrawn		
WLAN-EU-22	All EUDs must have their certificates revoked and resident image removed prior to disposal.	T=O	
WLAN-EU-23	Passwords for user to device (EUD selected from Mobile Platform section of CSfC Components List) authentication must have an entropy of at least 95 bits.	T=O	
WLAN-EU-24	If an NSA-approved DAR Solution is not implemented on EUDs, the MDF EUD must have the native platform DAR protection enabled.	T=O	WLAN-EU-48
WLAN-EU-25	Withdrawn		
WLAN-EU-26	Withdrawn		
WLAN-EU-27	The EUD maximum password lifetime must be less than 181 days.	T=O	
WLAN-EU-28	The EUD screen must lock after an AO approved period of inactivity.	T=O	
WLAN-EU-29	The EUD must perform a wipe of all protected data after 10 or more authentication failures.	T=O	WLAN-EU-47
WLAN-EU-30	During provisioning, all unnecessary keys must be destroyed from the EUD secure key storage.	T=O	
WLAN-EU-31	During provisioning, all unnecessary X.509 certificates must be removed from the EUD Trust Anchor Database.	T=O	
WLAN-EU-32	All display notifications must be disabled while in a locked state.	T=O	
WLAN-EU-33	USB mass storage mode must be disabled on the EUDs.	T=O	
WLAN-EU-34	USB data transfer must be disabled on the EUDs.	T=O	
WLAN-EU-35	Prior to installing new applications, the application digital signature must be verified.	T=O	
WLAN-EU-36	The EUD must be configured to only permit connections to allowlisted SSIDs.	T=O	
WLAN-EU-37	The EUD must be configured to only permit connection to SSIDs using certificates signed by the Outer CA.	T=O	
WLAN-EU-38	The EUD must only display allowlisted SSIDs to the user.	T=O	
WLAN-EU-39	The end user must only be able to access the applications that are necessary for the EUDs intended purpose.	T=O	
WLAN-EU-40	The management and control of the EUD connection to the WLAN System must be isolated from other EUD functions.	O	Optional
WLAN-EU-41	EUDs must prohibit the use of removable media through configuration, policy, or physical modification.	T=O	
WLAN-EU-42	Composed EUDs must implement the BIOS security guidelines specified in NIST SP 800-147.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-EU-43	Composed EUD's BIOS/Unified Extensible Firmware Interface (UEFI) must be configured to require a password before continuing the boot process.	O	Optional
WLAN-EU-44	Composed EUDs must have the BIOS/UEFI password enabled.	T=O	
WLAN-EU-45	If Composed EUD's PXE Boot feature must be disabled in the BIOS.	T=O	
WLAN-EU-46	Composed EUD's boot from removable media feature must be disabled in the BIOS.	T=O	
WLAN-EU-47	Security policy must administratively lock the account of the EUD user after three consecutive authentication failures. (Administrator intervention is required to unlock).	T=O	WLAN-EU-29
WLAN-EU-48	If an NSA-approved DAR Solution is not implemented on EUDs, the Composed EUD must have a layer of Software Full Disk Encryption or Hardware Full Disk Encryption Enabled.	T=O	WLAN-EU-24
WLAN-EU-49	The EUD must have all wireless interfaces disabled except for 802.11 while in operation.	T=O	WLAN-EU-20

12.3 Enhanced Virtualization Requirements

The following requirements are not considered threshold but may be implemented if the AO decides that virtualization is necessary for the security of their WLAN solution.

Table 11. Enhanced Virtualization Requirements

Req #	Requirement Description	Threshold/ Objective	Alternative
WLAN-VZ-1	The EUD and virtualization architecture must be able to securely isolate hardware components so that only authorized domains can access required components.	O	Optional
WLAN-VZ-2	The virtualization software must have the ability to create virtual TPMs (vTPMs).	O	Optional
WLAN-VZ-3	Each VM in this solution must perform a boot integrity check via a vTPM.	O	Optional
WLAN-VZ-4	The Wi-Fi drivers and hardware on the underlying host EUD must only be accessible to the WLAN domain. The other domains (Inner VPN, and User VPN) must not have access to the Wi-Fi drivers and hardware.	O	Optional
WLAN-VZ-5	The end user may only have access to the User domain and must not have access to any domains.	O	Optional
WLAN-VZ-6	The hypervisor must allow the configuration of virtual network infrastructure to other domains within the EUD to support the secure connections between each domain.	O	Optional
WLAN-VZ-7	The Inner VPN and the WLAN connections must all be implemented on separate IP stacks by using separate domains for each connection on the EUD.	O	Optional
WLAN-VZ-8	Rekeying of each domains' certificates and associated private keys must be done through re-provisioning prior to the expiration of keys.	O	WLAN-VZ-9

Req #	Requirement Description	Threshold/ Objective	Alternative
WLAN-VZ-9	Rekeying of a domain's certificates and associated private keys must be done over the WLAN solution network prior to expiration of keys.	O	WLAN-VZ-8
WLAN-VZ-10	All domains must have their certificates revoked and resident image removed prior to disposal.	O	Optional
WLAN-VZ-11	If an NSA-approved DAR Solution is not implemented on the user domain, the native platform DAR protection must be enabled.	O	Optional
WLAN-VZ-12	The WLAN domain must use a unique X.509 v3 device certificate, signed by the Outer CA, for mutual authentication with WLAN Access System.	O	Optional
WLAN-VZ-13	The Inner VPN domain must use a unique X.509 v3 device certificate, signed by the Inner CA, for mutual authentication with Inner VPN Gateways.	O	Optional
WLAN-VZ-14	The User domain password lifetime must be less than 181 days.	O	Optional
WLAN-VZ-15	The end user must not be able to change security relevant settings on any of the domains.	O	WLAN-VZ-17
WLAN-VZ-16	User domain must display a consent prompt that requires user to accept prior to using the device.	O	Optional
WLAN-VZ-17	The User domain must use Mandatory Access Control policy to prevent end users from changing security relevant settings.	O	WLAN-VZ-15
WLAN-VZ-18	Passwords for User domain authentication must be a minimum of 14 alpha-numeric case-sensitive characters.	O	Optional
WLAN-VZ-19	All domains must generate logs and send to a central SIEM in the enterprise network of the same classification label.	O	Optional
WLAN-VZ-20	The hypervisor must be configured with an administrative password.	O	Optional
WLAN-VZ-21	The End User must not be able to change any administrative settings in the hypervisor.	O	Optional
WLAN-VZ-22	The End User must not be able to create nor remove virtual machines on the EUD.	O	Optional
WLAN-VZ-23	The hypervisor must not allow any of the domains to access any cellular technologies that are integrated into the EUD.	O	Optional
WLAN-VZ-24	The user domain virtual/physical disk must be encrypted. This can be accomplished either by the hypervisor or by the OS running in the user domain.	O	Optional

12.4 WLAN Client Configuration Requirements

Table 12. WLAN Client (WC) Configuration Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-WC-1	The WLAN Client tunnel must be established at EUD start-up.	O	Optional

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-WC-2	The WLAN Client must authenticate the identity of the WLAN Authentication Server by verifying that the WLAN Authentication Server's certificate chain is rooted by the WLAN Trusted Root Certificate Authority.	T=O	
WLAN-WC-3	The WLAN Client must be configured to authenticate only specific servers through setting the client to accept only a WLAN Authentication Server certificate that contains a particular Distinguished Name or Subject Alternate Name (i.e., the client looks for the specified server name in the certificate during verification).	T=O	
WLAN-WC-4	A unique device certificate must be loaded into the WLAN Client along with the corresponding CA (signing) certificate.	T=O	
WLAN-WC-5	The device certificate must be used for WLAN Client authentication during EAP-TLS.	T=O	
WLAN-WC-6	The WLAN Client must provide the user with advance warning that the WLAN Client's device certificate is due to expire.	O	Optional
WLAN-WC-7	The WLAN Client must negotiate new session keys with the WLAN Access System at least once per hour.	T=O	
WLAN-WC-8	The WLAN Client must be prevented from using ad hoc mode (client-to-client connections).	T=O	
WLAN-WC-9	The WLAN Client must be prevented from using network bridging.	T=O	
WLAN-WC-10	The WLAN Client must only associate with authorized Access Points based on attributes such as SSID or allowlists and enforce based on the certificate presented by the Authentication Server during mutual authentication.	T=O	
WLAN-WC-11	The WLAN Client must verify that the WLAN Authentication Server X.509 v3 certificate contains the TLS Web Server Authentication Object Identifier (OID) (id-kp-serverAuth 1.3.6.1.5.5.7.3.1) in the Extended Key Usage extension.	T=O	
WLAN-WC-12	The device certificate for the WLAN Client must contain an extendedKeyUsage field indicating support for Client Authentication (OID 1.3.6.1.5.5.7.3.2).	T=O	
WLAN-WC-13	The WLAN Client must be managed from the Gray Management Network.	T=O	

