National Security Agency/
Central Security Service

CYBERSECURITY SOLUTIONS

WIRELESS LOCAL AREA NETWORK CAPABILITY PACKAGE V2.2

This Commercial Solutions for Classified (CSfC) Capability Package (CP) describes how to protect classified data (including Voice and Video) transiting Government Private Wi-Fi networks.

Version 2.2
26 June 2018

Campus WLAN Capability Package

CHANGE HISTORY

Title	Version	Date	Change Summary
Commercial Solutions for Classified (CSfC) Campus IEEE 802.11 Wireless Local Area Network (WLAN) Capability Package	0.9	December 14, 2012	• Initial release of CSfC Campus IEEE 802.11 Wireless Local Area Network (WLAN) guidance.
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.
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 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 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	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 CP's. • 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 9 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.
Commercial Solutions for Classified (CSfC) Campus Wireless Local Area Network (WLAN) Capability Package	2.2	26 June 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.'

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

Campus WLAN Capability Package

1 INTRODUCTION

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

IAC is delivering a generic CSfC Campus Wireless Local Area Network (WLAN) CP to meet the demand for commercial End User Devices (EUD) (i.e., 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. In WLAN CP Version 2.2, the Key Management Requirements have been relocated from the CP to a separate Key Management Annex.

2 PURPOSE AND USE

This CP provides reference architecture and corresponding configuration information that allows customers to select COTS products from the CSfC Components List 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. Throughout this document, requirements imposed on the Campus WLAN solution to ensure proper implementation are identified by a label consisting of the prefix "WLAN," a two-letter category, and a sequence number (e.g., WLAN-KM-11). To successfully implement a solution based on this CP all Threshold requirements, or the corresponding Objective requirements, must be implemented as described in Sections 9.1.

Customers who want to use this CP must register their solution with NSA. Additional information about the CSfC process is available on the CSfC web page (http://www.nsa.gov/resources/everyone/csfc/).

The Campus WLAN CP Version 2.2, approved by the Deputy National Manager (D/NM) for National Security Systems, is reviewed twice a year to ensure that the defined capabilities and other instructions still provide the security services and robustness required to account for technology development, new security issues, and new use cases. Solutions designed according to this CP must be registered with NSA/IAC. Once registered, a signed IAC Approval Letter will be sent validating that the Campus WLAN solution is registered as a CSfC solution validated to meet the requirements of the latest Campus 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 Program Management Office (PMO) team early in the process to ensure the solutions are properly scoped, vetted, and that the customers have an understanding of risks and available mitigations.

Please provide comments on usability, applicability, and/or shortcomings to your NSA/IAC Client Advocate and the Campus WLAN CP maintenance team at Wi-Fi@nsa.gov.

CNSS Policy No. 15, *National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems (NSS)*, identifies additional public algorithms to protect information within NSS. Specifically, the following algorithms will be required to protect all NSS up to Top Secret:

- AES 256 (confidentiality) – *Note that AES 256 is an objective requirement for WPA2 Enterprise this CP*.
- RSA 3072 or ECDSA P-384 (digital signature and authentication)
- RSA 3072, DH 3072 or ECDH P-384 (key exchange)
- SHA-384 (hashing and integrity)

Vendors are strongly encouraged to meet the objective algorithm requirements for Wi-Fi Protected Access II (WPA2) and Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) as soon as possible to comply with CNSS Policy No. 15.

Campus WLAN CP solutions must comply with Committee on National Security System (CNSS) policies and instructions. Any conflicts identified between this CP and NSS or local policy should be provided to the Campus WLAN CP Maintenance team.

3   LEGAL DISCLAIMER

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

The Campus WLAN solution uses two layers of cryptography, Internet Protocol Security (IPsec) using AES 256 and WPA2 using AES 128[1], to protect the confidentiality and integrity of the data as it transits the untrusted network. The two layers protecting a data flow are generated by the Virtual Private Network (VPN) Client and WLAN Client running on an EUD.   Figure 1 depicts at a high level the Campus WLAN solution within the context of the basic segments of the Campus WLAN architecture. Implementing a WLAN solution that uses two layers of IPsec encryption, a customer has the option of complying and registering with the Mobile Access CP version 2.0 instead of this CP.
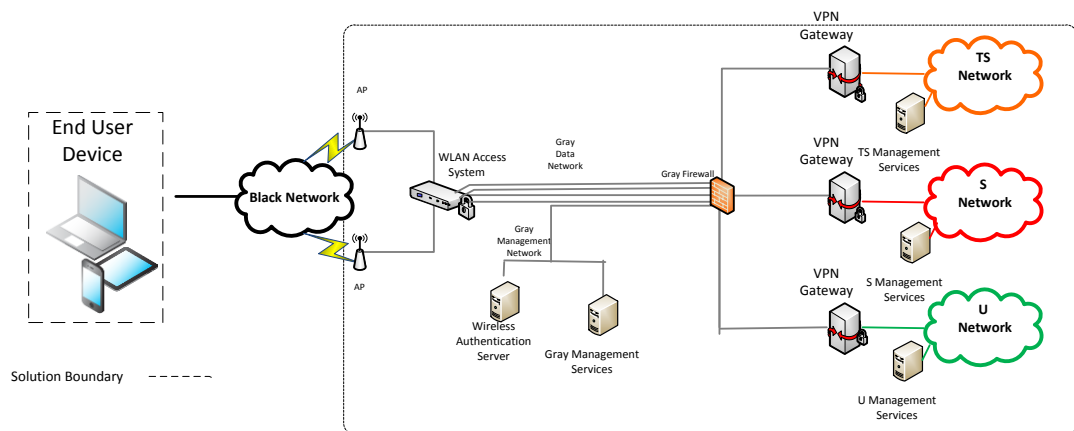
Figure 1. Overview of Campus WLAN CP

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 to urge them to sign a Memorandum of Agreement (MOA) with NSA and start the National Information Assurance Partnership (NIAP) evaluation process, which will enable 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

---

[1] This is a threshold requirement.

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.

While CSfC encourages industry innovation, trustworthiness of the components is paramount. Customers and their Integrators are advised that modifying a NIAP-evaluated component in a CSfC solution may invalidate its certification and trigger a revalidation process. To avoid delays, customers or Integrators who feel it is necessary to modify a component should engage the component vendor and consult NIAP through their Assurance Continuity Process (see http://www.niap-ccevs.org/Documents_and_Guidance/ccevs/scheme-pub-6.pdf) to determine whether such a modification will affect the component's certification. In case of a modification to a component, NSA's CSfC Program Management Office requires a statement from NIAP that the modification does not alter the certification, or the security, of the component. Modifications which trigger the revalidation process include, but are not limited to the following: modifying the original equipment manufacturers' code (to include digitally signing the code) or not leveraging the baseline NIAP-evaluated configuration.

4.1 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.

4.1.1 RED NETWORK

The term Red Network refers to a network logically located behind any Inner VPN Gateway with the additional protection of an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) as illustrated in Figure 3 and Figure 4. Red data consists of unencrypted classified data while Gray data consists of singly encrypted classified data. The Red Network is logically located behind an Inner VPN Gateway. The networks connected to End User Devices through the Campus WLAN solution are Red Networks. Red Networks are under the control of the solution owner or a trusted third party. The Red Network may only communicate with EUDs through the Campus WLAN solution if the EUDs operate at the same security level.

4.1.2 GRAY NETWORK

A Gray network contains classified data that has been singly encrypted. The network between an Inner VPN Gateway and the WLAN Access System is a Gray network. The Gray network is physically and logically under the control of the solution owner or a trusted third party. A Campus WLAN solution compliant with this CP physically treats the Gray network as a classified network even though all classified data is singly encrypted. If a solution owner's classification authority determines that the data on a Gray network is classified, perhaps by determining the Internet Protocol (IP) addresses used on the

Gray network interfaces are classified at some level, then the Campus WLAN solution described in this CP cannot be implemented, as it is not designed to ensure that such information will be afforded two layers of protection. Gray networks are either physically or cryptographically divided into two sub-networks, as follows:

- Gray Management network – The part of a Gray network that contains the management functions to run components supporting the Outer layer of WPA2, including the Outer (WPA2) tunnel Certificate Authority (CA) and the Gray admin and audit server functions. Note- the Inner and Outer CAs can both reside within the Red Network.

- Gray Data network – The part of a Gray network that carries data between Inner VPN Gateway and the WLAN Access System.

4.1.3 BLACK NETWORK

A Black network contains classified data that has been encrypted twice. The wireless network between the End User Device and the WLAN Access System in which data is protected with two layers of encryption (the IPsec and the WPA2 layers) is a Black network. The WPA2 layer can either terminate on the Access Point(s) (AP) or Wireless controller, depending on which vendor product is chosen from the CSfC Components List. For WPA2 tunnels terminating at the AP, encryption standards such as IPsec, Secure Shellv2 (SSHv2), TLS, or TLS/HTTPS must be used to encrypt data between the AP and the wireless controller. Black networks are not necessarily (and often will not be) under the control of the solution Owner or can be interfered with by external third party actors.

4.2 DATA, MANAGEMENT, AND CONTROL PLANE TRAFFIC

Data plane traffic is classified information, encrypted or not, 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 WPA 2 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, Security Information and Event Manager (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 11.1) require that time synchronization be performed, but do not require the use of any particular time synchronization protocol or technique. Notable exceptions are for IPsec session establishment and for certain certificate status distribution scenarios where, given their impact on the security of the solution, this CP provides detailed requirements. 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 are generally required to be separated from one another using physical or cryptographic separation. Use of a Virtual Local Area Network (VLAN) alone is not sufficient to separate data plane and management plane traffic. As a result, a solution may, for example, have a Gray Data network and a Gray Management network which are separate from one another, where the components on the Gray Management network are used to manage the components on the Gray Data network.

