18.2. Wireless Local Area Networks

Objective

18.2.1. Wireless local area networks are deployed in a secure manner that does not compromise the security of information and systems.

Context

Scope

18.2.2. This section covers information on 802.11x WLANs. It does not cover other wireless communications. These communication methods are covered in Chapter 11 - Communications Systems and Devices. The description 802.11x refers to all versions and 802.11 standards.

Title	Publisher	Source
802.11 Wi-Fi	IEEE	Wireless LAN Media Access Control and Physical Layer specification. 802.11a,b,g,etc. are amendments to the original 802.11 standard. Products that implement 802.11 standards must pass tests and are referred to as "Wi-Fi certified".
802.15 Wireless Personal Area Networks	IEEE	Communications specification that was approved in early 2002 by the IEEE for wireless personal area networks (WPANs and includes Bluetooth, Ultra Wideband, Zigbee and Mesh Networks.
802.16 Wireless Metropolitan Area Networks	IEEE	This family of standards covers Fixed and Mobile Broadband Wireless Access methods used to create Wireless Metropolitan Area Networks (WMANs.) Connects Base Stations to the Internet using OFDM in unlicensed (900 MHz, 2.4, 5.8 GHz) or licensed (700 MHz, 2.5 – 3.6 GHz) frequency bands. Products that implement 802.16 standards can undergo WiMAX certification testing.

18.2.3. Hardware Security Modules (HSMs) are defined as a hardware module or appliance that provides cryptographic functions. These functions include (but are not limited to) encryption, decryption, key generation, and hashing. The appliance usually also offers some level of physical tamper-resistance and has a user interface and a programmable interface. Refer also to Section 17.10 – Hardware Security Modules.

References

18.2.4. Further references can be found at:

Reference	Title	Publisher	Source
	Implementing Network Segmentation and Segregation	ASD	Implementing Network Segmentation and Segregation | Cyber.gov.au
	Wi-Fi Alliance certification programs	Wi-Fi Alliance	http://www.wi-fi.org/certification_programs.php
802.11	**IEEE Standard for Information Technology - Telecommunications and Information Exchange between systems - Local and Metropolitan Area - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications**	IEEE	http://standards.ieee.org/findstds/standard/802.11-2012.html
RFC 5247	**EAP specification**	IETF	https://datatracker.ietf.org/doc/html/rfc5247
RFC 5216	**EAP-TLS specification**	IETF	https://datatracker.ietf.org/doc/html/rfc5216
RFC 5281	**EAP-TTLS specification**	IETF	https://datatracker.ietf.org/doc/html/rfc5281
	Payment Card Industry (PCI) Hardware Security Module (HSM) - Security Requirements	PCI	Official PCI Security Standards Council Site - Document PCI HSM Frequently Asked Questions (pcisecuritystandards.org)
FIPS PUB 140-2	**FIPS PUB 140-2 - Security Requirements for Cryptographic Modules**	NIST	FIPS 140-2, Security Requirements for Cryptographic Modules | CSRC (nist.gov)
	Extensible Authentication Protocol	Microsoft	https://technet.microsoft.com/en-us/network/bb643147.aspx

Rationale & Controls

Bridging networks

18.2.5.R.01. **Rationale**

When connecting devices via Ethernet to an agency's fixed network, agencies need to be aware of the risks posed by active wireless functionality. Devices may automatically connect to any open wireless networks they have previously connected to, which a malicious actor can use to masquerade and establish a connection to the device. This compromised device could then be used as a bridge to access the agency's fixed network. Disabling wireless functionality on devices, preferably by a hardware switch, whenever connected to a fixed network can prevent this from occurring. Additionally, devices do not have to be configured to remember and automatically connect to open wireless networks that they have previously connected to.

18.2.5.C.01. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:3274]

Devices MUST NOT be configured to remember and automatically connect to any wireless networks that they have previously connected to.

18.2.5.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3282]

Wireless auto-connect functionality on devices SHOULD be disabled, preferably by a hardware switch, whenever connected to a fixed network.

Providing wireless communications for public access

18.2.6.R.01. **Rationale**

To ensure that a wireless network provided for public access cannot be used as a launching platform for attacks against an agency's system it MUST be **separated** from all other systems. Security architectures incorporating segmented networks, DMZ's and other segregation mechanisms are useful in this regard.