Table 13. Dedicated Outer WLAN (WO) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-WO-1	If a Dedicated Outer WLAN is used it must be dedicated to a single security level and only provide the Outer layer of Wi-Fi to Computing Devices connecting to a Red Network of the same security level.	T=O	
WLAN-WO-2	A Computing Device must only connect to a Dedicated Outer WLAN authorized as part of the WLAN CP solution.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-WO-3	The Dedicated Outer WLAN must comply with all requirements in Table 17.	T	WLAN-WO-6
WLAN-WO-4	If a Dedicated Outer WLAN is used, all EUDs must connect to Dedicated Outer WLAN devices with a wired connection.	T=O	
WLAN-WO-5	If a Dedicated Outer WLAN is used Wi-Fi must be disabled on the EUD.	T=O	
WLAN-WO-6	The Dedicated Outer WLAN must comply with all requirements in Table 18.	O	WLAN-WO-3

Table 14. Wireless Link (WL) Requirements

Req #	Requirement Description`	Threshold / Objective	Alternative
WLAN-WL-1	The WLAN Client and the WLAN Access System must use protocols and algorithms from Table 17.	T	WLAN-WL-9
WLAN-WL-2	The WLAN Client and the WLAN Access System must operate in WPA3-Enterprise 192-bit mode only.	T=O	
WLAN-WL-3	The WLAN Client and the WLAN Access System must use integrity algorithms that implements NIST AES Key Wrap with Hash-based Message Authentication Code (HMAC)-SHA-384-128 as specified in Section 11 of IEEE 802.11-2020.	T=O	
WLAN-WL-4	If WPA3 terminates on APs then all data between the Access Point(s) and Wireless controller must be encrypted using IPsec, SSHv2, TLS, DTLS or TLS/HTTPS.	T=O	
WLAN-WL-5	The WLAN Client and the WLAN Access System must operate with 802.11w (management frame protection) enabled.	T=O	
WLAN-WL-6	The WLAN Client and the WLAN Access System must disable WPA3 transition mode.	T=O	
WLAN-WL-7	The WLAN Client and the WLAN Access System must operate with Operating Channel Validation (OCV) enabled.	O	
WLAN-WL-8	The WLAN Client and the WLAN Access System must operate with Beacon Protection enabled.	O	
WLAN-WL-9	The WLAN Client and the WLAN Access System must use protocols and algorithms from Table 18.	O	WLAN-WL-1

Table 15. Approved CNSA 1.0 Algorithms for IPsec

Security Service	Algorithm Suite	Specifications
Confidentiality (Encryption)	Advanced Encryption Standard (AES)-256	FIPS PUB 197 IETF RFC 7296 IETF RFC 9206

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

Table 16. Approved CNSA 2.0 Algorithms for IPsec

Security Service	Algorithm Suite	Specifications
Confidentiality (Encryption)	AES-256-GCM	FIPS PUB 197
Authentication (Digital Signature)	ML-DSA-87	FIPS 204
Key Establishment	ML-KEM-1024	FIPS 203
Integrity (Hashing)	SHA-384 or SHA-512	FIPS PUB 180-4 IETF RFC 6234

Table 17. Approved CNSA 1.0 Algorithms for WPA3 Encryption and EAP-TLS

Security Service	Algorithm Suite	Specifications
Confidentiality (Encryption)	AES-256-CCMP	FIPS PUB 197
Authentication (Digital Signature)	RSA 3072 or, ECDSA over the curve P-384 with SHA-384 or SHA-512	FIPS PUB 186-4 IETF RFC 6239 IETF RFC 6380 IETF RFC 6460
Key Exchange/ Establishment	ECDH over the curve P-384 (DH Group 20) or, DH 3072	NIST SP 800-56A IETF RFC 7296
Integrity (Hashing)	SHA-384 or, SHA-512	FIPS PUB 180-4 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460

Table 18. Approved CNSA 2.0 Algorithms for WPA3 Encryption and EAP-TLS

Security Service	Algorithm Suite	Specifications
Confidentiality (Encryption)	AES-256-GCM	FIPS PUB 197
Authentication (Digital Signature)	ML-DSA-87	FIPS 204
Key Establishment	ML-KEM-1024	FIPS 203
Integrity (Hashing)	SHA-384 or SHA-512	FIPS PUB 180-4 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460

12.5 VPN COMPONENTS AND VPN CLIENT CONFIGURATION REQUIREMENTS

Table 19. VPN Components Configuration Requirements (CR)

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-CR-1	The VPN Components must use protocols and algorithms for creating all VPN tunnels selected from an Algorithm Suite in Table 15.	T	WLAN-CR-17, WLAN-CR-18, and WLAN-CR-19
WLAN-CR-2	Default, self-signed, or proprietary device certificates, which are frequently preinstalled by the vendor, for any WLAN Access System and VPN Gateway components must not be used for establishing Security Associations (SAs).	T	WLAN-CR-3
WLAN-CR-3	Default, self-signed, or proprietary device certificates, which are frequently preinstalled by the vendor, for any WLAN Access System and VPN Gateway components, must be removed.	O	WLAN-CR-2
WLAN-CR-4	All IPsec connections must use IETF standards compliant with IKE implementations (RFC 7296).	T=O	
WLAN-CR-5	All Access Systems and VPN Gateway components must use Cipher Block Chaining for IKE encryption.	T	WLAN-CR-16
WLAN-CR-6	All Access Systems and VPN Gateway components must use Cipher Block Chaining for ESP encryption with a Hash-based Message Authentication Code for integrity.	T	WLAN-CR-7
WLAN-CR-7	All Access Systems and VPN Gateway components must use Galois Counter Mode (GCM) for ESP encryption.	O	WLAN-CR-6
WLAN-CR-8	All Access Systems and VPN Gateway components must set the IKE SA lifetime to at most 24 hours.	T=O	
WLAN-CR-9	All Access Systems and VPN Gateway components must set the ESP SA lifetime to at most 8 hours.	T=O	
WLAN-CR-10	Each VPN Client must use a unique private key for authenticating to the VPN Gateway.	T=O	
WLAN-CR-11	The VPN Client must provide the user with advance warning that the VPN client certificate is due to expire.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-CR-12	The VPN Client must be configured to prohibit split tunneling.	T=O	
WLAN-CR-13	A unique device certificate must be loaded into the VPN Client along with the corresponding CA (signing) certificate.	T=O	
WLAN-CR-14	The device certificate must be used for VPN Client authentication during IPsec.	T=O	
WLAN-CR-15	The Inner VPN Component must use Tunnel Mode IPsec or Transport Mode IPsec using an associated IP tunneling protocol (e.g., Transport Mode IPsec with GRE).	T=O	
WLAN-CR-16	All Access Systems and VPN Gateway components must use Galois Counter Mode (GCM) for IKE encryption.	O	WLAN-CR-5
WLAN-CR-17	All IPsec connections must use IETF standards compliant with IKE implementations as specified in Commercial National Security Algorithm (CNSA) Suite 2.0 Profile for IPsec (*draft-guthrie-cnsa2-ipsec-profile)* including RFC 9370, RFC 9242 and RFC 7383.	O	WLAN-CR-1
WLAN-CR-18	All IPsec connections must use multiple key exchanges with an initial IKEv2 SA key exchange and an intermediate IKEv2 key exchange: • IKE_SA_INIT: The IKEv2 SA key exchange performed in IKE_SA_INIT must use a CNSA 1.0 key establishment algorithm (as specified in Table 15). • IKE_INTERMEDIATE: The IKEv2 SA key establishment performed in the IKE_INTERMEDIATE exchange must use ML-KEM-1024 (as specified in Table 16).	O	WLAN-CR-1
WLAN-CR-19	The VPN Components must use algorithms from the algorithm suite in Table 16 for all IPsec VPN tunnels, with the exception of the IKE_SA_INIT exchange.	O	WLAN-CR-1

12.6 WLAN Access System Configuration Requirements

The WLAN Access System is involved in establishing two encrypted channels. Once the WLAN Authentication Server passes the PMK to the WLAN Access System, the WLAN Access System establishes an encrypted channel with the WLAN Client for passing data. The WLAN Access System acts as a pass-through for the initial authentication exchange between the WLAN Client and the WLAN Authentication Server during which the PMK is securely negotiated.