4.3 HIGH-LEVEL DESIGN
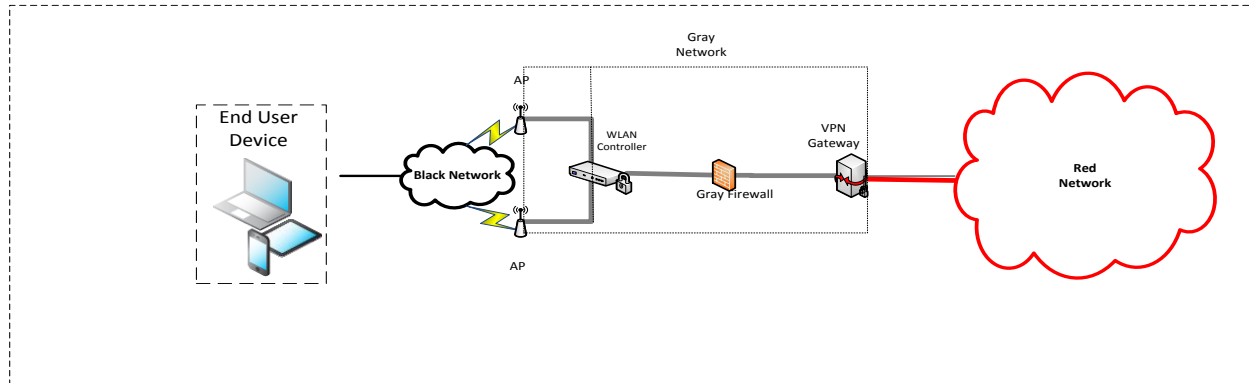
Figure 2. Campus WLAN Single Classification Implementation

The Campus WLAN CSfC solution is adaptable to support multiple capabilities, depending on the needs of the customer implementing the solution. If a customer does not have a need for supporting multiple classified networks, then those elements need not be included as part of the implementation as seen in Figure 2. In Figure 2 the Black/Gray boundary 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, as explained in Section 0.

4.3.1 MULTIPLE SECURITY LEVELS

A single implementation of the Campus WLAN solution may support Red Networks and EUDs of different security levels. The Campus WLAN solution provides secure connectivity between the Red Networks and EUDs within each security level while preventing Red Networks and EUDs of differing security levels from communicating with one another. This enables a customer to use the same physical wireless infrastructure to carry traffic from multiple networks.

4.3.1.1 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.
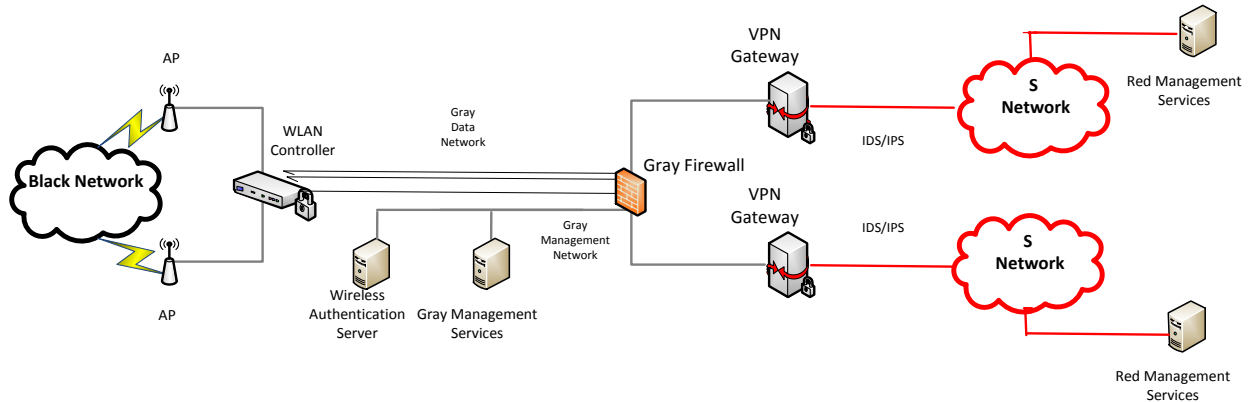
Figure 3. Campus WLAN Solution for Two Networks of the Same Classification Level

4.3.1.2   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 4.3.1.1, is still present. However, because the consequences of an unintended data flow between different classification levels are more severe than of one with a single classification level, an additional mechanism is necessary to further guard against such a flow from occurring.
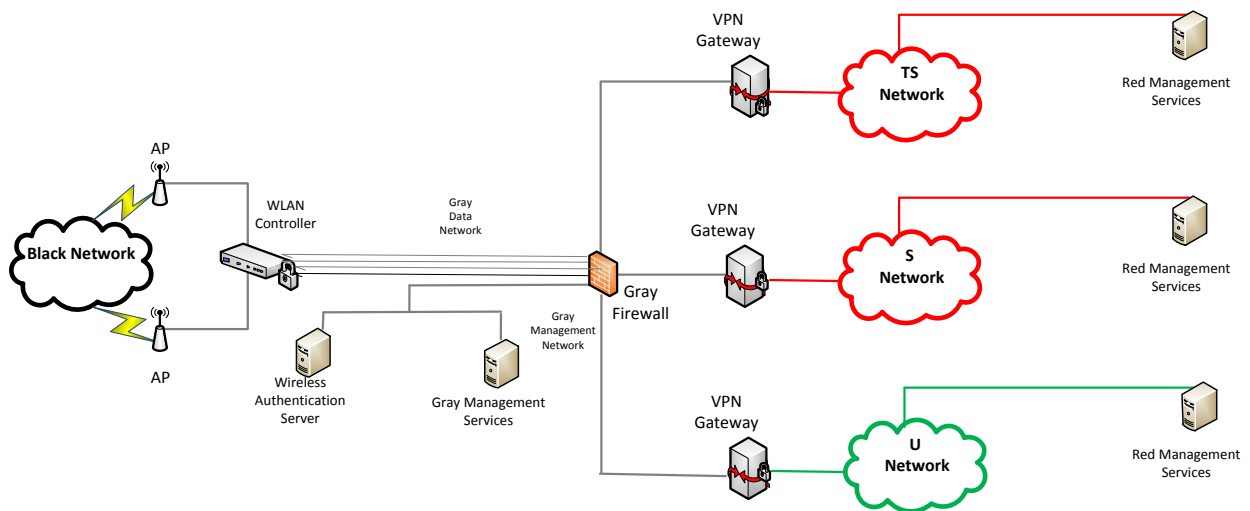
Figure 4. Campus WLAN Solution for Networks Operating at Different Classification Levels

This CP requires packet filtering within Gray networks as the 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, only allowing a packet through if the source and destination components are intended to communicate with one another and dropping the packet if they are not.

When multiple classification levels are being used, it is critical to enforce proper IP address assignment and firewall rule sets. The IP address assigned must be unique to that classification level such that the end user device is only able to send and receive traffic to 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 a whitelist or X.509 Certificate.

5 SOLUTION COMPONENTS

5.1 END USER DEVICE

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

Figure 5 shows the software architecture of a typical 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 WPA2 driver respectively.
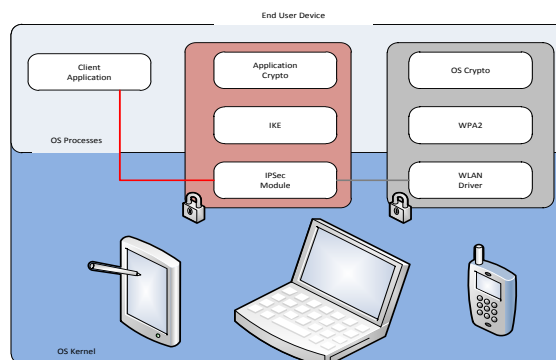
Figure 5. Campus WLAN End User Device Architecture

5.1.1 END USER DEVICE

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 EUD is to be used exclusively within physically secure environments, such as facilities and tactical environments with physical controls considered appropriate by the AO.

5.1.2 EUD DEPLOYMENT 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 (DAR CP) for the protection of information classified at the level of the associated Red Network to which the EUD is connected. Specification of such a DAR solution is outside the scope of this CP, but can be found in the Data at Rest CP. The NSA requires implementing organizations to define the circumstances in which an EUD that is part of the organization's solution 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 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 not to 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 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. This option is not permitted if any of the private keys or certificates stored on the EUD are considered classified by the AO. 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.

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 a nation state 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 communicates with through the Campus WLAN solution, since classified data may be present in volatile memory and/or displayed on screen. 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 an user access to an EUD after he or she agrees to the user agreement and receives training on how to use and protect their EUD.

5.2 WLAN CLIENT

The WLAN Client (also known as WPA2 supplicant) is a software application running on the End User Device that provides management and control of the wireless connection. 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 11 for the WLAN Client. The WLAN Client automatically establishes the WPA2 tunnel between the End User Device 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.

5.3 VPN CLIENT

The VPN Client is a software application running on the End User Device. The products chosen to implement the VPN services must provide cryptographic and functional services that meet or exceed the requirements listed in Section 11 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.

5.4 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.

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 utilize "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 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 WPA2 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, SSH, TLS, or TLS/HTTPS. If WPA2 terminates on the WLAN Controller, then the WPA2 encryption is used to protect the connection between the APs and the WLAN Controller.

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 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. The WLAN Access System should operate on its own separate hardware and/or virtual device(s), depending on the vendor implementation, as mentioned above. 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 11.6.

5.5 WLAN 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 a whitelist of devices and the enclave for which each device is provisioned. This whitelist 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 utilize information in the certificate of each EUD to make the access decision. Specifically, customers can utilize fields in the Distinguished Name of the Certificate (e.g., Organizational Unit field) or utilize 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.

5.6   GRAY FIREWALL

When supporting multiple enclaves, the Authentication Server will utilize the whitelist or certificate as part of the authentication of EUDs. 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 utilizes 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 Access Control List (ACL) rules.

A Campus WLAN solution that supports networks operating at different classification levels must include a Gray Firewall, as described in Section 4.3.1.2. The primary purpose of a Gray Firewall is for filtering traffic to only allow the proper traffic to flow to and from the VPN Gateway and WLAN Controller. The Gray Firewall must be selected from the CSfC Components List and must be physically separate from the WLAN Access System and the VPN Gateways.

5.7   ADMINISTRATION WORKSTATIONS

The WLAN Access System, WLAN Authentication Server, and the WLAN Client must have an administration workstation on the Gray Management network that allows for maintaining, monitoring, and controlling all security functionality for those devices. The administration devices for the VPN are located on the Red Network. These administration devices 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.

5.8 CERTIFICATE AUTHORITY

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

6 CAMPUS WLAN CONFIGURATION AND MANAGEMENT

6.1 EUD PROVISIONING

Initial provisioning of campus End User Devices 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 a wireless and wired connection capabilities to the End User Device 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 WPA2 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—note that a specific sequence is not implied:

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

- **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 End User Device. Disconnect the device from the Gray Network, connect to the Red Network, request certificates from the Inner CA, and load received material into the End User Device. 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 End User Device. There will also be differences based on whether the End User Device 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 End User Device 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.

6.2   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 End User Devices in Section 11.2 can be accomplished through a variety of mechanisms. First, the EUDs can be configured utilizing a Mobile Device Management (MDM) selected from the CSfC Components List. Alternatively, the EUD can be configured utilizing 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 End User Devices using an existing Enterprise Policy enforcement mechanism. Finally, customers can choose to utilize a hybrid approach with more than one of the above options.