18.2.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3290]

Agencies deploying a wireless network for public access MUST **separate** it from any other agency networks; including BYOD networks.

Using wireless communications

18.2.7.R.01.

Rationale

As the Accreditation Authority for TOP SECRET systems, GCSB has mandated that all agencies considering deploying a wireless TOP SECRET deployment seek approval from GCSB prior to initiating any networking projects.

18.2.7.C.01. **Control System Classifications(s): Top Secret; Compliance: Must Not** [CID:3298]

Agencies MUST NOT use wireless networks unless the security of the agency's wireless deployment has been approved by GCSB.

Selecting wireless access point equipment

18.2.8.R.01. **Rationale**

Wireless access points that have been certified in a Wi-Fi Alliance certification program provide an agency with assurance that they conform to wireless standards. Deploying wireless access points that are guaranteed to be interoperable with other wireless access points on a wireless network will limit incompatibility of wireless equipment and incorrect implementation of wireless devices by vendors.

18.2.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3302]

All wireless access points used for government wireless networks MUST be Wi-Fi Alliance certified.

802.1X Authentication

18.2.9.R.01. **Rationale**

A number of Extensible Authentication Protocol (EAP) methods, supported by the Wi-Fi Protected Access 2 and 3 (WPA2, WPA3) protocols, are available.

18.2.9.R.02. **Rationale**

Depending on the security requirements agencies deploying a secure wireless network can choose EAP-Transport Layer Security (EAP-TLS), EAP-Tunnelled Transport Layer Security (EAP-TTLS) or Protected EAP (PEAP) to perform mutual authentication.

EAP-TLS is considered one of the most secure EAP methods. With its inclusion in the initial release of the WPA2 standard, it enjoys wide support in wireless access points and in numerous operating systems such as Microsoft Windows, Linux and Apple OS X. EAP-TLS uses a public key infrastructure (PKI) to secure communications between devices and a Remote Access Dial In User Service (RADIUS) server through the use of X.509 certificates. While EAP-TLS provides strong mutual authentication, it requires an agency to have established a PKI. This involves either deploying their own certificate authority and issuing certificates, or purchasing certificates from a commercial certificate authority, for every device that accesses the wireless network. This can introduce additional costs and management overheads but the risk and security management advantages are significant.

The **EAP-TTLS/MSCHAPv2, or simply EAP-TTLS**, method is generally supported through the use of third party software. It has support in multiple operating systems including current and supported versions of Microsoft Windows client and server editions. EAP-TTLS is different to EAP-TLS in that devices do not authenticate to the server when the initial TLS tunnel is created. Only the server authenticates to devices. Once the TLS tunnel has been created, mutual authentication occurs through the use of another EAP method.

An advantage of EAP-TTLS over PEAP is that a username is never transmitted in the clear outside of the TLS tunnel. Another advantage of EAP-TTLS is that it provides support for many legacy EAP methods, while PEAP is generally limited to the use of EAP-MSCHAPv2.

PEAPv0/EAP-MSCHAPv2, or simply PEAP, is the second most widely supported EAP method after EAP-TLS. It enjoys wide support in wireless access points and in numerous operating systems such as Microsoft Windows, Linux and Apple OS X. PEAP operates in a very similar way to EAP-TTLS by creating a TLS tunnel which is used to protect another EAP method. PEAP differs from EAP-TTLS in that when the EAP-MSCHAPv2 method is used within the TLS tunnel, only the password portion is protected and not the username. This may allow an intruder to capture the username and replay it with a bogus password in order to lockout the user's account, causing a denial of service for that user. While EAP-MSCHAPv2 within PEAP is the most common implementation, Microsoft Windows supports the use of EAP-TLS within PEAP, known as PEAP-EAP-TLS. This approach is very similar in operation to traditional EAP-TLS yet provides increased protection, as parts of the certificate that are not encrypted with EAP-TLS are encrypted with PEAP-EAP-TLS. The downside to PEAP-EAP-TLS is its support is limited to Microsoft products.