Table 20. WLAN Access System (WS) Configuration Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-WS-1	The WLAN Access System must act as an EAP-TLS pass-through between the WLAN Client and WLAN Authentication Server for authentication and key establishment.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-WS-2	The WLAN Access System must negotiate new session keys with the WLAN Clients at least once per hour.	T=O	
WLAN-WS-3	Requirement has been relocated to the *Key Management Requirements Annex*.		
WLAN-WS-4	A unique device certificate must be loaded into the Authentication Server along with the corresponding CA (signing) certificate.	T=O	
WLAN-WS-5	When supporting multiple enclaves, the WLAN Access System must assign a firewall ACL to EUDs based on the attribute information provided by the Authentication Server.	T=O	
WLAN-WS-6	When supporting multiple enclaves, the WLAN Access System must route EUD traffic over the appropriate interface based on attribute information provided by the Authentication Server.	T=O	
WLAN-WS-7	When supporting multiple enclaves, the WLAN Access System must use unique physical internal interfaces for each enclave of the solution (i.e., VLAN Trunking of multiple enclaves is not permitted).	T=O	

Table 21. Wireless Infrastructure Authentication (IA) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-IA-1	The WLAN Access System and the WLAN authentication server must be physically co-located in the same rack and directly connected to each other.	T	WLAN-IA-2 and WLAN-IA-3
WLAN-IA-2	Communications between the WLAN Access System and the WLAN Authentication Server must be established with either an IPsec tunnel (using either IKEv2) or TLS/RADsec connection.	O	WLAN-IA-1
WLAN-IA-3	The IKE exchange and IPsec tunnel between the WLAN Access System and the WLAN Authentication Server must use protocols and algorithms selected from the Algorithm Suite in Table 15.	O	WLAN-IA-1, WLAN-IA-13, WLAN-IA-14, and WLAN-IA-15
WLAN-IA-4	The ESP SA tunnel between the WLAN Access System and the WLAN Authentication Server must be ESP using AES in Cipher Block Chaining (CBC) mode with a SHA-based HMAC for integrity.	T	WLAN-IA-5
WLAN-IA-5	The ESP SA tunnel between the WLAN Access System and the WLAN Authentication Server must be ESP use AES in GCM mode.	O	WLAN-IA-4
WLAN-IA-6	The lifetime of the IKE SA between the WLAN Access System and the WLAN Authentication Server must be set to 24 hours.	T=O	
WLAN-IA-7	The lifetime of the ESP SA between the WLAN Access System and the WLAN Authentication Server must be set to 8 hours or less.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-IA-8	The WLAN Access System and the WLAN Authentication Server must authenticate one another using X.509 v3 certificates.	O	WLAN-IA-9
WLAN-IA-9	The WLAN Access System and the WLAN Authentication Server must authenticate one another using pre-shared keys.	T	WLAN-IA-8
WLAN-IA-10	Composition rules for a pre-shared key between the WLAN Access System and the WLAN Authentication Server must be set by the Security Administrator.	T=O	
WLAN-IA-11	The entropy of a pre-shared key between the WLAN Access System and the WLAN Authentication Server must be a minimum of 256 bits.	T=O	
WLAN-IA-12	Withdrawn		
WLAN-IA-13	The IKE exchanges and IPsec tunnel between the WLAN Access System and the WLAN Authentication Server must use protocols and algorithms selected from the Algorithm Suite in Table 16, with the exception of the IKE_SA_INIT exchange.	O	WLAN-IA-3
WLAN-IA-14	All IPsec connections must use IETF standards compliant with IKE implementations as specified in Commercial National Security Algorithm (CNSA) Suite 2.0 Profile for IPsec (*draft-guthrie-cnsa2-ipsec-profile)* including RFC 9370, RFC 9242, and RFC 7383.	O	WLAN-IA-3
WLAN-IA-15	All IPsec connections must use multiple key exchanges with an initial IKEv2 SA key exchange and an intermediate IKEv2 key exchange: • IKE_SA_INIT: The IKEv2 SA key exchange performed in IKE_SA_INIT must use a CNSA 1.0 key establishment algorithm (as specified in Table 15). • IKE_INTERMEDIATE: The IKEv2 SA key establishment performed in the IKE_INTERMEDIATE exchange must use ML-KEM-1024 (as specified in Table 16).	O	WLAN-IA-3

Table 22. Wireless Authentication and Authorization (AA) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-AA-1	The WLAN Authentication Server and WLAN Client must perform mutual authentication using EAP-TLS with device certificates.	T=O	
WLAN-AA-2	The WLAN Client and the WLAN Authentication Server must use the AES key size and mode for WPA3 Enterprise from Table 17.	T	WLAN-AA-3

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-AA-3	The WLAN Client and the WLAN Authentication Server must use the AES key size and mode for WPA3 Enterprise from Table 18.	O	WLAN-AA-2
WLAN-AA-4	The WLAN Client and WLAN Authentication Server must use the EAP-TLS Cipher suite from the Threshold section of Table 17.	T	WLAN-AA-5
WLAN-AA-5	The WLAN Client and WLAN Authentication Server must use the EAP-TLS Cipher suite from the Objective section of Table 18.	O	WLAN-AA-4

Table 23. Wireless Authentication Server (WA) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-WA-1	The WLAN AS must use the most current CRL to check revocation status of the WLAN Client Certificate. If CRL does not exist, is invalid or has expired, authentication of the EUD will fail.	T=O	
WLAN-WA-2	Requirement has been relocated to the *Key Management Requirements Annex*.		
WLAN-WA-3	The WLAN Authentication Server must only successfully authenticate a WLAN Client if the WLAN Client's certificate contains an extendedKeyUsage certificate extension indicating support for Client Authentication (OID 1.3.6.1.5.5.7.3.2).	T=O	
WLAN-WA-4	The WLAN AS must use the Distinguished Name or the Subject Alternate Name contained in the WLAN Client's certificate to authenticate the identity of the WLAN Client.	T=O	
WLAN-WA-5	The WLAN Authentication Server must verify that the WLAN Client’s certificate is not expired.	T=O	
WLAN-WA-6	The WLAN AS must ensure that the WLAN Client’s certificate chain is rooted by the WLAN trusted root Certificate Authority.	T=O	
WLAN-WA-7	Withdrawn		
WLAN-WA-8	The WLAN Authentication Server must authenticate the identity of the WLAN Client by verifying that the WLAN Client’s certificate is not revoked.	T=O	
WLAN-WA-9	When supporting multiple enclaves, the AS must verify that the Common Name presented by the EUD certificate is included on an allowlist tied to an enclave.	T	WLAN-WA-10
WLAN-WA-10	When supporting multiple enclaves, the AS must verify that the certificate presented includes information in the Distinguished Name or Policy OIDs that ties the device to a single enclave.	O	WLAN-WA-9
WLAN-WA-11	When supporting multiple enclaves, the AS must provide attribute information on the appropriate enclave for the EUD to the Wireless Access System.	T=O	
WLAN-WA-12	The AS must log all successful authentication attempts.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-WA-13	The AS must log all failed authentication attempts.	T=O	

12.7 PORT FILTERING REQUIREMENTS

Port Filtering is composed of a component configured with ACLs. The system ensures that the traffic flowing to and from each component on the network is appropriate for the functionality of the component within the Campus WLAN solution.