7   CONTINUOUS MONITORING

The Campus WLAN CP allows customers to utilize 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 which occur on their solution. This continuous monitoring also enables the detection of any configuration errors in solution infrastructure components. At a minimum, this CP requires an Auditor to review alerts, events, and logs on a weekly basis. Operational and Strategic implementations of the Campus WLAN CP should review alerts, events, and logs on a more frequent basis. Customers may leverage Operation Centers to perform 24 hour, 7 day a week monitoring.
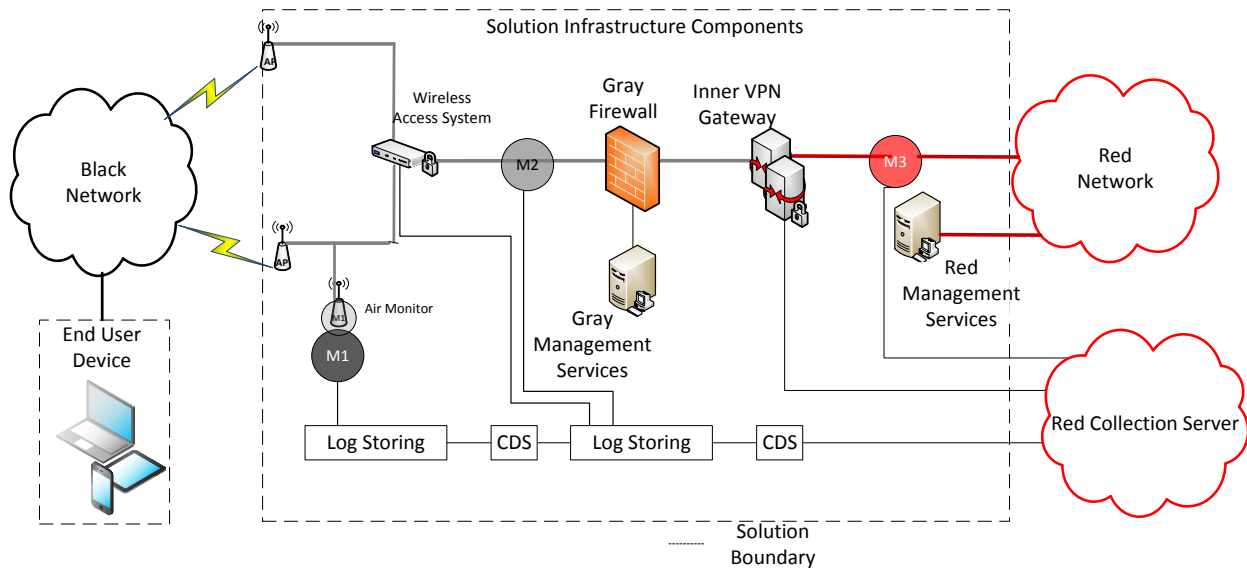
Figure 6. Campus WLAN Continuous Monitoring Points

Figure 6 shows the locations where continuous monitoring is recommended. Dedicated black/gray/red continuous monitoring components can be used but the figure illustrates how data could be moved to one place to assist in correlation.

Monitoring Point 1 - Wireless Intrusion Detection/Prevention System (WIDS/WIPS) Sensors are located not only near access points, but around the perimeter of the wireless network.

Monitoring Point 2 – Intrusion Detection System or Intrusion Prevention System is located between the Wireless Access System and the Gray Firewall.

Monitoring Point 3 – Intrusion Detection System or Intrusion Prevention System is located between the VPN Gateway and the Red Network.

7.1 INTRUSION DETECTION AND PREVENTION SYSTEM (IDS/IPS)

The Intrusion Detection and Prevention System is responsible for monitoring the network traffic flow to and from the Red Networks. The IDS/IPS can be either an IDS or an IPS; however, it is preferable to use an IPS to elicit real-time responses. The term IDS/IPS used in this CP will refer to both IDP and IPS technologies. The IDS/IPS will be configured to terminate the network connection or user session that is being used for an attack. The IPS must be configured to block all access to the targeted host, service, application, or any other resource from the source of an attack. The IDS/IPS must synchronize its time using a NTP to ensure log entries have accurate timestamps. An alert must be triggered on any connection attempt to the NTP server other than by the Wireless LAN Access system or the Gray Management network. Any traffic to the Authentication Server in the Gray Management network on ports other than the Radius Accounting and Authentication ports (UDP 1812 and 1813) must trigger an

alert. Traffic sent to DNS ports (TCP/UDP 53) other than on the DNS server must trigger an alert. DNS traffic must be inspected for volume of DNS traffic per IP address, volume of DNS traffic per domain, and number of hostname queries. The IDS/IPS must be deployed on the Red Network to monitor tunneled traffic being decrypted by the VPN Gateway. Traffic originating from a Red Network client going to a port other than ISAKMP/IKE (UDP 500) or IPsec NAT traversal (UDP 4500) on the inner VPN gateway must trigger an alert. The IDS/IPS must be deployed on the Gray Network to monitor tunneled traffic being decrypted by the Wireless LAN Access system. An alert must be generated if the Wireless LAN Access system receives traffic on any ports other than the SSH port (TCP 22) or the HTTPS port (TCP 443) from the Gray Management network.

Infrastructure components (servers and workstations) should be configured with Host-based IDS (HIDS) software in accordance with local policy.

7.2   WIRELESS INTRUSION DETECTION SYSTEM

A Wireless Intrusion Detection System consists of a group of sensors (preferably some dedi cated) and a central controller working together to provide 24/7 monitoring of the wireless spectrum to detect unauthorized or malicious WLAN activity. The system can either be stand-alone or integrated into the WLAN Access System. For the stand-alone case, ideally, information between the sensors and the controller will pass over a separate network dedicated to the WIDS, but an acceptable option is to connect the sensors over a virtual LAN established over the same wired network as used by the Wireless APs. For an integrated WIDS, whether the sensors can be placed on the Wireless network or must be placed on the Gray Network depends on the vendor's implementation.

7.3   SECURITY INFORMATION AND EVENT MANAGEMENT

The SIEM collects and analyzes log data from the WLAN Access System, Gray firewall, and IDS/IPS. 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. At a minimum, an auditor reviews the SIEM on a weekly basis. The SIEM is configured to provide alerts for specific events including if the WLAN Access System, Gray firewall, and IDS/IPS receive and drop any unexpected traffic, which could indicate a compromise of the WLAN Access System.

8   KEY MANAGEMENT

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

9 REQUIREMENTS OVERVIEW

The following five sections (Section 10 through Section 14, and the 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. Key Management Requirements have been relocated to a separate Key Management Requirements Annex.

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

9.2 REQUIREMENTS DESIGNATORS

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

Table 1 lists the digraphs used to group together related requirements and identifies the sections in

which those requirement groups can be found.

Table 1. Requirement Digraph

Digraph	Description	Section	Table
PS	Product Selection Requirements	Section 10	Table 2
SR	Overall Solution Requirements	Section 11.1	Table 3
EU	End User Device Requirements	Section 11.2	Table 4
WC	WLAN Client Configuration Requirements	Section 11.3	Table 5
WL	Wireless Link Requirements	Section 11.3	Table 6
CR	Configuration Requirements for VPN Components	Section 11.4	Table 9
WS	WLAN Access System Configuration Requirements	Section 11.5	Table 10
IA	Wireless Infrastructure Authentication Requirements	Section 11.5	Table 11
AA	Wireless Authentication and Authorization Requirements	Section 11.5	Table 12
WA	Wireless Authentication Server to WLAN Client Requirements	Section 11.5	Table 13
PF	Port Filtering Requirements for Solution Components	Section 11.6	Table 14
PR	End User Device Provisioning Requirements	Section 11.7	Table 15
WI	Wireless Intrusion Detection Configuration Requirements	Section 11.8	Table 16
CM	Configuration Change Detection Requirements	Section 11.9	Table 17
DM	Device Management Requirements	Section 11.10	Table 18
MR	Continuous Monitoring Requirements	Section 11.11	Table 19
AU	Auditing Requirements	Section 11.12	Table 20
FW	Gray Firewall Requirements	Section 11.14	Table 21
GD	Requirements for the Use and Handling of Solutions	Section 12.1	Table 22
RP	Incident Reporting Requirements	Section 12.2	Table 23
GD	Role-Based Personnel Requirements	Section 13	Table 24
TR	Test Requirements	Section 14.1	Table 25
KM	Key Management Requirements (See Key Management Requirements Annex)		

10 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 2. 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. All validated Mobile Platform components include validated WLAN Client implementations.	T=O	
WLAN-PS-4	Products used for Mobile Platform EUDs must be chosen from the list of Mobile Platforms on the CSfC Components List.	T=O	
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	The products used for the Inner and Outer CAs must either be chosen from the list of CAs on the CSfC Components List or the CAs must be pre-existing Enterprise CAs of the applicable network.	T=O	
WLAN-PS-7	IPS must be chosen from the list of IPS on the CSfC Components List.	O	Optional
WLAN-PS-8	Products used for the Gray 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.	O	Optional
WLAN-PS-10	The Inner VPN Gateway and the WLAN Access System must either:	O	Optional

Req #	Requirement Description	Threshold / Objective	Alternative
	• 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.		
WLAN-PS-11	The WLAN Access System, Gray Firewall, Inner VPN Gateway must use physically separate components, such that no component is used for more than one function.	T=O	
WLAN-PS-12	The Outer and Inner CAs 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. • or utilize an Enterprise PKI approved by the AO.	O	
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,	T=O	Optional

Req #	Requirement Description	Threshold / Objective	Alternative
	• be different libraries from the same manufacturer, where NSA has determined that the libraries meet the CSfC criteria for implementation independence.		
WLAN-PS-15	Each component that is selected out of 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	Components must be configured to use the NIAP-certified evaluated configuration.	T=O	

11 CONFIGURATION REQUIREMENTS

Once the products for the solution are selected, the next step is setting up the components and configuring them in a secure manner. This section consists of generic guidance for 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 consist 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 IAC/CSfC website (http://www.nsa.gov/resources/everyone/csfc/components-list/). 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.)