18.2.9.R.03. **Rationale**

Ultimately, an agency's choice in authentication method will often be based on the size of their wireless deployment, their security requirements and any existing authentication infrastructure. If an agency is primarily motivated by security they can implement either PEAP-EAP-TLS or EAP-TLS. If they are primarily motivated by flexibility and legacy support they can implement EAP-TTLS. If they are primarily motivated by simplicity they can implement PEAP with EAP-MSCHAPv2.

18.2.9.C.01. **Control System Classifications(s): Secret, Confidential, Top Secret; Compliance: Must** [CID:7538]

EAP-TLS or PEAP-EAP-TLS MUST be used on wireless networks to perform mutual authentication.

18.2.9.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3319]

EAP-TLS, PEAP-EAP-TLS, EAP-TTLS or PEAP MUST be used on wireless networks to perform mutual authentication.

Evaluation of 802.1X authentication implementation

18.2.10.R.01. **Rationale**

The security of 802.1X authentication is dependent on three main elements and their interaction. These three elements include supplicants (clients) that support the 802.1X authentication protocol, authenticators (wireless access points) that facilitate communication between supplicants and the authentication server, and the authentication server (RADIUS server) that is used for authentication, authorisation and accounting purposes. To provide assurance that these elements have been implemented appropriately, supplicants, authenticators and the authentication server used in wireless networks must have completed an appropriate product evaluation.

18.2.10.C.01. **Control System Classifications(s): Secret, Top Secret, Confidential; Compliance: Must** [CID:3326]

Supplicants, authenticators and the authentication server used in wireless networks MUST have completed an appropriate product evaluation.

18.2.10.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3329]

Supplicants, authenticators and the authentication server used in wireless networks SHOULD have completed an appropriate product evaluation.

Issuing certificates for authentication

18.2.11.R.01. **Rationale**

Certificates for authenticating to wireless networks can be issued to either or both devices and users. For assurance, certificates must be generated using a certificate authority product or hardware security module (HSM) that has completed an appropriate product evaluation.

18.2.11.R.02. **Rationale**

When issuing certificates to devices accessing wireless networks, agencies need to be aware of the risk that these certificates could be stolen by malicious software. Once compromised, the certificate could be used on another device to gain unauthorised access to the wireless network. Agencies also need to be aware that in only issuing a certificate to a device, any actions taken by a user will only be attributable to the device and not a specific user.

18.2.11.R.03. **Rationale**

When issuing certificates to users accessing wireless networks, they can either be in the form of a certificate that is stored on a device or a certificate that is stored within a smart card. Issuing certificates on smart cards provides increased security, but usually at a higher cost. Security is improved because a user is more likely to notice a missing smart card and alert their local security team, who is then able to revoke the credentials on the RADIUS server. This can minimise the time an intruder has access to a wireless network.

18.2.11.R.04. **Rationale**

In addition, to reduce the likelihood of a stolen smart card from being used to gain unauthorised access to a wireless network, two-factor authentication can be implemented through the use of Personal Identification Numbers (PINs) on smart cards. This is essential when a smart card grants a user any form of administrative access on a wireless network or attached network resource.

18.2.11.R.05. **Rationale**

For the highest level of security, unique certificates should be issued for both devices and users. In addition, the certificates for a device and user must not be stored on the same device. Finally, certificates for users accessing wireless networks should be issued on smart cards with access PINs and not stored with a device when not in use.

18.2.11.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3343]

Agencies MUST generate certificates using a certificate authority product or hardware security module that has completed an appropriate product evaluation.

18.2.11.C.02. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:3346]

The certificates for both a device and user accessing a wireless network MUST NOT be stored on the same device.

18.2.11.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3348]

Agencies SHOULD use unique certificates for both devices and users accessing a wireless network.

18.2.11.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3350]

Certificates for users accessing wireless networks SHOULD be issued on smart cards with access PINs and not stored with a device when not in use.

18.2.11.C.05. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3351]

Certificates stored on devices accessing wireless networks SHOULD be protected by implementing full disk encryption on the devices.