Table 24. Solution Components Port Filtering (PF) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-PF-1	All components within the solution must have all network interfaces restricted to the fewest address ranges, ports, and protocols possible.	T=O	
WLAN-PF-2	All components within the solution must have all unused network interfaces disabled.	T=O	
WLAN-PF-3	For all interfaces connected to a Gray Network, traffic filtering rules must be applied to both inbound and outbound traffic, such that only EAP-TLS, IKE, IPsec, and control plane protocols (as defined in this Capability Package) approved by policy are allowed. All packets not explicitly allowed must be blocked.	T=O	
WLAN-PF-4	Any service or feature that allows an EUD to contact a third-party server (such as one maintained by the manufacturer) must be blocked.	T	WLAN-PF-5
WLAN-PF-5	Any service or feature that allows a EUD to contact a third-party server (such as one maintained by the manufacturer) must be disabled.	O	WLAN-PF-4
WLAN-PF-6	The WLAN Access System must block all data ports and IP addresses on their Gray Management network interface that are not necessary for the management of the WLAN Access System.	T=O	
WLAN-PF-7	Interfaces of the WLAN Access System must be based on known MAC addresses of EUDs to further protect against unknown WLAN Clients.	T=O	
WLAN-PF-8	Traffic filtering rules on the EUD must be applied based on known VPN Gateway addresses or address range to further protect against unknown IPsec traffic.	T=O	
WLAN-PF-9	The internal interface of the Inner VPN Gateway must prohibit all management plane traffic (e.g., SSHv2, Remote Desktop Protocol (RDP), Telnet) originating from EUDs destined for the Red Network.	T=O	
WLAN-PF-10	The internal interface of the Inner VPN Gateway must prohibit traffic destined for the Red Management Network (e.g., Red Management Network IP addresses) originating from End User Devices.	T=O	
WLAN-PF-11	CDPs must only allow inbound HTTP traffic.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-PF-12	For the Inner VPN Gateway interface connected to a Gray Network, traffic filtering rules must be applied to both inbound and outbound traffic, such that only IKE, ESP, and management and control plane protocols (as defined in this CP) approved by organization-defined policy are allowed.	T=O	
WLAN-PF-13	The Inner Firewall must implement an ACL which only permits ingress/egress traffic from/to Inner Encryption endpoints.	T=O	
WLAN-PF-14	Multicast messages received on any interfaces of the WLAN Access System, Gray Firewall, and Inner Encryption Components must be dropped.	T=O	
WLAN-PF-15	Management plane traffic must only be initiated from the Gray administrative work stations with the exception of logging or authentication traffic which may be initiated from WLAN Access System.	T=O	
WLAN-PF-16	The Gray Firewall must only permit EUDs traffic to the Inner Encryption Component associated with the appropriate classification level.	T=O	
WLAN-PF-17	EUDs must prohibit ingress and egress of routing protocols.	T=O	

12.8 End User Device Provisioning Requirements

Table 25. EUD Provisioning Requirements (PR)

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-PR-1	A Provisioning WLAN using WPA3-PSK authentication and encryption must be established on the Red Network to support wireless provisioning of EUDs.	T	WLAN-PR-5
WLAN-PR-2	The Provisioning WLAN on the Gray Management Network must be contained within a shielded enclosure that provides 100 dB of attenuation across the frequency range from 2 to 6 GHz.	T	WLAN-PR-5
WLAN-PR-3	The Provisioning WLAN on the Red Network must be contained within a shielded enclosure that provides 100 dB of attenuation across the frequency range from 2 to 6 GHz.	T	WLAN-PR-5
WLAN-PR-4	EUDs must be provisioned over the provisioning WLANs.	T	WLAN-PR-5
WLAN-PR-5	EUDs must be provisioned over wired connections.	O	WLAN-PR-4
WLAN-PR-6	When a EUD has been successfully provisioned, its identity (ITU-T X.509v3 Distinguished Name or Subject Alternate Name) must be recorded in authorization databases accessible to the WLAN Authentication Server and VPN Gateway.	T=O	
WLAN-PR-7	EUDs must be provisioned to be disabled by having their certificates revoked.	T=O	
WLAN-PR-8	The EUD must be loaded with an authorized software build during provisioning.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-PR-9	The EUD must be loaded with WLAN and VPN configuration profiles during provisioning.	T=O	
WLAN-PR-10	Strong passwords for the EUD must be used to comply with the requirements of the policy established by the AO.	T=O	
WLAN-PR-11	Services not authorized by the AO must be disabled during the provisioning of the EUD.	T=O	

12.9 Configuration Requirements for Wireless Intrusion Detection System (WIDS)

Configuration Requirements for WIDS have been relocated to the *Wireless Intrusion Detection System/Wireless Intrusion Prevention System (WIDS/WIPS) Annex.*

Table 26. WIDS/WIPS Requirements

Req #	Requirement Description	Threshold/ Objective	Alternative
WLAN-WIDS-0	Meet all requirements defined in the *CSfC Wireless Intrusion Detection System/Wireless Intrusion Prevention System (WIDS/WIPS) Requirements Annex* that apply to the WLAN CP for government private wireless.	T=O	

12.10 Configuration Change Detection Requirements

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

12.11 Device Management Requirements

Only authorized Security Administrators will be allowed to administer the components. The WLAN solution will be used as transport for the SSHv2, IPsec, or TLS data from the Administration Workstation to the component.

Table 27. Device Management (DM) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-DM-1	Administration Workstations must be dedicated for the purposes given in the CP and must be physically separated from workstations used to manage non-CSfC solutions.	T=O	
WLAN-DM-2	Withdrawn		
WLAN-DM-3	Antivirus software must be running on all Administration Workstations.	T=O	
WLAN-DM-4	All components must be configured to restrict the IP address range for the network administration device to the smallest range possible.	T=O	
WLAN-DM-5	The Gray Management network must not be directly connected to Non-secure Internet Protocol Router Network (NIPRNet) or any other Unclassified network not dedicated to the administration of CSfC solutions.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-DM-6	All administration of solution components must be performed from an Administration Workstation remotely using one of SSHv2, IPsec, or TLS 1.2 or later version; or by managing the solution components locally.	T=O	
WLAN-DM-7	Security Administrators must authenticate to solution components before performing administrative functions.	T	WLAN-DM-8
WLAN-DM-8	Security Administrators must authenticate to solution components with Commercial National Security Algorithm (CNSA) Suite-compliant certificates before performing administrative functions remotely.	O	WLAN-DM-7
WLAN-DM-9	Security Administrators must establish a security policy for EUDs per the implementing organization's local policy to include procedures for continuous physical control.	T=O	
WLAN-DM-10	Withdrawn		
WLAN-DM-11	Security Administrators must initiate certificate signing requests for solution components as part of their initial keying within the solution.	T=O	
WLAN-DM-12	Devices must use Enrollment over Secure Transport (EST) as detailed in IETF RFC 7030 for certificate management.	O	Optional
WLAN-DM-13	Withdrawn		
WLAN-DM-14	Withdrawn		
WLAN-DM-15	Withdrawn		
WLAN-DM-16	When managing solution components over the Black Network, the management traffic must be encrypted with a CNSA Suite algorithm (See Table 17).	T=O	
WLAN-DM-17	The CSfC solution owner must identify authorized SAs to initiate certificate requests.	T=O	
WLAN-DM-18	Authentication of SAs must be enforced by either procedural or technical controls.	T=O	
WLAN-DM-19	The same administration workstation must not be used to manage Inner Encryption Components and the WLAN Access System.	T=O	
WLAN-DM-20	The Gray Management Network must be used exclusively for all management of the Outer Encryption Component, Gray Firewall, if present, and Solution Components within the Gray Network.	T=O	
WLAN-DM-21	The Gray Management Network must not be directly connected to the Non-secure Internet Protocol Router Network (NIPRNet) or any other Unclassified network not dedicated to the administration of CSfC solutions.	T=O	
WLAN-DM-22	The Gray Management and Gray Data Networks must be separated by the Gray Firewall using unique physical interfaces and stateful traffic filtering rules (e.g., ACLs).	T=O	WLAN-DM-23
WLAN-DM-23	The Gray Management and Gray Data Networks must be separated by the Gray Firewall using unique physical interfaces and with at least two separate VRFs for the Gray Data Network and Gray Management Network.	O	WLAN-DM-22

12.12 Continuous Monitoring Requirements

Continuous Monitoring Requirements have been relocated to the *Continuous Monitoring Requirements Annex.*

Table 28. Continuous Monitoring Requirements

Req #	Requirement Description	Threshold/ Objective	Alternative
WLAN-CM-0	Meet all requirements defined in the *Continuous Monitoring Annex* that apply to the WLAN CP.	T=O	

12.13 Auditing Requirements

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

12.14 Key Management Requirements

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

Table 29. Key Management Requirements

Req #	Requirement Description	Threshold/ Objective	Alternative
WLAN-KM-0	Meet all requirements defined in the *CSfC Key Management Requirements Annex* that apply to the WLAN CP.	T=O	