11.1 OVERALL SOLUTION REQUIREMENTS

Table 3. 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 the VPN Gateway 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.[2]	T=O	

11.2 END USER DEVICES REQUIREMENTS

Table 4. End User Device (EU) Requirements

---

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

Req #	Requirement Description	Threshold / Objective	Alternative
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	
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	

Req #	Requirement Description	Threshold / Objective	Alternative
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 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.	T=O	
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	The EUD must have all cellular access disabled.	T=O	
WLAN-EU-20	The EUD must have all network and wireless interfaces disabled except for 802.11.	T=O	
WLAN-EU-21	The EUD must have all cellular services disabled.	O	Optional
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 authentication must be a minimum of 6 alpha-numeric case sensitive characters.	T=O	
WLAN-EU-24	The native platform DAR protection must be enabled[3].	T=O	
WLAN-EU-25	Withdrawn		
WLAN-EU-26	Withdrawn		
WLAN-EU-27	The EUD maximum password lifetime must be less than 181 days.	T=O	

---

[3] If the WLAN Solution is implemented in conjunction with a NSA approved DAR Solution, then all applicable DAR CP requirements must also be implemented.

Req #	Requirement Description	Threshold / Objective	Alternative
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-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.	O	Optional
WLAN-EU-33	USB mass storage mode must be disabled on the EUDs.	O	Optional
WLAN-EU-34	USB data transfer must be disabled on the EUDs.	O	Optional
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 whitelisted 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 whitelisted SSIDs to the user.	T=O	
WLAN-EU-39	The EUD must only permit the execution of applications on a whitelist.	O	Optional
WLAN-EU-40	The management and control of the EUD connection to the WLAN System must be isolated from other EUD functions.	O	Optional

11.3 CONFIGURATION REQUIREMENTS FOR THE WLAN CLIENT

Table 5. 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.	T=O	
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	

Req #	Requirement Description	Threshold / Objective	Alternative
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.	T=O	
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 whitelists 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 accessible via the Campus WLAN.	T=O	

Table 6. 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 selected from nine that are approved to protect the highest classification level of the Red Network data.	T=O	
WLAN-WL-2	The WLAN Client and the WLAN Access System must operate in WPA2-Enterprise mode.	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 802.11-2012.	T=O	
WLAN-WL-4	If WPA2 terminates on APs then all data between the Access Point(s) and Wireless controller must be encrypted using IPsec, SSHv2, TLS, or TLS/HTTPS.	T=O	

Table 7. IPSec Encryption (Approved Algorithms for Classified)

Security Service	Algorithm Suite	Specifications
Confidentiality (Encryption)	AES-256	FIPS PUB 197 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460
Authentication (Digital Signature) (Threshold – Unclassified Only)	RSA 3072	FIPS PUB 186-4
Authentication (Digital Signature) (Objective) (Threshold – All Classified NSS)	RSA 3072 or, ECDSA over the curve P-384 with SHA-384	FIPS PUB 186-4 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 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460 NIST SP 800-56A

Security Service	Algorithm Suite	Specifications
Integrity (Hashing)	SHA-384	FIPS PUB 180-4 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460
Can protect	Up to Top Secret	

Table 8. WPA2 Encryption and EAP-TLS (Approved Algorithms)

Security Service	Algorithm Suite	Specifications
Confidentiality (Encryption)	AES-128-CCMP (Threshold) AES-256-CCMP (Objective)	FIPS PUB 197
EAP-TLS Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (Threshold) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (Objective)	IETF RFC 5216 IETF RFC 5246

11.4 CONFIGURATION REQUIREMENTS FOR VPN COMPONENTS AND VPN CLIENT

Table 9. Configuration Requirements (CR) for VPN Components

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 7 that are approved to protect the highest classification level of the Red Network data.	T=O	
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

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-CR-4	All IPsec connections must use IETF standards compliant with IKE implementations (RFC 5996 or RFC 2409).	T=O	
WLAN-CR-5	All Access Systems and VPN Gateway components must use Cipher Block Chaining for IKE encryption.	T=O	
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	
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	

11.5 CONFIGURATION REQUIREMENTS FOR THE WLAN ACCESS SYSTEM

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 10. 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	
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 utilize unique physical internal interfaces for each enclave of the solution (e.g., VLAN Trunking of multiple enclaves is not permitted).	T=O	

Table 11. 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
WLAN-IA-2	Communications between the WLAN Access System and the WLAN Authentication Server must be established with either an IPsec tunnel (using either IKEv1 or IKEv2) or TLS/RADsec connection.	O	WLAN-IA-1

Req #	Requirement Description	Threshold / Objective	Alternative
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 6 Table 6.	T=O	
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	
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	The IKE exchange between the WLAN Access System and the WLAN Authentication Server must use algorithms selected from Table 6 Table 6.	T=O	

Table 12. 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 WPA2 Enterprise from the Threshold Section of Table 7.	T	WLAN-AA-3
WLAN-AA-3	The WLAN Client and the WLAN Authentication Server must use the AES key size and mode for WPA2 Enterprise from the Objective Section of Table 7.	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 7.	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 7.	O	WLAN-AA-4

Table 13. Wireless Authentication Server (WA) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-WA-1	The WLAN Authentication Server 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	

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

11.6 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 14. Port Filtering (PF) Requirements for Solution Components

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	

Req #	Requirement Description	Threshold / Objective	Alternative
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 a 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., SSH, 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	

11.7 END USER DEVICE PROVISIONING REQUIREMENTS

Table 15. EUD Provisioning Requirements (PR)

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-PR-1	A Provisioning WLAN using WPA2-PSK authentication and encryption must be established on the Red Network to support wireless provisioning of EUDs.	T	
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-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-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	
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	

11.8 **CONFIGURATION REQUIREMENTS FOR WIRELESS INTRUSION DETECTION SYSTEM (WIDS)**

Table 16. Wireless IDS (WI) Configuration Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-WI-1	The WIDS must use a whitelist of all authorized wireless network devices (i.e., Access points and EUDs) and allow for administrator modifications.	T=O	
WLAN-WI-2	The WIDS must detect access points which are not on the whitelist, but are within the coverage area of the WIDS sensors.	T=O	
WLAN-WI-3	The WIDS must detect EUDs which are not on the whitelist, but are within the coverage area of the WIDS sensors.	T=O	
WLAN-WI-4	The WIDS must allow for administrator-defined rogue AP detection classification rules.	T=O	
WLAN-WI-5	The WIDS must detect if a rogue AP is connected via wire to the network.	O	Optional
WLAN-WI-6	The WIDS must distinguish between the mere presence of unauthorized wireless hardware within the coverage area of the WIDS sensors and an attempt to use that hardware to gain access to the wireless network.	T=O	
WLAN-WI-7	All communication between WIDS components must be done via a secure connection (using SSHv2, IPSec, TLS, or TLS/HTTPS).	O	Optional
WLAN-WI-8	The WIDS must geographically locate all wireless hardware operating in the coverage area of the WIDS sensors.	O	Optional
WLAN-WI-9	The WIDS must be configured to monitor all 802.11 frame types and subtypes between unauthorized EUDs and authorized APs.	T=O	
WLAN-WI-10	The WIDS must be configured to monitor all 802.11 frame types and subtypes between unauthorized APs and authorized EUDs.	T=O	
WLAN-WI-11	The WIDS must be configured to monitor all 802.11 frame types and subtypes between authorized APs and authorized EUDs.	T=O	
WLAN-WI-12	The WIDS must allow for capturing the raw frames that triggered an alert as well as options on how long to continue capturing the frames.	O	Optional

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-WI-13	The WIDS must monitor and analyze traffic from all 802.11 channels within the 2.4Ghz and 4.9/5.0Ghz bands including those outside regulatory domain.	T=O	
WLAN-WI-14	The WIDS must monitor and analyze traffic from all 802.11 channels within the 3.6Ghz and 60Ghz bands.	O	Optional
WLAN-WI-15	The WIDS must detect the use of unauthorized wireless channels by whitelisted devices.	T=O	
WLAN-WI-16	The WIDS must determine which SSIDs are permitted on the network based on whitelisted APs or have the ability to be configured with a list of permitted SSIDs.	T=O	
WLAN-WI-17	The WIDS must detect whitelisted APs using SSIDs not permitted on the network (including hidden SSID).	T=O	
WLAN-WI-18	The WIDS must detect and log unauthorized APs broadcasting the same SSID as a whitelisted AP.	T=O	
WLAN-WI-19	The WIDS must detect whitelisted EUDs associating to SSIDs not permitted on the network (including hidden SSID).	T=O	
WLAN-WI-20	The WIDS must be configured to detect whitelisted devices attempting to use unauthorized authentication methods.	T=O	
WLAN-WI-21	The WIDS must detect whitelisted devices attempting to use unauthorized encryption schemes.	T=O	
WLAN-WI-22	The WIDS must be configured to process 802.11 traffic up to the data rate that is supported by the equipment in the wireless network.	T=O	
WLAN-WI-23	The WIDS must log the signal strength of hardware operating in the coverage area of the WIDS sensors.	T=O	
WLAN-WI-24	The WIDS must detect and log when it receives 802.11 frames being sent with a transmit power above maximum transmit power levels according to country regulations.	T=O	
WLAN-WI-25	The WIDS should support user-defined and customizable attack signatures.	T=O	
WLAN-WI-26	The WIDS must detect Radio Frequency (RF)-based Denial-of-Service (DoS) attacks.	T=O	
WLAN-WI-27	The WIDS must perform protocol anomaly analysis to detect violations of WLAN standards such as 802.11 and 802.1X.	T=O	
WLAN-WI-28	The WIDS must detect and log deauthentication flooding.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-WI-29	The WIDS must detect and log disassociation flooding.	T=O	
WLAN-WI-30	The WIDS must use anomaly-based detection, to detect, log, and generate an alert when the network's activity deviates from an established network baseline.	O	Optional
WLAN-WI-31	The WIDS must monitor bandwidth usage.	O	Optional
WLAN-WI-32	The WIDS must monitor number of users/wireless clients.	O	Optional
WLAN-WI-33	The WIDS must monitor times of usage.	T=O	
WLAN-WI-34	The WIDS must track the connection status of each client (authorized or unauthorized) in real time including, but not limited to, whether the client is offline, associated, or authentication is pending.	T=O	
WLAN-WI-35	The WIDS must detect and log illegal state transitions, such as a client device transmitting data frames through an AP to a network device before being associated and authenticated.	T=O	
WLAN-WI-36	The WIDS must detect and log an event where an attacker spoofs the Media Access Control (MAC) address of an authorized client to attempt to connect to the legitimate network.	T=O	
WLAN-WI-37	The WIDS must detect and log an event where two sensors in physically separate (non-overlapping) locations (such as different buildings) receive frames with the same MAC address at the same time.	T=O	
WLAN-WI-38	The WIDS must detect and log an event where a whitelisted EUD's MAC address appears in multiple physically distant locations.	O	Optional
WLAN-WI-39	The WIDS must detect whitelisted EUDs establishing peer-to-peer connections with other whitelisted devices or unauthorized devices.	O	Optional
WLAN-WI-40	The WIDS must detect EUDs bridging two network interfaces (wired and wireless). If the wired interface is connected to the internal network and the wireless interface is connected to a Rogue AP, this can expose traffic from the internal network.	O	Optional
WLAN-WI-41	The WIDS must detect and log the presence of an 802.11 bridge.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-WI-42	The WIDS must detect and log the presence of a single device transmitting beacons looking for a bridge.	T=O	
WLAN-WI-43	The WIDS must detect and log the presence of two or more devices transmitting bridge data frames.	T=O	
WLAN-WI-44	The WIDS must provide the ability to remove or disable all WIDS components' non-secure communications paths used for management and event monitoring including HTTP, SNMPv1, File Transfer Protocol (FTP), and Telnet.	T=O	
WLAN-WI-45	The WIDS must allow for alert notification filtering such as alert notification type, severity levels, and number of alerts to receive.	T=O	
WLAN-WI-46	The WIDS alert notifications must be descriptive to show the significance of alerts.	T=O	
WLAN-WI-47	The WIDS must support the ability to export event logs and reports into industry standard formats such as Comma Separated Values (CSV) and Common Log Format (CLF).	T=O	

