Classification: UNCLASSIFIED

Registration #

Solution Name:

Date Submitted:

INFORMATION ASSURANCE CAPABILITIES

Commercial Solutions for Classified

harnessing the power of commercial industry

Campus Wireless LAN Capability Package

Version 2.2

Compliance Checklist

Classification: UNCLASSIFIED

1 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 1. Production Selection Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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: • 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	O	Optional	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
	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,	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
	• be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence.			
WLAN-PS-14	The cryptographic libraries used by the WLAN Access System and the Inner VPN Gateway must either: • come from different manufacturers, where neither manufacturer is a subsidiary of the other; or, • be different libraries from the same manufacturer, where NSA has determined that the libraries meet the CSfC criteria for implementation independence.	T=O	Optional	
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-PS-16	Components must be configured to use the NIAP-certified evaluated configuration.	T=O		

2 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.)

2.1 OVERALL SOLUTION REQUIREMENTS

Table 2. Overall Solution Requirements (SR)

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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.[1]	T=O		

2.2 END USER DEVICES REQUIREMENTS

Table 3. End User Device (EU) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

[1] 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	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-EU-11	Users of EUDs must successfully authenticate themselves to the services they access on their respective Red Network using an AO-approved method.	T=O		
WLAN-EU-12	Red Network services must not transmit any classified data to EUDs until user authentication succeeds.	T=O		
WLAN-EU-13	The EUD must lock the screen and require user re-authentication after an AO-approved period of inactivity.	T=O		
WLAN-EU-14	All EUD users must sign an organization-defined user agreement before being authorized to use an EUD.	T=O		
WLAN-EU-15	All EUD users must receive an organization-developed training course for operating an EUD prior to use.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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[2].	T=O		
WLAN-EU-25	Withdrawn			

[2] 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	Compliance (Explain how your solution meets this requirement)
WLAN-EU-26	Withdrawn			
WLAN-EU-27	The EUD maximum password lifetime must be less than 181 days.	T=O		
WLAN-EU-28	The EUD screen must lock after an AO approved period of inactivity.	T=O		
WLAN-EU-29	The EUD must perform a wipe of all protected data after 10 or more authentication failures.	T=O		
WLAN-EU-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	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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	

2.3 CONFIGURATION REQUIREMENTS FOR THE WLAN CLIENT

Table 4. WLAN Client (WC) Configuration Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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 5. Wireless Link (WL) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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 6. 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

Security Service	Algorithm Suite	Specifications
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
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 7. 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

2.4 CONFIGURATION REQUIREMENTS FOR VPN COMPONENTS AND VPN CLIENT

Table 8. Configuration Requirements (CR) for VPN Components

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-CR-1	The VPN Components must use protocols and algorithms for creating all VPN tunnels selected from an Algorithm Suite in Table 6 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	
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

2.5 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 9. WLAN Access System (WS) Configuration Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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 10. Wireless Infrastructure Authentication (IA) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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 orIKEv2) or TLS/RADsec connection.	O	WLAN-IA-1	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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 5.	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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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 5 Table 5.	T=O		

Table 11. Wireless Authentication and Authorization (AA) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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 6.	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 6.	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 6.	T	WLAN-AA-5	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-AA-5	The WLAN Client and WLAN Authentication Server must use the EAP-TLS Cipher suite from the Objective section of Table 6.	O	WLAN-AA-4	

Table 12. Wireless Authentication Server (WA) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-WA-4	The WLAN AS must use the Distinguished Name or the Subject Alternate Name contained in the WLAN Client's certificate to authenticate the identity of the WLAN Client.	T=O		
WLAN-WA-5	The WLAN Authentication Server must verify that the WLAN Client's certificate is not expired.	T=O		
WLAN-WA-6	The WLAN AS must ensure that the WLAN Client's certificate chain is rooted by the WLAN trusted root Certificate Authority.	T=O		
WLAN-WA-7	Withdrawn			
WLAN-WA-8	The WLAN Authentication Server must authenticate the identity of the WLAN Client by verifying that the WLAN Client's certificate is not revoked.	T=O		
WLAN-WA-9	When supporting multiple enclaves, the AS must verify that the Common Name presented by the EUD certificate is included on a whitelist tied to an enclave.	T	WLAN-WA-10	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

2.6 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 13. Port Filtering (PF) Requirements for Solution Components