Using commercial certification authorities for certificate generation

18.2.12.R.01. **Rationale**

A security risk exists with EAP-TTLS and PEAP when a commercial certificate authority's certificates are automatically trusted by devices using vendor trusted certificate stores. This trust can be exploited by obtaining certificates from a commercial certificate authority under false pretences, as devices can be tricked into trusting their signed certificate. This will allow the capture of authentication credentials presented by devices, which in the case of EAP-MSCHAPv2 can be cracked using a brute force attack granting not only network access but most likely Active Directory credentials as well.
To reduce this risk, devices can be configured to:

- validate the server certificate;
- disable any trust for certificates generated by commercial certificate authorities that are not trusted;
- disable the ability to prompt users to authorise net servers or commercial certificate authorities; and
- set devices to enable identity privacy to prevent usernames being sent prior to being authenticated by the RADIUS server.

18.2.12.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3354]

Devices MUST be configured to validate the server certificate, disable any trust for certificates generated by commercial certificate authorities that are not trusted and disable the ability to prompt users to authorise new servers or commercial certification authorities.

18.2.12.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3355]

Devices SHOULD be set to enable identity privacy.

Caching 802.1X authentication outcomes

18.2.13.R.01. **Rationale**

When 802.1X authentication is used, a shared secret key known as the Pairwise Master Key (PMK) is generated. Upon successful authentication of a device, the PMK can be cached to assist with fast roaming between wireless access points. When a device roams away from a wireless access point that it has authenticated to, it will not need to perform a full re-authentication should it roam back while the cached PMK remains valid. To further assist with roaming, wireless access points can be configured to pre-authenticate a device to other neighbouring wireless access points that the device might roam to. Although requiring full authentication for a device each time it roams between wireless access points is ideal, agencies can chose to use PMK caching and pre-authentication if they have a business requirement for fast roaming. If PMK caching is used, the PMK caching period should not be set to greater than 1440 minutes (24 hours).

18.2.13.C.01. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:3358]

The PMK caching period SHOULD NOT be set to greater than 1440 minutes (24 hours).

Remote Authentication Dial-In User Service (RADIUS) authentication

18.2.14.R.01. **Rationale**

The RADIUS authentication process that occurs between wireless access points and the RADIUS server is distinct and a separate to the 802.1X authentication process. During the initial configuration of wireless networks using 802.1X authentication, a shared secret is entered into either the wireless access points or the RADIUS server. If configured on the wireless access points, the shared secret is sent to the RADIUS server via the RADIUS protocol, and vice versa if configured on the RADIUS server. This shared secret is used for both RADIUS authentication and confidentiality of RADIUS traffic.

18.2.14.R.02. **Rationale**

An intruder that is able to gain access to the RADIUS traffic sent between wireless access points and the RADIUS server may be able to perform a brute force or an off-line dictionary attack to recover the shared secret. This in turn allows the intruder to decrypt all communications between wireless access points and the RADIUS server. To mitigate this security risk, communications between wireless access points and a RADIUS server must be encapsulated with an additional layer of encryption using an appropriate encryption product (See Chapter 17 – Cryptography).

18.2.14.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3362]

Communications between wireless access points and a RADIUS server MUST be encapsulated with an additional layer of encryption using an approved encryption product (See Chapter 17 – Cryptography).

Encryption

18.2.15.R.01. **Rationale**

As wireless transmissions are capable of radiating outside of secure areas into unsecure areas they need to be encrypted to the same level as classified information communicated over cabled infrastructure in unsecure areas.

18.2.15.C.01.

Control System Classifications(s): All Classifications; Compliance: Must [CID:3365]

Agencies using wireless networks MUST ensure that classified information is protected by cryptography that meets the assurance level mandated for the communication of information over unclassified network infrastructure (See Section 17.2, Suite B).

Cipher Block Chaining Message Authentication Code Protocol (CCMP) Encryption

18.2.16.R.01. **Rationale**

As wireless transmissions are capable of radiating outside of secure areas, agencies cannot rely on the traditional approach of physical security to protect against unauthorised access to sensitive or classified information on wireless networks. Using the AES based Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) helps protect the confidentiality and integrity of all wireless network traffic.

18.2.16.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3368]

CCMP MUST be used to protect the confidentiality and integrity of all wireless network traffic.