12.15 Gray Firewall Requirements

Table 30. Gray Firewall (FW) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-FW-1	Gray Network Firewall must permit IKE and IPsec traffic between the EUDs VPN Client and VPN Gateway protecting networks of the same classification level.	T=O	
WLAN-FW-2	Gray Network Firewall must allow HTTP traffic between the Authentication Server and the Gray CDP or OCSP responder.	T	WLAN-FW-3 and WLAN-FW-4
WLAN-FW-3	Gray Network Firewall must allow HTTP GET requests from the Authentication Server to the Gray CDP or OCSP responder for the URL of the CRL OCSP Response needed by the VPN Gateway, and block all other HTTP requests.	O	WLAN-FW-2
WLAN-FW-4	Gray Network Firewall must allow HTTP responses from the Gray CDP or OCSP responder to the Authentication Server that contain a well-formed CRL per IETF RFC 5280 or OCSP Response per RFC 6960, and block all other HTTP responses.	O	WLAN-FW-2
WLAN-FW-5	Gray Network Firewall must only accept management traffic on the physical ports connected to the Gray Management network.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-FW-6	Gray Network Firewall must only permit packets whose source and destination IP addresses match the external interfaces of the VPN Components that support Red Networks of the same classification level.	T=O	
WLAN-FW-7	Gray Network Firewall must block all packets whose source address does not match a list of addresses or address ranges known to be reachable from the interface on which the packet was received.	T=O	
WLAN-FW-8	Gray Network Firewall must deny all traffic that is not explicitly allowed by requirements WLAN-FW-1, WLAN-FW-2, WLAN-FW-3, WLAN-FW-4, or WLAN-FW-5.	T=O	
WLAN-FW-9	Gray Network Firewall must allow control plane traffic (NTP, DHCP, DNS).	T=O	

12.16 MULTI-FACTOR AUTHENTICATION REQUIREMENTS

Table 31. Multi-Factor Authentication Use Case Requirements

Req #	Requirement Description	Threshold/ Objective	Alternative
WLAN-MFA-1	A second factor of authentication, such as a token or smartcard, must be implemented for logging into a Physical EUD in a user's possession.	O	WLAN-MFA-2 or WLAN-MFA-3
WLAN-MFA-2	A second factor of authentication, such as a token or smartcard, must be implemented for an EUD to authenticate to the Inner Encryption Component.	O	WLAN-MFA-1 or WLAN-MFA-3
WLAN-MFA-3	A second factor of authentication, such as a token or smartcard, must be implemented for a user to authenticate into a Red VDI Environment user session.	O	WLAN-MFA-1 or WLAN-MFA-2
WLAN-MFA-4	The second factor of authentication must be a physically separate device from the EUD.	O	
WLAN-MFA-5	The second factor of authentication must not be used as a replacement for the primary authentication method.	O	
WLAN-MFA-6	The second factor of authentication must implement a user generated password and a token generated one-time password.	O	WLAN-MFA-14
WLAN-MFA-7	The management server for the second factor of authentication must be located in the 'Red Management Services' network or the 'Red' network.	O	WLAN-MFA-14
WLAN-MFA-8	The token generated one-time password must implement a time-based algorithm.	O	WLAN-MFA-14
WLAN-MFA-9	In the event of loss of continuous physical control, the token must be considered compromised, reported to the AO/Delegated Approval Authority (DAA), and must not be reused.	O	
WLAN-MFA-10	If the second factor of authentication's seed file is compromised, all tokens are considered compromised and must be replaced.	O	WLAN-MFA-14

Req #	Requirement Description	Threshold/ Objective	Alternative
WLAN-MFA-11	During procurement, the vendor must not be permitted to store backups of seed files.	O	WLAN-MFA-14
WLAN-MFA-12	All seed files must be encrypted during transport.	O	WLAN-MFA-14
WLAN-MFA-13	Authentication tokens must be physically secured in a separate storage container from the EUD.	O	
WLAN-MFA-14	The second factor of authentication must implement a user generated password and a PKI based smart card.	O	WLAN-MFA-6 WLAN-MFA-7 WLAN-MFA-8 WLAN-MFA-10 WLAN-MFA-11 WLAN-MFA-12

13 REQUIREMENTS FOR SOLUTION OPERATION, MAINTENANCE, AND HANDLING

13.1 USE AND HANDLING OF SOLUTIONS (GD) REQUIREMENTS

The following requirements must be followed regarding the use and handling of the solution.

Table 32. Use and Handling of Solutions Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-GD-1	All solution infrastructure components must be physically protected as classified devices, classified at the highest classification level of the Red Network.	T=O	
WLAN-GD-2	Only authorized and appropriately cleared (or escorted) administrators and security personnel must have physical access to the solution Infrastructure components.	T=O	
WLAN-GD-3	Only authorized and appropriately cleared users, administrators, and security personnel must have physical access to EUDs.	T=O	
WLAN-GD-4	All components of the solution must be disposed of as classified devices, unless declassified using AO-approved procedures.	T=O	
WLAN-GD-5	EUDs using a NSA-approved DAR solution must be disposed of in accordance with the disposal requirements for the DAR solution.	T=O	
WLAN-GD-6	All EUDs must have their certificates revoked prior to disposal.	T=O	
WLAN-GD-7	Users must periodically inspect the physical attributes of EUDs for signs of tampering or other unauthorized changes.	T=O	
WLAN-GD-8	Acquisition and procurement documentation must not include information about how the equipment will be used, to include that it will be used to protect classified information.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-GD-9	The solution owner must allow, and fully cooperate with, NSA or its authorized agent to perform an IA compliance audit (including, but not limited to, inspection, testing, observation, interviewing) of the solution implementation to ensure it meets the latest version of the CP.	T=O	
WLAN-GD-10	As part of the annual solution re-registration process, the AO will ensure that a compliance audit must be conducted every year against the latest version of the WLAN CP.	T=O	
WLAN-GD-11	Results of the compliance audit must be provided to and reviewed by the AO.	T=O	
WLAN-GD-12	Customers interested in registering their solution against the WLAN CP must register with NSA and receive approval prior to AO authorization to operate.	T=O	
WLAN-GD-13	The implementing organization must complete and submit a WLAN CP requirements compliance matrix to their respective AO.	T=O	
WLAN-GD-14	Registration and re-registration against the WLAN CP must include submission of WLAN CP registration forms and compliance matrix to NSA.	T=O	
WLAN-GD-15	When a new approved version of the WLAN CP is published by NSA, the AO must ensure compliance against this new CP within six months or by the next re-registration date (whichever is greater).	T=O	
WLAN-GD-16	Solution implementation information, which was provided to NSA during solution registration, must be updated annually (in accordance with Section 15.3) as part annual solution re-registration process.	T=O	
WLAN-GD-17	Audit log data must be maintained for a minimum of 1 year.	T=O	
WLAN-GD-18	The amount of storage remaining for audit events must be assessed quarterly in order to ensure that adequate memory space is available to continue recording new audit events.	T=O	
WLAN-GD-19	Audit data must be frequently off-loaded to a backup storage medium.	T=O	
WLAN-GD-20	A set of procedures must be developed by the implementing organization 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	
WLAN-GD-21	The implementing organization must develop a continuity of operations plan for auditing capability, which includes a mechanism or method for determining when the audit log is reaching its maximum storage capacity.	T=O	
WLAN-GD-22	The implementing organization must develop a continuity of operations plan for auditing capability, which includes a mechanism or method for off-loading audit log data for long- term storage.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-GD-23	The implementing organization must develop a continuity of operations plan for auditing capability, which includes a mechanism or method for responding to an overflow of audit log data within a product.	T=O	
WLAN-GD-24	The implementing organization must develop a continuity of operations plan for auditing capability which includes a mechanism or method for ensuring that the audit log can be maintained during power events.	T=O	
WLAN-GD-25	Strong passwords must be used that comply with the requirements of the AO.	T=O	
WLAN-GD-26	Security critical patches must be tested and subsequently applied to all components in the solution in accordance with local policy and this CP.	T=O	
WLAN-GD-27	Local policy must dictate how the Security Administrator will install patches to solution components.	T=O	
WLAN-GD-28	Solution components must comply with local TEMPEST policy.	T=O	
WLAN-GD-29	Software, settings, keys, and all other configuration data persistently stored on EUDs must be handled as controlled unclassified information or higher classification.	T=O	
WLAN-GD-30	All hardware components must be tracked through an AO-approved inventory management process that identifies each component as part of a CSfC solution.	T=O	
WLAN-GD-31	If a CDS is being leveraged within the solution, then it must adhere with all applicable organizational policy and be on the NCDSMO CDS Baseline. (For example, DoD customers must also adhere to DoDI 8540.01 and the DISN Connection Process Guide).	T=O	

Additional WLAN-GD requirements can be found in Section 14.