11.9 CONFIGURATION CHANGE DETECTION REQUIREMENTS

Table 17. Configuration Change Detection (CM) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-CM-1	A baseline configuration for all components must be maintained by the Security Administrator and be available to the Auditor.	T=O	
WLAN-CM-2	An automated process must ensure that configuration changes are logged.	T=O	
WLAN-CM-3	Log messages generated for configuration changes must include the specific changes made to the configuration.	T=O	
WLAN-CM-4	All solution components must be configured with a monitoring service that detects all changes to configuration.	T=O	

11.10 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 18. 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	
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.	T=O	
WLAN-DM-10	EUDs must generate logs and send to a central SIEM in the Red Network.	O	Optional

Req #	Requirement Description	Threshold / Objective	Alternative
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	The WLAN Access System and solution components within the Gray Network must forward log entries to a SIEM on the Gray Management network (or SIEM in the Red Network if using an AO approved one-way tap) within 10 minutes.	T=O	
WLAN-DM-14	All logs forwarded to a SIEM on the Gray Management network must be encrypted using SSHv2, IPsec, or TLS 1.1 or later.	T	WLAN-DM-15
WLAN-DM-15	All logs forwarded to a SIEM on a Red Management network must be encrypted using SSHv2, IPsec, or TLS 1.1 or later.	O	WLAN-DM-14
WLAN-DM-16	When managing solution components over the Black network, the management traffic must be encrypted with a CNSA Suite algorithm (See Table 8).	T=O	

11.11 CONTINUOUS MONITORING REQUIREMENTS

Table 19. Continuous Monitoring (MR) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-MR-1	Traffic on the Gray and before the Red Networks must be monitored from an IDS.	T	WLAN-MR-2
WLAN-MR-2	Traffic on the Gray and before Red Networks must be monitored from an IPS.	O	WLAN-MR-1
WLAN-MR-3	The WIDS must encrypt and sign all alerts pushed to a remote system administrator.	O	WLAN-MR-4
WLAN-MR-4	System administrators must authenticate all alerts received by the WIDS.	T	WLAN-MR-3
WLAN-MR-5	All event monitoring of the WIDS must be remotely performed from the Gray Management Network through SSHv2, IPsec, or TLS.	T=O	
WLAN-MR-6	The IDS in the solution must be configured to send alerts to the Security Administrator.	T	WLAN-MR-7

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-MR-7	The IPS in the solution must be configured to block malicious traffic flows and alert the Security Administrator.	O	WLAN-MR-6
WLAN-MR-8	The IDS in the solution must be configured with rules that generate alerts upon detection of any unauthorized destination IP addresses.	T	WLAN-MR-9
WLAN-MR-9	The IPS in the solution must be configured with rules that block and generate alerts upon detection of any unauthorized destination IP addresses.	O	WLAN-MR-8
WLAN-MR-10	The IDS in the solution must be configured with rules that generate alerts upon detection of any unauthorized source IP addresses.	T	WLAN-MR-11
WLAN-MR-11	The IPS in the solution must be configured with rules that block and generate alerts upon detection of any unauthorized source IP addresses.	O	WLAN-MR-10
WLAN-MR-12	A Network-based Intrusion Detection System (NIDS) must be deployed on the Gray Management Network to monitor traffic arriving from or leaving to the WLAN Access System.	O	Optional
WLAN-MR-13	The NIDS must report all matches to the attack signatures on the NIDS to both inbound and outbound traffic.	O	Optional
WLAN-MR-14	The NIDS must be regularly updated with attack signatures in accordance with local policy.	O	Optional

11.12 AUDITING REQUIREMENTS

Table 20. Auditing (AU) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-AU-1	VPN Gateways must log establishment of a VPN tunnel.	T=O	
WLAN-AU-2	VPN Gateways must log termination of a VPN tunnel.	T=O	
WLAN-AU-3	VPN Clients must log establishment of a VPN tunnel.	T=O	
WLAN-AU-4	VPN Clients must log termination of a VPN tunnel.	T=O	
WLAN-AU-5	Solution components must log all actions performed on the audit log (off-loading, deletion, etc.).	T=O	
WLAN-AU-6	Solution components must log all actions involving identification and authentication.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-AU-7	Solution components must log attempts to perform an unauthorized action (read, write, execute, delete, etc.) on an object.	T=O	
WLAN-AU-8	Solution components must log all actions performed by a user with super-user or administrator privileges.	T=O	
WLAN-AU-9	Solution components must log escalation of user privileges.	T=O	
WLAN-AU-10	Solution components must log generation, loading, and revocation of certificates.	T=O	
WLAN-AU-11	Solution components must log changes to time.	T=O	
WLAN-AU-12	Each log entry must record the date and time of the event.	T=O	
WLAN-AU-13	Each log entry must include the identifier of the event.	T=O	
WLAN-AU-14	Each log entry must record the type of event.	T=O	
WLAN-AU-15	Each log entry must record the success or failure of the event to include failure code, when available.	T=O	
WLAN-AU-16	Each log entry must record the subject identity.	T=O	
WLAN-AU-17	Each log entry must record the source address for network-based events.	T=O	
WLAN-AU-18	Each log entry must record the user and, for role-based events, role identity, where applicable.	T=O	
WLAN-AU-19	Auditors must detect when two or more simultaneous VPN connections from different IP addresses are established using the same EUD device certificate.	O	Optional
WLAN-AU-20	Upon notification of two or more simultaneous VPN connections from different IP addresses using the same EUD device certificate, the Certificate Authority Administrator must revoke the device certificate and provide an updated CRL to the Security Administrator.	O	Optional
WLAN-AU-21	The Security Administrator must immediately drop the session upon notification of two or more simultaneous VPN connections from different IP addresses using the same EUD device certificate.	O	
WLAN-AU-22	The WIDS must log when sensors fail to communicate.	T=O	
WLAN-AU-23	The EUD must log all successful and unsuccessful logins.	O	Optional
WLAN-AU-24	The EUD must log all successful and unsuccessful logouts.	O	Optional

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-AU-25	The EUD must audit installation and removal of software.	O	Optional
WLAN-AU-26	The EUD must audit attempts to change security-relevant configuration items.	O	Optional
WLAN-AU-27	The EUD must audit changes to security-relevant configuration items.	O	Optional
WLAN-AU-28	The EUD must audit signature verification and certificate validation.	O	Optional
WLAN-AU-29	Auditors must compare and analyze collected network flow data against the established baseline on at least a weekly basis.	T=O	

11.13 KEY MANAGEMENT REQUIREMENTS

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

11.14 GRAY FIREWALL REQUIREMENTS

Table 21. 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

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-FW-5	Gray Network Firewall must only accept management traffic on the physical ports connected to the Gray Management network.	T=O	
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 REQUIREMENTS FOR SOLUTION OPERATION, MAINTENANCE, AND HANDLING

12.1 REQUIREMENTS FOR THE USE AND HANDLING OF SOLUTIONS (GD)

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

Table 22. Requirements for the Use and Handling of Solutions

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	

Req #	Requirement Description	Threshold / Objective	Alternative
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	
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	The AO will ensure that a compliance audit must be conducted every year against the latest version of the WLAN CP as part annual solution re-registration process.	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 6 months or by the next re-registration date (whichever is greater).	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-GD-16	Solution implementation information, which was provided to NSA during solution registration, must be updated annually (in accordance with Section 14.3) 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	
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	

Req #	Requirement Description	Threshold / Objective	Alternative
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	

Additional WLAN-GD requirements can be found in Section 12.

12.2 REQUIREMENTS FOR INCIDENT REPORTING

Table 23 lists requirements for reporting security incidents to NSA to be followed in the event that a solution owner identifies a security incident which 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, Certificate Authority Administrators (CAAs), and Auditors are familiar with maintaining the solution in accordance with this CP. Based on familiarity with the known-good configuration of the solution, personnel responsible for the operations and maintenance of the solution will be better equipped to identify reportable incidents.

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

Table 23 only provides requirements directly related to the incident reporting process. See Section 11.11 for requirements supporting the detection of events that may reveal that a reportable incident has occurred.

Table 23. 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-16 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	

Req #	Requirement Description	Threshold / Objective	Alternative
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	
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	

13 ROLE-BASED PERSONNEL REQUIREMENTS

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

Security Administrator – The Security Administrator must be responsible for maintaining, monitoring, and controlling 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) Ensuring that the latest security-critical software patches and updates (such as Information Assurance Vulnerability Alerts (IAVAs)) are applied to each product.

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

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

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

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

6) Provisioning and maintaining EUDs in accordance with this CP for implementations that include them.

Certificate Authority Administrator (CAA) – The CAA must be responsible for maintaining, monitoring, and controlling all security functions for the CA products. CAA duties include, but are not limited to, the following:

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

2) Maintaining and updating the CRL.

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

Auditor – The Auditor must be responsible for reviewing the actions performed by the Security Administrator and CAA 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, the following:

1) Reviewing, managing, controlling, and maintaining security audit log data.

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

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

3) Documenting, testing, and maintaining the solution.

4) Responding 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:

- Ensuring the EUD is only operated in physical spaces which comply with the end user agreement.

- Alerting the Security Administrator immediately upon a EUD being lost, stolen, or suspected of being tampered with.