Temporal Key Integrity Protocol (TKIP) and Wireless Encryption Protocol (WEP)

18.2.17.R.01. **Rationale**

CCMP was introduced in WPA2 to address feasible attacks against the Temporal Integrity Key Protocol (TKIP) used by the Wi-Fi Protected Access (WPA) protocol as well as the original Wireless Encryption Protocol (WEP). A malicious actor seeking to exploit vulnerabilities in TKIP and WEP can attempt to connect to wireless access points using one of these protocols. By default, wireless access points will attempt to accommodate this request by falling back to a legacy protocol that the device supports. Disabling or removing TKIP and WEP support from wireless access points ensures that wireless access points do not fall back to an insecure encryption protocol.

18.2.17.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3373]

TKIP and WEP support MUST be disabled or removed from wireless access points.

Wired Equivalent Privacy (WEP)

18.2.18.R.01. **Rationale**

WEP has serious flaws which allow it to be trivially compromised. A WEP network should be considered equivalent to an unprotected network.

18.2.18.C.01. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:3379]

Agencies MUST NOT use WEP for wireless deployments.

Wi-Fi Protected Access (WPA)

18.2.19.R.01. **Rationale**

As wireless networks are often capable of being accessed from outside the perimeter of secured spaces, all wireless network traffic requires suitable cryptographic protection. For this purpose, it is recommended that Wi-Fi Protected Access 3 (WPA3) be used as it provides equivalent or greater security than its predecessor Wi-Fi Protected Access 2 (WPA2).

WPA3 has also prohibited the use of various outdated and insecure cipher suites. WPA3-Enterprise supports three enterprise modes of operation: enterprise only mode, transition mode and 192-bit mode. Preference is given to WPA3-Enterprise 192-bit mode as this mode ensures no algorithms with known weaknesses are used.

18.2.19.C.01. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:7539]

Agencies MUST NOT use Wi-Fi Protected Access (WPA) for wireless deployments.

18.2.19.C.02. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:3386]

Agencies SHOULD NOT use Wi-Fi Protected Access 2 (WPA2) for wireless deployments.

18.2.19.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7540]

Agencies SHOULD use Wi-Fi Protected Access 3 (WPA3) for wireless deployments with preference given to WPA3-Enterprise 192-bit mode.

Pre-shared keys

18.2.20.R.01. **Rationale**

The use of pre-shared keys is poor practice and not recommended for wireless authentication, in common with many authentication and encryption

mechanisms, the greater the length of pre-shared keys the greater the security they provide.

18.2.20.C.01. **Control System Classifications(s): Confidential, Secret, Top Secret; Compliance: Must Not** [CID:3391]

Agencies MUST NOT use pre-shared keys for wireless authentication.

18.2.20.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3392]

If pre-shared keys are used, agencies SHOULD use random keys of the maximum allowable length.

18.2.20.C.03. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:3393]

Agencies SHOULD NOT use pre-shared keys for wireless authentication.

Administrative interfaces for wireless access points

18.2.21.R.01. **Rationale**

Administrative interfaces may allow users to modify the configuration and security settings of wireless access points. Often wireless access points by default allow users to access the administrative interface over methods such as fixed network connections, wireless network connections and serial connections directly on the device. Disabling the administrative interface on wireless access points will prevent unauthorised connections.

18.2.21.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3397]

Agencies SHOULD disable the administrative interface on wireless access points for wireless connections.

Protecting management frames on wireless networks

18.2.22.R.01. **Rationale**

Effective DoS attacks can be performed on the 802.11 protocol by exploiting unprotected management frames using inexpensive commercial hardware. WPA2 provides no protection for management frames and therefore does not prevent spoofing or DoS attacks. Note, in WPA3 this feature is built into the standard.

18.2.22.R.02. **Rationale**

The current release of the 802.11 standard provides no protection for management frames and therefore does not prevent spoofing or DoS attacks.

18.2.22.R.03. **Rationale**

However, 802.11w was ratified in 2009 and specifically addresses the protection of management frames on wireless networks. Wireless access points and devices should be upgraded to support the 802.11w amendment or any later amendment or version that includes a capability for the protection of management frames.

18.2.22.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3408]

Wireless access points and devices SHOULD be upgraded to support a minimum of the 802.11w amendment.

Default service set identifiers (SSIDs)

18.2.23.R.01. **Rationale**

All wireless access points are configured with a default Service Set Identifier (SSID). The SSID is commonly used to identify the name of a wireless network to users. As the default SSIDs of wireless access points are well documented on online forums, along with default accounts and passwords, it is important to change the default SSID and default passwords of wireless access points.