13.2 Requirements for Incident Reporting

Table 33 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 and Auditors are familiar with maintaining the solution in accordance with this CP. Familiarity with the approved configuration of the solution will better equip operations and maintenance personnel 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 33 only provides requirements directly related to the incident reporting process. See Section 12.12 for requirements supporting the detection of events that may reveal that a reportable incident has occurred.

Table 33. Incident Reporting Requirements (RP)

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-RP-1	Solution owners must report confirmed incidents meeting the criteria in WLAN-RP-3 through WLAN-RP-15 within 24 hours of detection via Joint Incident Management System (JIMS) or contacting NSA as specified in the CSfC Registration Letter issued for the solution.	T=O	
WLAN-RP-2	At a minimum, the organization must provide the following information when reporting security incidents: • CSfC Registration Number • Point of Contact (POC) name, phone, email • Alternate POC name, phone, email • Classification 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	
WLAN-RP-3	Solution owners must report a security failure in any of the CSfC solution components.	T=O	
WLAN-RP-4	Solution owners must report any evidence of a compromise or spillage of classified data caused by a failure of the CSfC solution.	T=O	
WLAN-RP-5	For Gray Network interfaces, solution owners must report any malicious inbound and outbound traffic.	T=O	
WLAN-RP-6	Solution owners must report any evidence of an unauthorized device/user gaining access to the classified network via the solution.	T=O	
WLAN-RP-7	Solution owners must report if a solution component sends traffic with an unauthorized destination address.	T=O	
WLAN-RP-8	Solution owners must report any malicious configuration changes to the components.	T=O	
WLAN-RP-9	Solution owners must report any unauthorized escalation of privileges to any of the CSfC solution components.	T=O	
WLAN-RP-10	Solution owners must report if two or more simultaneous VPN connections from different IP addresses are established using the same EUD device certificate.	T=O	
WLAN-RP-11	Solution owners must report any evidence of malicious physical tampering with solution components.	T=O	
WLAN-RP-12	Solution owners must report any evidence that one or both of the layers of the solution failed to protect the data.	T=O	
WLAN-RP-13	Solution owners must report any significant degradation of services provided by the solution.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-RP-14	Solution owners must report malicious discrepancies in the number of connections established the WLAN Access System.	T=O	
WLAN-RP-15	Solution owners must report malicious discrepancies in the number of VPN connections established by the Inner VPN Gateway.	T=O	

14 ROLE-BASED PERSONNEL REQUIREMENTS

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

Security Administrator – The Security Administrator must be responsible to maintain, monitor, and control all security functions for the entire suite of products composing the WLAN solution. Security Administrator duties include, but are not limited to, the following:

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

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

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

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

5) Ensure that the implemented WLAN solution remains compliant with the latest version of this CP.

6) Provision and maintain EUDs in accordance with this CP for implementations that include them.

Auditor – The Auditor must be responsible to review the actions performed by the Security Administrator and events recorded in the audit logs to ensure that no action or event represents a compromise to the security of the WLAN solution. Auditor duties include, but are not limited to:

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

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

3) The Auditor will only be authorized access to Outer and Inner administrative components.

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

1) Acquire the products that compose the solution.

2) Configure the WLAN solution in accordance with this CP.

3) Document, test, and maintain the solution.

4) Respond to incidents affecting the solution.

End User –An End User may operate an EUD from physical locations not owned, operated, or controlled by the government. The End User must be responsible for operating the EUD in accordance with this CP and an organization-defined user agreement. Remote User duties include, but are not limited to the following:

- Ensure the EUD is only operated in physical spaces which comply with the end user agreement.
- Alert the Security Administrator immediately upon a EUD being lost, stolen, or suspected of being tampered with.

Additional requirements related to the personnel that perform these roles in a WLAN solution are as follows:

Table 34. Role-Based Personnel Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-GD-32	The Security Administrator, Auditor, EUD User, and solution Integrators must be cleared to the highest level of data protected by the solution. When an Enterprise CA is used in the solution, the administrator for that system may also support this solution, provided they meet this requirement.	T=O	
WLAN-GD-33	The Security Administrator and Auditor roles must be performed by different people.	T=O	
WLAN-GD-34	All Security Administrators, EUD Users, and Auditors must meet local IA training requirements.	T=O	
WLAN-GD-35	Upon discovering an EUD is lost, stolen or altered, an EUD User must immediately report the incident to their Security Administrator.	T=O	
WLAN-GD-36	Requirement has been relocated to the *Key Management Requirements Annex*.		
WLAN-GD-37	The Security Administrator(s) for the Inner Encryption Endpoints and supporting components on Enterprise/Red Networks must be different individuals from the Security Administrator(s) for the WLAN Access System and supporting components on Gray Networks.	T=O	
WLAN-GD-38	Administrators must periodically inspect the physical attributes of infrastructure hardware for signs of tampering or other unauthorized changes.	T=O	
WLAN-GD-39	Withdrawn		

15 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 a System 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 WLAN solution as described in Section 15.1.
- The customer has system certification and accreditation performed using the risk assessment information referenced in Section 15.2.
- The customer provides the results from testing and system certification and accreditation to the AO for use in making an approval decision. The AO is ultimately responsible for ensuring that all requirements from the CP have been properly implemented in accordance with the CP.
- The customer registers the solution with NSA and re-registers yearly to validate its continued use as detailed in Section 15.3.
- Customers who want to use a variant of the solution detailed in this CP will contact their NSA/CSD Client Advocate to determine ways to obtain NSA approval.
- The AO will ensure that a compliance audit must be conducted every year against the latest version of the WLAN CP, and the results must be provided to the AO.
- The AO will ensure that certificate revocation information is updated on all the solution components in the 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 13.2.

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

15.1 SOLUTION TESTING

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

The security features and operational capabilities associated with the use of the solution must be tested. The following is a general high-level methodology for developing the test plan and procedures and for the execution of those procedures to validate the implementation and functionality of the WLAN

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. At a minimum, include product model and serial numbers, and software version numbers.

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

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

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

The following test requirement has been developed to ensure that the WLAN solution functions properly and meets the configuration requirements from Section 12. Testing of these requirements should be used as a minimum framework for the development of the detailed test plan and procedures

Table 35. Test Requirement

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

15.2 Risk Assessment

The risk assessment of the WLAN 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/CSD Client Advocate 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 must be provided a copy of the NSA risk assessment for their consideration in approving the use of the solution.

15.3 Registration of Solutions

All customers using CSfC solutions to protect information on National Security Systems must register their solution with NSA prior to operational use. This registration will allow NSA to track where WLAN CP 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 at (https://www.nsa.gov/resources/commercial-solutions-for-classified-program).

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 in order 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 CP that has been approved by the D/NM is published, customers will have six months to bring their solutions into compliance with the new version of the CP and re-register their solution (see requirement WLAN-GD-15). Customers are also required to update their registrations whenever the information provided on the registration form changes, to include AO and POC information.

APPENDIX A. GLOSSARY OF TERMS

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), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls (NIST SP 800-37).

Authorization Boundary – All components of an information system to be authorized for operation by an AO and excludes separately authorized systems, to which the information system is connected.

Authorizing Official (AO) – 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.

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.

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.

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.

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 (See Section 4.2.3).

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

Certificate 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 CP 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).

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

Commercial National Security Algorithm (CNSA) - Set of commercial algorithms capable of protecting data through Top Secret level (previously known as Suite B).

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.

Continuous Physical Control - The AO defines what is considered “Continuous Physical Control.” Previously called “positive control.”

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.

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 (Committee on National Security Systems Instruction CNSSI 4009).

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

End User Device (EUD) – A form-factor agnostic component of the WLAN solution that can include a mobile phone, tablet, or laptop computer. EUDs can be composed of multiple components to provide physical separation between layers of encryption.

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 (see Section 4.2.2).

Gray Firewall – A stateful traffic filtering firewall placed on the Gray Network to provide filtering of ports, protocols, and IP addresses to ensure traffic reaches the correct Inner Encryption Endpoint or is dropped.