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

Table 24. Role-Based Personnel Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-GD-31	The Security Administrator, CAAs, 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 CAA already in place may also support this solution, provided they meet this requirement.	T=O	
WLAN-GD-32	The Security Administrator, CAA, and Auditor roles must be performed by different people.	T=O	
WLAN-GD-33	All Security Administrators, CAAs, EUD Users, and Auditors must meet local IA training requirements.	T=O	
WLAN-GD-34	The CAA(s) for the Inner tunnel must be different individuals from the CAA(s) for the Outer tunnel.	O	Optional
WLAN-GD-35	Upon discovering an EUD is lost, stolen or altered, an EUD User must immediately report the incident to their Security Administrator and Certificate Authority Administrator.	T=O	
WLAN-GD-36	Upon notification of a lost, stolen or altered EUD, the Certificate Authority Administrators must revoke that EUD's certificates.	T=O	
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 Outer VPN Gateway 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.	O	Optional
WLAN-GD-39	The Auditor must review all logs specified in this CP at least once a week.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-GD-40	Security Administrators must initiate the certificate revocation process prior to disposal of any solution component.	T=O	
WLAN-GD-41	Auditing of the Outer and Inner CA operations must be performed by individuals who were not involved in the development of the Certificate Policy and CPS, or integration of the WLAN solution.	T=O	

14 INFORMATION TO SUPPORT AO

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

- The customer, possibly with support from 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, see Section 14.1.

- The customer has system certification and accreditation performed using the risk assessment information referenced in Section 14.2.

- 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 14.3.

- Customers who want to use a variant of the solution detailed in this CP will contact their NSA/IAD 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 12.2.

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

14.1 SOLUTION TESTING

This section provides a framework for a Test and Evaluation (T&E) plan and procedures to validate the implementation of a 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. Include product model and serial numbers, and software version numbers at a minimum.

3) Develop a test plan for the specific implementation using the test requirements from the Testing Requirement 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 testing requirement has been developed to ensure that the WLAN solution functions properly and meets the configuration requirements from Section 11. Testing of these requirements should be used as a minimum framework for the development of the detailed test plan and procedures

Table 25. Test Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WLAN-TR-1	Requirement has been relocated to the Key Management Requirements Annex.		

14.2 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/IAC 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.

14.3 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 http://www.nsa.gov/resources/everyone/csfc/solution-registration.shtml.

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.

15 TESTING REQUIREMENTS

The testing requirements for the WLAN solution can be found in a separate document, as an annex to this CP. This document contains the specific tests that allow the Security Administrator or Integrator to ensure they have properly configured the solution. Contact the CSfC PMO to obtain the WLAN CP Testing Annex.

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 4.1.3).

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 4009 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 Mobile Access 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 (see Section 5.1.2 for explanation of detailed differences between VPN EUD and TLS EUD solution design options).

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 4.1.2).

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 Outer VPN Gateway 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 4.1.1)

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 can 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 and Outer VPN Gateways, Certificate Authorities, and Administration Workstations, but does not include EUDs.

APPENDIX B.   ACRONYMS

Acronym	Definition
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
CNSS	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
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
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
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
ECDH	Elliptic Curve Diffie-Hellman
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral

Acronym	Definition
ECDSA	Elliptic Curve Digital Signature Algorithm
ESP	Encapsulating Security Payload
EST	Enrollment Over Secure Transport
EUD	End User Device
FIPS	Federal Information Processing Standards
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
MAC	Media Access Control
MDM	Mobile Device Manager
MOA	Memorandum of Agreement
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

Acronym	Definition
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
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 Manager
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
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-F- Protected Access
WPA2	Wi-Fi Protected Access II

APPENDIX C.   REFERENCES

CNSSI 1300	*CNSSI 1300, National Security Systems Public Key Infrastructure X.509 Certificate Policy*	December 2014
CNSSI 4009	*CNSSI 4009, National Information Assurance (IA) Glossary Committee for National Security Systems.* http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf	April 2015
CNSSP 15	*CNSS Policy (CNSSP) Number 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems Committee for National Security Systems*	October 2016
CNSSD 505	*CNSS Directive (CNSSD) Number 505, Supply Chain Risk Management (SCRM)*	March 2012
FIPS 140	*Federal Information Processing Standard 140, Security Requirements For Cryptographic Modules National Institute for Standards and Technology FIPS Publication* http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf	May 2001
FIPS 180	*Federal Information Processing Standard 180-4, Secure Hash Standard (SHS)*	March 2012
FIPS 186	*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	*Federal Information Processing Standard 201, Personal Identity Verification (PIV) of Federal Employees and Contractors National Institute for Standards and Technology FIPS Publication* http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf	March 2006
IPsec VPN Client PP	*Protection Profile for IPsec Virtual Private Network (VPN) Clients.* http://www.niap-ccevs.org/pp	October 2013
ISO 09594-8	*Iso9594-8 Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 2001*	March 2013
Commercial National Security Algorithm Suite	*NSA Guidance on Encryption Algorithms* https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm	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 5759	*IETF RFC 5759 Suite B Certificate and Certificate Revocation List (CRL) Profile.* J. Solinas and L. Zieglar.	January 2010
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 6239	*IETF RFC 6239 Suite B Cryptographic Suites for Secure Shell (SSH).* K. Igoe.	May 2011
RFC 6379	*IETF RFC 6379 Suite B Cryptographic Suites for IPsec.* L. Law and J. Solinas.	October 2011
RFC 6380	*IETF RFC 6380 Suite B Profile for Internet Protocol Security (IPsec).* K. Burgin and M. Peck.	October 2011

RFC 6460	*IETF RFC 6460 Suite B Profile for Transport Layer Security (TLS)*. M. Salter and R. Housley.	January 2012
RFC 6818	*IETF RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. P. Yee	January 2013
RFC 7030	*IETF RFC 7030 Enrollment over Secure Transport*. M. Pritikin, P. Yee, and D. Harkins.	October 2013
SP 800-53	*NIST Special Publication 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations*. Joint Task Force Transformation Initiative.	April 2013
SP 800-56A	*NIST Special Publication 800-56A Rev. 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*. E. Barker, et. al.	May 2013
SP 800-56B	*NIST Special Publication 800-56B, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*. E. Barker, et. al.	August 2009
SP 800-56C	*NIST Special Publication 800-56C, Recommendation for Key Derivation through Extraction-then-Expansion*. L. Chen.	November 2011
SP 800-131A	*NIST Special Publication 800-131A, Recommendation for Transitioning of Cryptographic Algorithms and Key Lengths*. E. Barker.	January 2011
SP 800-147	*NIST Special Publication 800-147, BIOS Protection Guidelines*. D. Cooper, et. al.	April 2011

APPENDIX D. REQUIREMENTS MAPPINGS TO CNSSI 1253 / NIST SP 800-53 CONTROLS

Most of the requirements in this Capability Package support the implementation of security controls specified in NIST SP 800-53 Revision 4. This appendix is provided for customers who must demonstrate implementation of a set of NIST SP 800-53 security controls as part of their Risk Management Framework (formerly known as the C&A) process for a system incorporating a Campus WLAN solution that complies with this Capability Package.

Note that the presence of a mapping between a requirement and a NIST SP 800-53 security control does not necessarily indicate that the requirement is by itself sufficient to fully address the security control. Instead, it indicates that implementation of the requirement provides some degree of support to implementation of the security control. Additional work outside the scope of this Capability Package may be needed for the overall system to implement the security control.

The security controls mapping for SP 800-53 is the same for CNSSI 1253 and does not represent a High Water Mark (HWM) since that concept does not apply to NSS. Security controls selected under CNSSI 1253 will be tailored according to the individual impact levels for confidentiality, integrity, and availability and adjusted per Appendix J of CNSSI 1253.

Table 26. Mappings to CNSSI 1253/NIST SP 800-53 Security Controls

Requirement	CNSSI-1253	NIST SP 800-53 Revision 4 Security Controls
WLAN-PS-1	SA-4(6)(7)	SA-4(6)(7)
WLAN-PS-2	SA-4(6)(7)	SA-4(6)(7)
WLAN-PS-3	SA-4(6)(7)	SA-4(6)(7)
WLAN-PS-4	SA-4(6)(7)	SA-4(6)(7)
WLAN-PS-5	SA-4(6)(7)	SA-4(6)(7)
WLAN-PS-6	SA-4(6)(7)	SA-4(6)(7)
WLAN-PS-7	SA-4(6)(7)	SA-4(6)(7)
WLAN-PS-8	SA-12(13)	SA-12(13)
WLAN-PS-9	SC-3	SC-3
WLAN-PS-10	SA-12(13)	SA-12(13)
WLAN-PS-11	SA-12(13)	SA-12(13)
WLAN-PS-12	SA-12(13)	SA-12(13)
WLAN-PS-13	SA-9(1), SA-12(2)(8), SA-13	SA-9(1), SA-12(2)(8), SA-13
WLAN-PS-14	SA-4(7)	SA-4(7)
WLAN-SR-1	AC-2	AC-2
WLAN-SR-2	AU-8(1B)	AU-8(1B)
WLAN-SR-3	AU-8(1B)	AU-8(1B)
WLAN-SR-4	CM-7	CM-7

Requirement	CNSSI-1253	NIST SP 800-53 Revision 4 Security Controls
WLAN-SR-5	SI-3(2)	SI-3(2)
WLAN-SR-6	AC-4, CM-6, CM-9	AC-4, CM-6, CM-9
WLAN-EU-1	AC-5, AC-6(1)(3)(5), AC-18(1)(4)	AC-5, AC-6(1)(3)(5), AC-18(1)(4)
WLAN-EU-2	AC-2(7)(a), AC-3(7), AC-5, AC-6(1)(3)(5), AC-18(1)(4), IA-2(1)(3)	AC-2(7)(a), AC-3(7), AC-5, AC-6(1)(3)(5), AC-18(1)(4), IA-2(1)(3)
WLAN-EU-3	CM-7(5)	CM-7(5)
WLAN-EU-4	CM-11(2)	CM-11(2)
WLAN-EU-5	AC-2,	AC-2,
WLAN-EU-6	AC-7(1)(2)	AC-7(1)(2)
WLAN-EU-7	SC-13, SC-17	SC-13, SC-17
WLAN-EU-8	SC-13, SC-17	SC-13, SC-17
WLAN-EU-9	IR-8	IR-8
WLAN-EU-10	IR-8	IR-8
WLAN-EU-11	AC-2, AC-3, IA-2, IA-11	AC-2, AC-3, IA-2, IA-11
WLAN-EU-12	AC-2, AC-3, IA-2, IA-11	AC-2, AC-3, IA-2, IA-11
WLAN-EU-13	AC-11, IA-11	AC-11, IA-11
WLAN-EU-14	PL-4, PS-6	PL-4, PS-6
WLAN-EU-15	AC-18, PL-4	AC-18, PL-4
WLAN-EU-16	PS-6, PE-18(1), PE-19, PE-20, SC-43, AT-2, AT-4, PS-3(1)(2), PS-6, AC-2, IA-4(2), PL-4, PS-6	PS-6, PE-18(1), PE-19, PE-20, SC-43, AT-2, AT-4, PS-3(1)(2), PS-6, AC-2, IA-4(2), PL-4, PS-6
WLAN-EU-17	SC-43, SC-7, AC-19(4)	SC-43, SC-7, AC-19(4)
WLAN-EU-18	SC-42(2)	SC-42(2)
WLAN-EU-19	SC-42(3)	SC-42(3)
WLAN-EU-20	CM-6	CM-6
WLAN-EU-21	SC-42(3)	SC-42(3)
WLAN-EU-22	MP-6	MP-6
WLAN-EU-23	IA-5(1)	IA-5(1)
WLAN-EU-24	SC-28	SC-28
WLAN-EU-25	withdrawn	withdrawn
WLAN-EU-26	withdrawn	withdrawn
WLAN-EU-27	IA-5(1)	IA-5(1)
WLAN-EU-28	withdrawn	withdrawn
WLAN-EU-29	AC-2(6)	AC-2(6)
WLAN-EU-30	IA-5	IA-5
WLAN-EU-31	IA-5	IA-5
WLAN-EU-32	AC-11(1)	AC-11(1)
WLAN-EU-33	MP-7, CM-6	MP-7, CM-6
WLAN-EU-34	MP-7, CM-6	MP-7, CM-6