18.2.23.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3416]

Agencies MUST change the default SSID of wireless access points.

18.2.23.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3418]

Agencies MUST rename or remove default accounts and passwords.

Changing the SSID

18.2.24.R.01. **Rationale**

When changing the default SSID, it is important that it lowers the profile of an agency's wireless network. In doing so, the SSID of a wireless network should not be readily associated with an agency, the location of or within their premises, or the functionality of the network.

18.2.24.R.02. **Rationale**

This procedure applies to all wireless network assets owned/or managed by the agency, including any guest or other publicly accessible networks.

18.2.24.C.01. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:3505]

The SSID of a wireless network SHOULD NOT be readily associated with an agency, the premises, location or the functionality of the network.

SSID Broadcasting

18.2.25.R.01. **Rationale**

A common method to lower the profile of wireless networks is disabling SSID broadcasting. While this ensures that the existence of wireless networks are not broadcast overtly using beacon frames, the SSID is still broadcast in probe requests, probe responses, association requests and re-association requests for the network. Malicious actors can determine the SSID of wireless networks by capturing these requests and responses. By disabling SSID broadcasting agencies will make it more difficult for legitimate users to connect to wireless networks as legacy operating systems have only limited support for hidden SSIDs. Disabling SSID broadcasting infringes the design of the 802.11x standards.

18.2.25.R.02. **Rationale**

A further risk exists where an intruder can configure a wireless access point to broadcast the same SSID as the hidden SSID used by a legitimate wireless network. In this scenario devices will automatically connect to the wireless access point that is broadcasting the SSID they are configured to use before probing for a wireless access point that accepts the hidden SSID. Once the device is connected to the intruder's wireless access point the intruder can steal authentication credentials from the device to perform an adversary-in-the-middle attack to capture legitimate wireless network traffic or to later reuse to gain access to the legitimate wireless network.

18.2.25.R.03. **Rationale**

Disabling SSID broadcasting is not considered to be an effective control and may introduce additional risks.

18.2.25.C.01. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:3514]

Agencies SHOULD NOT disable SSID broadcasting on wireless networks.

Static addressing

18.2.26.R.01. **Rationale**

Rogue devices or Access Points (APs) are unauthorised Wireless Access Points operating outside of the control of an agency. Assigning static IP addresses for devices accessing wireless networks can prevent a rogue device when connecting to a network from being assigned a routable IP address. However, some malicious actors will be able to determine IP addresses of legitimate users and use this information to guess or spoof valid IP address ranges for wireless networks. Configuring devices to use static IP addresses introduces a management overhead without any tangible security benefit.

18.2.26.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3520]

Agencies SHOULD use the Dynamic Host Configuration Protocol (DHCP) for assigning IP addresses on wireless networks.

Media Access Control address filtering

18.2.27.R.01. **Rationale**

Devices that connect to wireless networks have a unique Media Access Control (MAC) address. It is possible to use MAC address filtering on wireless access points to restrict which devices can connect to wireless networks. While this approach will introduce a management overhead of configuring allow lists of approved MAC addresses, it can prevent rogue devices from connecting to wireless networks. However, some malicious actors will be able to determine valid MAC addresses of legitimate users already on wireless networks and use this information to spoof valid MAC addresses and gain access to a network. MAC address filtering introduces a management overhead without any real tangible security benefit.

18.2.27.C.01. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:3529]

MAC address filtering SHOULD NOT be used as a security mechanism to restrict which devices connect to a wireless network.

Documentation

18.2.28.R.01. **Rationale**

Wireless device driver and WAP vulnerabilities are very exposed to the threat environment and require specific attention as exploits can gain immediate unauthorised access to the network.

18.2.28.C.01.

Control System Classifications(s): All Classifications; Compliance: Should [CID:3533]

Key generation, distribution and rekeying procedures SHOULD be documented in the SecPlan for the wireless network.

18.2.28.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3534]

Wireless device drivers and their versions SHOULD be documented in the SecPlan for the wireless network.