Internal Interface – The interface on a VPN Gateway or Inner Encryption Component that connects to the inner network (i.e., the Gray Network on the WLAN Access System or the Red Network on the Inner Encryption Component).

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 SIEM 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.

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

Red Network – A network that contains classified data that is not encrypted (see Section 4.2.1)

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

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 VPN tunnel (either on the same interface or another network interface). Split tunneling is explicitly prohibited in WLAN CP compliant configurations (see WLAN-CR-12).

Secure Real-Time Protocol (SRTP) Client – A component on the EUD that facilitates encryption for voice communications.

Transport Layer Security (TLS) Client – A component on a TLS EUD that provides the Inner layer of Data in Transit (DIT) encryption.

TLS Component – Refers to both TLS Clients and TLS-Protected Servers.

Virtual Private Network (VPN) Client – A VPN application installed on an EUD.

VPN Component – The term used to refer to VPN Gateways and VPN Clients.

VPN Gateway – A VPN device physically located within the VPN infrastructure.

VPN Infrastructure – Physically protected in a secure facility and includes Inner, Certificate Authorities, and Administration Workstations, but does not include EUDs.

APPENDIX B. ACRONYMS

Acronym	Meaning
ACL	Access Control List
AES	Advanced Encryption Standard
AO	Authorizing Official
AP	Access Point
ARP	Address Resolution Protocol
AS	Authentication Server
BIOS	Basic Input/Output System
CA	Certificate Authority
CAA	Certificate Authority Administrator
CBC	Cipher Block Chaining
CDP	CRL Distribution Point
CDS	Cross Domain Solution
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
CSR	Certificate Signing Request
CSV	Comma Separated Value
CUI	Controlled Unclassified Information
DAR	Data-At-Rest
DDoS	Distributed Denial of Service
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DiT	Data-in-Transit
DM	Device Management
DN	Domain Name
DNS	Domain Name System
D/NM	Deputy National Manager
DoD	Department of Defense
DoE	Department of Energy
DoS	Denial of Service
DSA	Digital Signature Algorithm
DSC	Dedicated Security Component
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
ECDH	Elliptic Curve Diffie-Hellman
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
ESP	Encapsulating Security Payload
EST	Enrollment Over Secure Transport
EUD	End User Device
FIPS	Federal Information Processing Standards

Acronym	Meaning
GCM	Galois Counter Mode
GOTS	Government Off-the-Shelf
GPS	Global Positioning System
HIDS	Host Based Intrusion Detection System
HMAC	Hash-based Message Authentication Code
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IA	Information Assurance
IAVA	Information Assurance Vulnerability Alert
ICT	Information Communication Technology
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IS-IS	Intermediate System to Intermediate System
JIMS	Joint Incident Management System
KM	Key Management
KMI	Key Management Infrastructure
LMS	Leighton-Micali Signature
MAC	Media Access Control
MDF	Mobile Device Fundamentals
MDM	Mobile Device Manager
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism
ML-DSA	Module-Lattice-Based Digital Signature
MOA	Memorandum of Agreement
MTU	Maximum Transmission Unit
NDP	Neighbor Discovery Protocol
NIAP	National Information Assurance Partnership
NIDS	Network-based Intrusion Detection System
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
OID	Object Identifier
OPSEC	Operational Security
OS	Operating System
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PKCS	Public Key Cryptographic Standard
PKI	Public Key Infrastructure
PMK	Pairwise-Master Key

Acronym	Meaning
POC	Point of Contact
PTP	Precision Time Protocol
RADIUS	Remote Authentication Dial in User Service
RDP	Remote Desktop Protocol
RFC	Request for Comment
RSA	Rivest Shamir Adelman algorithm
S3	Secure Sharing Suite
SA	Security Association
SCRM	Supply Chain Risk Management
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SIPRNet	Secret Internet Protocol Router Network
SRTP	Secure Real-Time Protocol
SSH	Secure Shell
SSID	Service Set Identifier
SSHv2	Secure Shell Version 2
T	Threshold
T&E	Test and Evaluation
TFFW	Traffic Filtering Firewall
TLS	Transport Layer Security
URL	Uniform Resource Locator
VDI	Virtual Desktop Interface
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPA3	Wi-Fi Protected Access 3
XMSS	Xtended Merkle Signature Scheme

APPENDIX C. REFERENCES

CNSSI No. 1200	CNSS Instruction No. 1200, *National Information Assurance Instruction for Space Systems Used to Support National Security Missions,* May 7, 2014.	7 May 2014
CNSSI No. 1253	CNSS Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems,* March 27, 2014.	27 March 2014
CNSSI 1300	*CNSSI 1300, National Security Systems Public Key Infrastructure X.509 Certificate Policy*	December 2021
CNSSI 4009	*CNSSI 4009, National Information Assurance (IA) Glossary Committee for National Security Systems.*	March 2022
CNSSP 7	CNSS Policy No. 7, *Policy on the Use of Commercial Solutions to Protect National Security Systems,* December 9, 2015.	9 December 2015
CNSSP 8	CNSS Policy No. 8, *Policy Governing the Release and Transfer of U.S. Government Cryptologic National Security Systems Technical Security Material, Information, and Techniques to Foreign Governments and International Organizations,* August 2012.	August 2012
CNSSP 11	CNSS Policy No. 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Technology Products,* June 10, 2013.	February 2025
CNSSP 15	*CNSS Policy (CNSSP) Number 15, Use of Public Standards for Secure Information Sharing*	October 2016
CNSSP 15	*CNSS Policy (CNSSP) Number 15, National Policy on the Use of Public Standards for Secure Information Sharing (CNSA 2.0)*	December 2024
CNSSP 22	CNSS Policy No. 22*, Policy on Information Assurance Risk Management for National Security Systems,* August 2016.	August 2016
CNSSD 500	CNSS Directive No. 500, *Information Assurance (IA) Education, Training and Awareness,* August 2006.	August 2006
CNSSD 502	CNSS Directive No. 502, *National Directive on Security of National Security Systems,* December 16, 2004.	16 December 2004
CNSSD 505	*CNSS Directive (CNSSD) Number 505, Supply Chain Risk Management (SCRM)*	February 2025
CSfC CM Annex	*CSfC Continuous Monitoring Annex, v1.1.0*	March 2023
CSfC Data-at-Rest CP	*CSfC Data-at-Rest Capability Package, v5.1.0*	March 2026
CSfC KM Req. Annex	*CSfC Key Management Requirements Annex, v3.0.0*	March 2026

CSfC Symmetric KM Req. Annex	*CSfC Symmetric Key Management Requirements Annex, v3.0.0*	March 2026
CSfC WIDS/WIPS Annex	*CSfC Wireless Intrusion Detection System (WIDS)/Wireless Intrusion Prevention System (WIPS) Annex, v2.0.0*	March 2024
FIPS 140-3	*Federal Information Processing Standard 140, Security Requirements For Cryptographic Modules National Institute for Standards and Technology FIPS Publication*	March 2019
FIPS 180-4	*Federal Information Processing Standard 180-4, Secure Hash Standard (SHS)*	August 2015
FIPS 186-4	*Federal Information Processing Standard 186-4, Digital Signature Standard (DSS)*	July 2013
FIPS 197	*Federal Information Processing Standard 197, Advanced Encryption Standard (AES)*	November 2001
FIPS 201-2	*Federal Information Processing Standard 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors*	August 2015
FIPS 203	*Module-Lattice-Based Key-Encapsulation Mechanism Standard*	August 2024
FIPS 204	*Module-Lattice-Based Digital Signature Standard*	August 2024
IPsec VPN Client PP	*Virtual Private Network PP-Module for VPN Client*, Version 2.3	August 2021
ISO 09594-8	*Iso9594-8 Information Technology-Open Systems Interconnection-The Directory – Part 8: Public-key and attribute certificate frameworks*	March 2013
Commercial National Security Algorithm Suite	*NSA Guidance on Encryption Algorithms*	December 2015
RFC 2409	*IETF RFC 2409 The Internet Key Exchange (IKE)*. D. Harkins and D. Carrel.	November 1998
RFC 3647	*IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* Internet Engineering Task Force	November 2003
RFC 3711	*IETF RFC 3711 The Secure Real-Time Transport Protocol (SRTP).* M. Baugher and D. McGrew.	March 2004
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 4492	*IETF RFC 4492 Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS).* S. Blake-Wilson, N. Bolyard, V. Gupta, C. Hawk Corriente, B. Moeller, and Ruhr-Uni Bochum.	May 2006
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 5996	*IETF RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2)*. C. Kaufman, et. al.	September 2010
RFC 6188	*IETF RFC 6188 The Use of AES 192 and AES 256 in Secure RTP.* D. McGrew.	March 2011
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 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 8391	*XMSS: eXtended Merkle Signature Scheme*	May 2018
RFC 8446	*IETF RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3. E. Rescorla.*	August 2018
RFC 8784	*Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security*	June 2020
RFC 9151	*IETF RFC 9151 Commercial National Security Algorithm (CNSA) Profile for TLS and DTLS 1.2 and 1.3.* D. Cooley.	April 2022