Requirement	CNSSI-1253	NIST SP 800-53 Revision 4 Security Controls
WLAN-EU-35	SI-7(15)	SI-7(15)
WLAN-EU-36	AC-18	AC-18
WLAN-EU-37	AC-18	AC-18
WLAN-EU-38	AC-18	AC-18
WLAN-EU-39	CM-7(5)	CM-7(5)
WLAN-WC-1	CM-6	CM-6
WLAN-WC-2	AC-18(1), SC-12	AC-18(1), SC-12
WLAN-WC-3	IA-5(2)	IA-5(2)
WLAN-WC-4	IA-5(2)	IA-5(2)
WLAN-WC-5	AC-18(1)	AC-18(1)
WLAN-WC-6	SC-17	SC-17
WLAN-WC-7	IA-5	IA-5
WLAN-WC-8	CM-6	CM-6
WLAN-WC-9	CM-6	CM-6
WLAN-WC-10	AC-18	AC-18
WLAN-WC-11	SC-17	SC-17
WLAN-WC-12	SC-17	SC-17
WLAN-WC-13	CM-6, SC-43	CM-6, SC-43
WLAN-WL-1	SC-13	SC-13
WLAN-WL-2	SC-13	SC-13
WLAN-WL-3	SC-13	SC-13
WLAN-WL-4	SC-8(1)	SC-8(1)
WLAN-CR-1	SC-13	SC-13
WLAN-CR-2	SC-17, IA-5(5)	SC-17, IA-5(5)
WLAN-CR-3	IA-5(5)	IA-5(5)
WLAN-CR-4	SC-13	SC-13
WLAN-CR-5	SC-13	SC-13
WLAN-CR-6	SC-13	SC-13
WLAN-CR-7	SC-13	SC-13
WLAN-CR-8	SC-13	SC-13
WLAN-CR-9	SC-13	SC-13
WLAN-CR-10	SC-12	SC-12
WLAN-CR-11	SC-17	SC-17
WLAN-CR-12	SC-17	SC-17
WLAN-WS-1	SC-11, CM-6	SC-11, CM-6
WLAN-WS-2	SC-12	SC-12

Requirement	CNSSI-1253	NIST SP 800-53 Revision 4 Security Controls
WLAN-WS-3	IA-5(2)	IA-5(2)
WLAN-WS-4	SC-17, SC-12	SC-17, SC-12
WLAN-WS-5	SC-7	SC-7
WLAN-WS-6	SC-7	SC-7
WLAN-WS-7	SC-7, SC-7(14), SC-7(21), SC-7(22)	SC-7, SC-7(14), SC-7(21), SC-7(22)
WLAN-IA-1	SC-7	SC-7
WLAN-IA-2	SC-8(1)	SC-8(1)
WLAN-IA-3	SC-13	SC-13
WLAN-IA-4	SC-13	SC-13
WLAN-IA-5	SC-13	SC-13
WLAN-IA-6	SC-12	SC-12
WLAN-IA-7	SC-12	SC-12
WLAN-IA-8	SC-13	SC-13
WLAN-IA-9	SC-12	SC-12
WLAN-IA-10	AC-6(1)	AC-6(1)
WLAN-IA-11	IA-5(1)	IA-5(1)
WLAN-IA-12	SC-13	SC-13
WLAN-AA-1	SC-8(1)	SC-8(1)
WLAN-AA-2	SC-13	SC-13
WLAN-AA-3	SC-13	SC-13
WLAN-AA-4	SC-13	SC-13
WLAN-WA-1	IA-5(2)	IA-5(2)
WLAN-WA-2	SC-12	SC-12
WLAN-WA-3	SC-12	SC-12
WLAN-WA-4	IA-5(2)	IA-5(2)
WLAN-WA-5	IA-5(2)	IA-5(2)
WLAN-WA-6	IA-5(14)	IA-5(14)
WLAN-WA-7	*withdrawn*	*withdrawn*
WLAN-WA-8	IA-5(2)	IA-5(2)
WLAN-WA-9	SC-23(5)	SC-23(5)
WLAN-WA-10	SC-23(5)	SC-23(5)
WLAN-WA-11	SC-23(5)	SC-23(5)
WLAN-WA-12	AU-2	AU-2
WLAN-WA-13	AU-2	AU-2
WLAN-PF-1	SC-43, CM-7	SC-43, CM-7
WLAN-PF-2	CM-7	CM-7

Requirement	CNSSI-1253	NIST SP 800-53 Revision 4 Security Controls
WLAN-PF-3	SC-7(5)	SC-7(5)
WLAN-PF-4	SC-7(5), CM-7	SC-7(5), CM-7
WLAN-PF-5	CM-7	CM-7
WLAN-PF-6	SC-7(5), CM-7	SC-7(5), CM-7
WLAN-PF-7	CM-2	CM-2
WLAN-PF-8	AC-4(1), SC-7, CA-9	AC-4(1), SC-7, CA-9
WLAN-PF-9	SC-7, CA-9	SC-7, CA-9
WLAN-PF-10	SC-7, CA-9	SC-7, CA-9
WLAN-PR-1	CM-2, AC-18	CM-2, AC-18
WLAN-PR-2	CM-2, AC-18(5), SC-40(2)	CM-2, AC-18(5), SC-40(2)
WLAN-PR-3	CM-2, AC-18(5), SC-40(2)	CM-2, AC-18(5), SC-40(2)
WLAN-PR-4	SC-7, CM-2	SC-7, CM-2
WLAN-PR-5	AC-18(3)	AC-18(3)
WLAN-PR-6	IA-5	IA-5
WLAN-PR-7	CM-2	CM-2
WLAN-PR-8	CM-7(5)	CM-7(5)
WLAN-PR-9	CM-2	CM-2
WLAN-PR-10	IA-5(1)	IA-5(1)
WLAN-PR-11	CM-2, CM-7(5), CA-6	CM-2, CM-7(5), CA-6
WLAN-VG-1	withdrawn	withdrawn
WLAN-VG-2	withdrawn	withdrawn
WLAN-VG-3	withdrawn	withdrawn
WLAN-VG-4	withdrawn	withdrawn
WLAN-VG-5	withdrawn	withdrawn
WLAN-VG-6	withdrawn	withdrawn
WLAN-WI-1	SI-4(14)	SI-4(14)
WLAN-WI-2	SI-4(14)	SI-4(14)
WLAN-WI-3	SI-4(14)	SI-4(14)
WLAN-WI-4	CM-5, AC-6(1)	CM-5, AC-6(1)
WLAN-WI-5	SI-4(15)	SI-4(15)
WLAN-WI-6	SI-4(4)	SI-4(4)
WLAN-WI-7	CM-6, CM-7	CM-6, CM-7
WLAN-WI-8	CM-2, CP-2(6), CP-7	CM-2, CP-2(6), CP-7
WLAN-WI-9	SI-4(14)	SI-4(14)
WLAN-WI-10	SI-4(14)	SI-4(14)
WLAN-WI-11	SI-4(14)	SI-4(14)
WLAN-WI-12	SI-4, AU-14(2)	SI-4, AU-14(2)

Requirement	CNSSI-1253	NIST SP 800-53 Revision 4 Security Controls
WLAN-WI-13	SI-4	SI-4
WLAN-WI-14	SI-4	SI-4
WLAN-WI-15	SI-4, CM-6	SI-4, CM-6
WLAN-WI-16	CM-6	CM-6
WLAN-WI-17	CM-6	CM-6
WLAN-WI-18	AU-2, SI-4	AU-2, SI-4
WLAN-WI-19	SI-4	SI-4
WLAN-WI-20	SI-4	SI-4
WLAN-WI-21	SI-4	SI-4
WLAN-WI-22	CM-6	CM-6
WLAN-WI-23	AU-2, SI-4	AU-2, SI-4
WLAN-WI-24	AU-2, SI-4	AU-2, SI-4
WLAN-WI-25	SI-3(7), SI-4(24)	SI-3(7), SI-4(24)
WLAN-WI-26	SC-5(3)	SC-5(3)
WLAN-WI-27	SC-7(17)	SC-7(17)
WLAN-WI-28	AU-2, SI-4	AU-2, SI-4
WLAN-WI-29	AU-2, SI-4	AU-2, SI-4
WLAN-WI-30	SC-5(2)	SC-5(2)
WLAN-WI-31	SI-4	SI-4
WLAN-WI-32	SI-4	SI-4
WLAN-WI-33	SI-4	SI-4
WLAN-WI-34	AU-2, SI-4	AU-2, SI-4
WLAN-WI-35	AU-2, SI-4	AU-2, SI-4
WLAN-WI-36	AU-2, SI-4	AU-2, SI-4
WLAN-WI-37	AU-2, SI-4	AU-2, SI-4
WLAN-WI-38	AU-2, SI-4	AU-2, SI-4
WLAN-WI-39	SI-4	SI-4
WLAN-WI-40	SI-4(15)	SI-4(15)
WLAN-WI-41	SI-4	SI-4
WLAN-WI-42	AU-2, SI-4	AU-2, SI-4
WLAN-WI-43	AU-2, SI-4	AU-2, SI-4
WLAN-WI-44	CM-6, CM-7	CM-6, CM-7
WLAN-WI-45	SI-4	SI-4
WLAN-WI-46	SI-4	SI-4
WLAN-WI-47	AU-12(2)	AU-12(2)
WLAN-CM-1	CM-2	CM-2
WLAN-CM-2	CM-3(1)	CM-3(1)
WLAN-CM-3	CM-3(1)	CM-3(1)
WLAN-CM-4	CM-6, SI-7	CM-6, SI-7