Non-agency devices connecting to agency controlled wireless networks

18.2.29.R.01. **Rationale**

As agencies have no control over the security of non-agency devices or knowledge of the security posture of such devices, allowing them to connect to agency controlled wireless networks poses a serious threat. Of particular concern is that non-agency devices may be infected with viruses, malware or other malicious code that could crossover onto the agency network. Furthermore, any non-agency devices connecting to agency controlled wireless networks will take on the classification of the network and will need to be appropriately sanitised and declassified before being released back to their owners.

18.2.29.R.02. **Rationale**

The practice of Bring Your Own Device (BYOD) is becoming more widespread but introduces a significant number of additional risks to agency systems. Refer to Section 21.4 for guidance on the use of BYOD.

18.2.29.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3583]

Where BYOD has been approved by an agency, any wireless network allowing BYOD connections MUST be segregated from all other agency networks, including any agency wireless networks.

18.2.29.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3586]

Any BYOD devices MUST comply with the policies and configuration described in Section 21.4– BYOD.

18.2.29.C.03. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:3588]

Agencies MUST NOT allow non-agency devices to connect to agency controlled wireless networks not intended or configured for BYOD devices or for public access.

Agency devices connecting to non-agency controlled wireless networks

18.2.30.R.01. **Rationale**

When agency devices connect to non-agency controlled wireless networks, particularly public wireless networks, the devices may be exposed to viruses, malware or other malicious code.

18.2.30.R.02. **Rationale**

If any agency device becomes infected and is later connected to an agency controlled wireless network then a crossover of viruses, malware or malicious code could occur.

18.2.30.C.01. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:3600]

Agencies SHOULD NOT allow agency devices to connect to non-agency controlled wireless networks.

Connecting wireless networks to fixed networks

18.2.31.R.01. **Rationale**

When an agency has a business requirement to connect a wireless network to a fixed network, it is important that they consider the security risks. While fixed networks can be designed with a certain degree of physical security, wireless networks are often easily accessible outside of the agency's controlled area. Treating connections between wireless networks and fixed networks in the same way agencies would treat connections between fixed networks and the Internet can help protect against an intrusion originating from a wireless network against a fixed network. For example, agencies can implement a gateway to inspect and control the flow of information between the two networks.

18.2.31.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3609]

Connections between wireless networks and fixed networks SHOULD be treated in the same way as connections between fixed networks and the Internet.

Wireless network footprint and Radio Frequency (RF) Controls

18.2.32.R.01. **Rationale**

Minimising the output power of wireless access points will reduce the footprint of wireless networks. Instead of deploying a small number of wireless access points that broadcast on high power, more wireless access points that use minimal broadcast power should be deployed to achieve the desired wireless network footprint. This has the added benefit of providing redundancy for a wireless network should a wireless access point become unserviceable. In such a case, the output power of other wireless access points can be temporarily increased to cover the footprint gap until the unserviceable wireless access point can be replaced.

18.2.32.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3614]

Instead of deploying a small number of wireless access points that broadcast on high power, more wireless access points that use minimal broadcast power SHOULD be deployed to achieve the desired wireless network footprint.

Radio Frequency (RF) Propagation & Controls

18.2.33.R.01. **Rationale**

An additional method to limit a wireless network's footprint is through the use of radio frequency (RF) shielding on an agency's premises. While expensive, this will limit the wireless communications to areas under the control of an agency. RF shielding on an agency's premises has the added benefit of preventing the jamming of wireless networks from outside of the premises in which wireless networks are operating.

18.2.33.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3617]

The effective range of wireless communications outside an agency's area of control SHOULD be limited by:

- Minimising the output power level of wireless devices.
- Implementing RF shielding within buildings in which wireless networks are used.

Interference between wireless networks

18.2.34.R.01. **Rationale**

Where multiple wireless networks are deployed in close proximity, there is the potential for RF interference to adversely impact the availability of the network, especially when networks are operating on commonly used default channels of 1 and 11. This interference is also apparent where a large number of wireless networks are is use in close proximity to the agency's premises.

18.2.34.R.02. **Rationale**

Sufficiently separating wireless networks through the use of channel separation can help reduce this risk. This can be achieved by using wireless networks that are configured to operate with at least one channel separation. For example, channels 1, 3 and 5 could be used to separate three wireless networks.

18.2.34.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3621]

Wireless networks SHOULD use channel separation.