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-PF-1	All components within the solution must have all network interfaces restricted to the fewest address ranges, ports, and protocols possible.	T=O		
WLAN-PF-2	All components within the solution must have all unused network interfaces disabled.	T=O		
WLAN-PF-3	For all interfaces connected to a Gray Network, traffic filtering rules must be applied to both inbound and outbound traffic, such that only EAP-TLS, IKE, IPsec, and control plane protocols (as defined in this Capability Package) approved by policy are allowed. All packets not explicitly allowed must be blocked.	T=O		
WLAN-PF-4	Any service or feature that allows a EUD to contact a third party server (such as one maintained by the manufacturer) must be blocked.	T	WLAN-PF-5	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

2.7 END USER DEVICE PROVISIONING REQUIREMENTS

Table 14. EUD Provisioning Requirements (PR)

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

2.8 CONFIGURATION REQUIREMENTS FOR WIRELESS INTRUSION DETECTION SYSTEM (WIDS)

Table 15. Wireless IDS (WI) Configuration Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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	
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	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		
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	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-WI-41	The WIDS must detect and log the presence of an 802.11 bridge.	T=O		
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

2.9 CONFIGURATION CHANGE DETECTION REQUIREMENTS

Table 16. Configuration Change Detection (CM) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

2.10 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 17. Device Management (DM) Requirements

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

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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	Compliance (Explain how your solution meets this requirement)
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 7).	T=O		

2.11 CONTINUOUS MONITORING REQUIREMENTS

Table 18. Continuous Monitoring (MR) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-MR-6	The IDS in the solution must be configured to send alerts to the Security Administrator.	T	WLAN-MR-7	
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	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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	

2.12 AUDITING REQUIREMENTS

Table 19. Auditing (AU) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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	
WLAN-AU-25	The EUD must audit installation and removal of software.	O	Optional	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

2.13 KEY MANAGEMENT REQUIREMENTS

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

2.14 GRAY FIREWALL REQUIREMENTS

Table 20. Gray Firewall (FW) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-FW-4	Gray Network Firewall must allow HTTP responses from the Gray CDP or OCSP responder to the Authentication Server that contain a well-formed CRL per IETF RFC 5280 or OCSP Response per RFC 6960, and block all other HTTP responses.	O	WLAN-FW-2	
WLAN-FW-5	Gray Network Firewall must only accept management traffic on the physical ports connected to the Gray Management network.	T=O		
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

3 REQUIREMENTS FOR SOLUTION OPERATION, MAINTENANCE, AND HANDLING

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

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

Table 21. Requirements for the Use and Handling of Solutions

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-GD-2	Only authorized and appropriately cleared (or escorted) administrators and security personnel must have physical access to the solution Infrastructure components.	T=O		
WLAN-GD-3	Only authorized and appropriately cleared users, administrators, and security personnel must have physical access to EUDs.	T=O		
WLAN-GD-4	All components of the solution must be disposed of as classified devices, unless declassified using AO-approved procedures.	T=O		
WLAN-GD-5	EUDs using a NSA-approved DAR solution must be disposed of in accordance with the disposal requirements for the DAR solution.	T=O		
WLAN-GD-6	All EUDs must have their certificates revoked prior to disposal.	T=O		
WLAN-GD-7	Users must periodically inspect the physical attributes of EUDs for signs of tampering or other unauthorized changes.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		
WLAN-GD-16	Solution implementation information, which was provided to NSA during solution registration, must be updated annually (in accordance with Section 5.2) as part annual solution re-registration process.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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	Compliance (Explain how your solution meets this requirement)
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 Section3.

3.2 REQUIREMENTS FOR INCIDENT REPORTING

Table 22 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 22 only provides requirements directly related to the incident reporting process. See Section 2.11 for requirements supporting the detection of events that may reveal that a reportable incident has occurred.

Table 22. Incident Reporting Requirements (RP)

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-RP-4	Solution owners must report any evidence of a compromise or spillage of classified data caused by a failure of the CSfC solution.	T=O		
WLAN-RP-5	For Gray Network interfaces, solution owners must report any malicious inbound and outbound traffic.	T=O		
WLAN-RP-6	Solution owners must report any evidence of an unauthorized device/user gaining access to the classified network via the solution.	T=O		
WLAN-RP-7	Solution owners must report if a solution component sends traffic with an unauthorized destination address.	T=O		
WLAN-RP-8	Solution owners must report any malicious configuration changes to the components.	T=O		
WLAN-RP-9	Solution owners must report any unauthorized escalation of privileges to any of the CSfC solution components.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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		

4 ROLE-BASED PERSONNEL REQUIREMENTS

Table 23. Role-Based Personnel Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
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	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-GD-39	The Auditor must review all logs specified in this CP at least once a week.	T=O		
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		

5 INFORMATION TO SUPPORT AO

Table 24. Test Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-TR-1	The organization implementing the CP must perform all tests listed in the WLAN CP Testing Annex.	T=O		

5.1 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.

5.2 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.

6 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.