Requirement	CNSSI-1253	NIST SP 800-53 Revision 4 Security Controls
WLAN-DM-1	CM-7, AC-5	CM-7, AC-5
WLAN-DM-2	Withdrawn	Withdrawn
WLAN-DM-3	SI-3	SI-3
WLAN-DM-4	CM-7	CM-7
WLAN-DM-5	AC-4(2)	AC-4(2)
WLAN-DM-6	AC-6(3), CM-7	AC-6(3), CM-7
WLAN-DM-7	AC-3	AC-3
WLAN-DM-8	SC-13	SC-13
WLAN-DM-9	AT-3, PL-7	AT-3, PL-7
WLAN-DM-10	AU-6(4)	AU-6(4)
WLAN-DM-11	SC-12	SC-12
WLAN-DM-12	SC-12	SC-12
WLAN-DM-13	AU-6(4)	AU-6(4)
WLAN-DM-14	CM-6, CM-7	CM-6, CM-7
WLAN-DM-15	CM-6, CM-7	CM-6, CM-7
WLAN-DM-16	SC-13	SC-13
WLAN-MR-1	SI-4	SI-4
WLAN-MR-2	SI-4	SI-4
WLAN-MR-3	SI-4, SC-13	SI-4, SC-13
WLAN-MR-4	AU-10(2)	AU-10(2)
WLAN-MR-5	CM-2, CM-7	CM-2, CM-7
WLAN-MR-6	SI-4, CM-6	SI-4, CM-6
WLAN-MR-7	SI-4, CM-6	SI-4, CM-6
WLAN-MR-8	AU-2, SI-4	AU-2, SI-4
WLAN-MR-9	AU-2, SI-4	AU-2, SI-4
WLAN-MR-10	AU-2, SI-4	AU-2, SI-4
WLAN-MR-11	AU-2, SI-4	AU-2, SI-4
WLAN-MR-12	SC-7, SI-4	SC-7, SI-4
WLAN-MR-13	SI-4, CM-6	SI-4, CM-6
WLAN-MR-14	PL-7	PL-7
WLAN-AU-1	AU-2	AU-2
WLAN-AU-2	AU-2	AU-2
WLAN-AU-3	AU-2	AU-2
WLAN-AU-4	AU-2	AU-2
WLAN-AU-5	AU-2	AU-2
WLAN-AU-6	AU-2	AU-2
WLAN-AU-7	AU-2	AU-2

Requirement	CNSSI-1253	NIST SP 800-53 Revision 4 Security Controls
WLAN-AU-8	AU-2	AU-2
WLAN-AU-9	AU-2	AU-2
WLAN-AU-10	AU-2	AU-2
WLAN-AU-11	AU-2	AU-2
WLAN-AU-12	AU-3	AU-3
WLAN-AU-13	AU-3	AU-3
WLAN-AU-14	AU-3	AU-3
WLAN-AU-15	AU-3	AU-3
WLAN-AU-16	AU-3	AU-3
WLAN-AU-17	AU-3	AU-3
WLAN-AU-18	AU-3	AU-3
WLAN-AU-19	AU-6, SI-4, SI-5	AU-6, SI-4, SI-5
WLAN-AU-20	AU-2, AU-6(7)	AU-2, AU-6(7)
WLAN-AU-21	AU-2, AU-6(7)	AU-2, AU-6(7)
WLAN-AU-22	AU-2	AU-2
WLAN-AU-23	AU-2	AU-2
WLAN-AU-24	AU-2	AU-2
WLAN-AU-25	AU-2	AU-2
WLAN-AU-26	AU-2, SI-7(8)	AU-2, SI-7(8)
WLAN-AU-27	AU-2, SI-7(8)	AU-2, SI-7(8)
WLAN-AU-28	AU-2	AU-2
WLAN-AU-29	SI-4(13)	SI-4(13)
WLAN-KM-1	CA-6, IA-5(6)	CA-6, IA-5(6)
WLAN-KM-2	CM-7	CM-7
WLAN-KM-3	IA-5(2), CM-7	IA-5(2), CM-7
WLAN-KM-4	SC-17	SC-17
WLAN-KM-5	SC-12	SC-12
WLAN-KM-6	SC-17	SC-17
WLAN-KM-7	IA-5(6)	IA-5(6)
WLAN-KM-8	SI-3	SI-3
WLAN-KM-9	SC-12	SC-12
WLAN-KM-10	CA-6	CA-6
WLAN-KM-11	CM-6	CM-6
WLAN-KM-12	CM-6	CM-6
WLAN-KM-13	SC-13	SC-13
WLAN-KM-14	SC-17	SC-17
WLAN-KM-15	SC-17	SC-17
WLAN-KM-16	SC-13	SC-13
WLAN-KM-17	IA-5(6)	IA-5(6)

Requirement	CNSSI-1253	NIST SP 800-53 Revision 4 Security Controls
WLAN-KM-18	SC-17	SC-17
WLAN-KM-19	SC-12	SC-12
WLAN-KM-20	SC-17	SC-17
WLAN-KM-21	SC-12	SC-12
WLAN-KM-22	SC-17	SC-17
WLAN-KM-23	SC-17	SC-17
WLAN-KM-24	SC-17	SC-17
WLAN-KM-25	SC-12	SC-12
WLAN-KM-26	SC-12	SC-12
WLAN-KM-27	SC-12	SC-12
WLAN-KM-28	SC-12	SC-12
WLAN-KM-29	SC-12	SC-12
WLAN-KM-30	SC-12	SC-12
WLAN-KM-31	SC-12	SC-12
WLAN-KM-32	SC-12	SC-12
WLAN-KM-33	SC-12	SC-12
WLAN-KM-34	SC-12	SC-12
WLAN-KM-35	SC-17	SC-17
WLAN-KM-36	SC-17	SC-17
WLAN-KM-37	SC-12	SC-12
WLAN-KM-38	SC-17, SC-12	SC-17, SC-12
WLAN-KM-39	SC-17	SC-17
WLAN-KM-40	SC-17	SC-17
WLAN-KM-41	SC-17	SC-17
WLAN-KM-42	SC-17	SC-17
WLAN-KM-43	SC-17	SC-17
WLAN-KM-44	SC-17	SC-17
WLAN-KM-45	SC-17	SC-17
WLAN-KM-46	SC-12	SC-12
WLAN-KM-47	SC-12	SC-12
WLAN-KM-48	SC-12	SC-12
WLAN-KM-49	SC-12	SC-12
WLAN-KM-50	SC-17	SC-17
WLAN-KM-51	SC-17	SC-17
WLAN-FW-1	CM-7, CM-7(21)	CM-7, CM-7(21)
WLAN-FW-2	CM-7, CM-7(21)	CM-7, CM-7(21)
WLAN-FW-3	CM-7, CM-7(21)	CM-7, CM-7(21)
WLAN-FW-4	CM-7, SC-7	CM-7, SC-7
WLAN-FW-5	CM-7, PL-7, AC-4(21), SC-7(13)	CM-7, PL-7, AC-4(21), SC-7(13)

Requirement	CNSSI-1253	NIST SP 800-53 Revision 4 Security Controls
WLAN-FW-6	PL-7, AC-4(21), SC-7, CM-7	PL-7, AC-4(21), SC-7, CM-7
WLAN-FW-7	PL-7, AC-4(21), SC-7, CM-7	PL-7, AC-4(21), SC-7, CM-7
WLAN-FW-8	SC-7	SC-7
WLAN-FW-9	CM-6, SC-7(5)	CM-6, SC-7(5)
WLAN-GD-1	CA-6, PE-1, PE-3	CA-6, PE-1, PE-3
WLAN-GD-2	PE-2, PE-3	PE-2, PE-3
WLAN-GD-3	PE-2, PE-3	PE-2, PE-3
WLAN-GD-4	PL-2, MP-8	PL-2, MP-8
WLAN-GD-5	PL-7, SC-13, AC-19(5)	PL-7, SC-13, AC-19(5)
WLAN-GD-6	SC-12	SC-12
WLAN-GD-7	SA-18(2), CM-3, CM-2(7), PE-3(5)	SA-18(2), CM-3, CM-2(7), PE-3(5)
WLAN-GD-8	SA-1, PM-11	SA-1, PM-11
WLAN-GD-9	CA-2(1)	CA-2(1)
WLAN-GD-10	CA-2	CA-2
WLAN-GD-11	CA-2	CA-2
WLAN-GD-12	N/A	N/A
WLAN-GD-13	CA-2	CA-2
WLAN-GD-14	N/A	N/A
WLAN-GD-15	CA-6	CA-6
WLAN-GD-16	CA-6	CA-6
WLAN-GD-17	AU-11	AU-11
WLAN-GD-18	AU-4	AU-4
WLAN-GD-19	AU-4(1)	AU-4(1)
WLAN-GD-20	IR-6	IR-6
WLAN-GD-21	AU-4	AU-4
WLAN-GD-22	AU-11(1)	AU-11(1)
WLAN-GD-23	AU-5(3)	AU-5(3)
WLAN-GD-24	AU-15	AU-15
WLAN-GD-25	IA-5(1)	IA-5(1)
WLAN-GD-26	SI-2, CM-9, CM-3	SI-2, CM-9, CM-3
WLAN-GD-27	SI-2, CM-9, CM-3	SI-2, CM-9, CM-3
WLAN-GD-28	PE-19(1)	PE-19(1)
WLAN-GD-29	RA-2, MP-4	RA-2, MP-4
WLAN-GD-30	CM-8	CM-8
WLAN-RP-1	IR-6	IR-6
WLAN-RP-2	IR-6, IR-8	IR-6, IR-8
WLAN-RP-3	IR-8	IR-8
WLAN-RP-4	IR-9	IR-9

Requirement	CNSSI-1253	NIST SP 800-53 Revision 4 Security Controls
WLAN-RP-5	IR-8	IR-8
WLAN-RP-6	IR-8	IR-8
WLAN-RP-7	IR-8	IR-8
WLAN-RP-8	IR-8	IR-8
WLAN-RP-9	IR-8	IR-8
WLAN-RP-10	IR-8	IR-8
WLAN-RP-11	IR-8	IR-8
WLAN-RP-12	IR-8	IR-8
WLAN-RP-13	IR-8	IR-8
WLAN-RP-14	IR-8	IR-8
WLAN-RP-15	IR-8	IR-8