NIST SP 800-37 Rev. 2	National Institute of Standards and Technology (NIST SP) 800-37 Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* December 2018.	December 2018
SP 800-53	*NIST Special Publication 800-53 Rev. 5, Security and Privacy Controls for Federal Information Systems and Organizations*.	December 2020
SP 800-56A	*NIST Special Publication 800-56A Rev. 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*. E. Barker, et. al.	April 2018
SP 800-56B	*NIST Special Publication 800-56B Rev. 2, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*. E. Barker, et. al.	March 2019
SP 800-56C	*NIST Special Publication 800-56C Rev. 2, Recommendation for Key Derivation Methods in Key-Establishment Schemes*. L. Chen.	August 2020
NIST SP 800-111	National Institute of Standards Special Publication (NIST SP) 800-111, *Guide to Storage Encryption Technologies for End User Devices,* November 2007.	November 2007
NIST SP 800-131A	*NIST Special Publication 800-131A Rev. 2, Transitioning the Use of Cryptographic Algorithms and Key Lengths*. E. Barker.	March 2019
NIST SP 800-137	National Institute of Standards and Technology Special Publication (NIST SP) 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* September 2011.	September 2011
SP 800-147	*NIST Special Publication 800-147, BIOS Protection Guidelines*. D. Cooper, et. al.	April 2011
NIST SP 800-208	*Recommendation for Stateful Hash-Based Signature Schemes*	October 2020
RFC 9370	Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)	May 2023
RFC 9242	Intermediate Exchange in the Internet Key Exchange Protocol Version 2 (IKEv2)	May 2022
RFC 7383	Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation	November 2014
draft-kampanakis-ml-kem-ikev2	Post-quantum Key Exchange with ML-KEM in the Internet Key Exchange Protocol Version 2 (IKEv2)	
draft-becker-cnsa2-tls-profile	Commercial National Security Algorithm (CNSA) Suite Profile for TLS 1.3	
RFC 9190	EAP-TLS 1.3: Using the Extensible Authentication Protocol with TLS 1.3	February 2022

APPENDIX D. TACTICAL SOLUTION IMPLEMENTATIONS

Although the majority of customers instantiating solutions based on the Campus WLAN CP will be used for Strategic or Operational Environments, some organizations may deploy the Campus WLAN CP in Tactical Environments. These Tactical Environments include a specific set of Size, Weight, and Power (SWaP) constraints not found in traditional environments.

Organizations intending to deploy a Campus WLAN CP Solution for Tactical Environments may use this Appendix, which accommodates the SWaP constraints unique to their environment. This Appendix may only be used to protect Tactical Data classified as SECRET or below. The CP follows CNSSI 4009, which defines Tactical Data as, "Information that requires protection from disclosure and modification for a limited duration as determined by the originator or information owner." In addition to protecting Tactical Data, organizations that register their solution using this Appendix must be deployed at the Tactical Edge. The CP follows CNSSI 4009, which defines the Tactical Edge as, "The platforms, sites, and personnel (U.S. military, allied, coalition partners, first responders) operating at lethal risk in a battle space or crisis environment characterized by 1) a dependence on information systems and connectivity for survival and mission success, 2) high threats to the operational readiness of both information systems and connectivity, and 3) users are fully engaged, highly stressed, and dependent on the availability, integrity, and transparency of their information systems."

If an organization's planned solution meets the three criteria above then their solution may be registered using the requirement accommodations in this Appendix. The Campus WLAN CP Registration form must explicitly state that the solution is being used in Tactical Environments and provide justification on how the above criteria are met. In general, customers registering with this Appendix will be deployed in support of Battalion and below (or equivalent) unit structure. Typically, these Tactical Environments are located in austere environments where communication infrastructure is generally limited.

Table 36 defines the Tactical Implementation Overlay Requirements and may be used by customers meeting the criteria above when they configure, test, register, and operate their Campus WLAN Solution. All other requirements stand as written in the body of the CP. Any questions on the use of this Appendix should be directed to wi-fi@nsa.gov and csfc@nsa.gov.

Table 36. Tactical Implementation Overlay Requirements

Req #	Requirement Description	Threshold/ Objective	Alternative
WLAN-PS-11	The WLAN Access System, Gray Firewall, Inner VPN Gateway and Inner Firewall must use physically separate components, such that no component is used for more than one function.	O	WLAN-TO-1
WLAN-TO-1	The WLAN Access System must be physically separate from the Inner Encryption Components.	T	WLAN-PS-11
WLAN-EU-7	Rekeying of an EUD's certificates and associated private keys must be done through re-provisioning prior to expiration of keys.	O	
WLAN-EU-12	Red Network services must not transmit any classified data to EUDs until user authentication succeeds.	O	

Req #	Requirement Description	Threshold/ Objective	Alternative
WLAN-EU-33	USB mass storage mode must be disabled on the EUDs.	O	
WLAN-GD-21	The implementing organization must develop a continuity of operations plan for auditing capability, which includes a mechanism or method for determining when the audit log is reaching its maximum storage capacity.	O	
WLAN-GD-22	The implementing organization must develop a continuity of operations plan for auditing capability, which includes a mechanism or method for off-loading audit log data for long- term storage.	O	
WLAN-GD-23	The implementing organization must develop a continuity of operations plan for auditing capability, which includes a mechanism or method for responding to an overflow of audit log data within a product.	O	
WLAN-GD-24	The implementing organization must develop a continuity of operations plan for auditing capability which includes a mechanism or method for ensuring that the audit log can be maintained during power events.	O	
WLAN-WIDS-0	Meet all requirements defined in the *CSfC Wireless Intrusion Detection System/Wireless Intrusion Prevention System (WIDS/WIPS) Requirements Annex* that apply to the WLAN CP for government private wireless.	O	
WLAN-CM-0	Meet all requirements defined in the CSfC *Continuous Monitoring Annex* that apply to the WLAN CP.	O	WLAN-TO-2
WLAN-TO-2	Meet all requirements defined in the CSfC *Continuous Monitoring Annex* in Appendix D, Tactical Solution Continuous Monitoring Implementations, that apply to the WLAN CP.	T=O	WLAN-CM-0

Table 37. EUD Type Summarization

EUD Configuration	Description	MDF EUD Components	Composed EUD Components	Benefit
Base EUD	An EUD built to function within the constraints of a typical OS or MDF platform	MDF EUD	Operating System EUD Hardware Platform WLAN Client	Minimum Standard for EUDs within CSfC
Software Separated EUD: EUD with Containerization	An EUD built around a standard OS with a containerization engine running to abstract out critical function into separate namespaces	N/A	Operating System EUD Hardware Platform	Offers more usability but no difference in security than base EUD
Software Separated EUD: EUD with Virtualization	An EUD built around a Hypervisor without the hardware abstraction; separates critical functions into separate virtual	N/A	Operating System EUD Hardware Platform WLAN Client	Offers more usability and marginal increase to security
Software Separated EUD: Separation Kernel	An EUD built around a separation kernel and relies on the kernel to segment out critical function	N/A	Operating System EUD Hardware Platform WLAN Client	Offers lower-level isolation giving it increased levels of security
Virtualized EUD: Type 1 Hypervisor with Hardware Abstraction	An EUD built around a Type 1 Hypervisor with hardware abstraction capabilities to separate the critical functions into separate virtual	Virtualization Client MDF EUD	Virtualization Client EUD Hardware Platform WLAN Client	Offers more usability and increases the security of an WLAN EUD with abstraction of the Wi-Fi driver and hardware
Hardware Separated EUD	An EUD with critical functions such as transport, encryption and Red Compute into separate dedicated hardware components	MDF PP Dedicated Outer WLAN	GPOS PP GPCP PP Dedicated Outer WLAN	High risk functions are physically separated into separate hardware such as the Dedicated Outer WLAN use case