GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO 2100.2C
3/11/2021

GSA ORDER

SUBJECT: GSA Wireless Local Area Network (WLAN) Security

1. Purpose. This Order sets forth the General Services Administration's (GSA) policy on securing Wireless Local Area Networks (WLANs). This Order is based on industry best practices in securing wireless networks including Institute of Electrical and Electronics Engineers (IEEE) 802.11, an evolving family of specifications for WLANs (such as in a home or other building). This Order applies to the entire 802.11 family of WLANs.

2. Background.

a. Legacy WLANs were inherently insecure. Wired Equivalent Privacy encryption can be broken in as little as 10 minutes regardless of the key length. Media Access Control address filtering is used as a method of authentication whose address traverses the airwaves in clear text and has also been shown to be vulnerable. Although these methods will slow the casual attacker, they are not adequate to secure the enterprise network. Wi-Fi Protected Access (WPA) was also shown to be insecure due to the limitations of the message integrity code hash function.

b. To ensure risk is minimized to the agency's internal network using legacy wireless devices, securing of the network must be accomplished by implementing the wireless network outside the agency's firewall, and/or by using Virtual Private Network technology that includes user authentication. Further information on wireless security can be found at "NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs)."

c. The IEEE approved specification 802.11i for wireless security in 2004, and has continued to update it in order to further increase the security of WLANs. 802.11i significantly increases the security of WLANs through the use of Advanced Encryption Standard (AES) for encryption and Extensible Authentication Protocol (EAP) for user authentication (referencing 802.1X). This technology has been standardized as WPA by

the Wi-Fi Alliance. GSA currently employs WPA2. WPA3 was released in January, 2018; however, GSA has yet to implement this technology due to the age of our current infrastructure and the cost required to upgrade. Furthermore, WPA2 has not yet been shown to be vulnerable to attack. Thus, WPA3 will be considered as infrastructure upgrades allow; until then WPA2 will continue to be the deployed security standard.

3. Cancellation. This Order cancels and supersedes CIO P 2100.2B GSA Wireless Local Area Network (LAN) Security, dated May 8, 2014.

4. Objective. The objective of this policy is to ensure that GSA WLANs minimize the risk of unauthorized users gaining access to GSA information or information technology (IT) resources through Wi-Fi connectivity.

5. Applicability.

a. This policy applies to GSA Federal employees and authorized users of IT in GSA's Services, Staff Offices, and Regions. Authorized users include all employees of GSA and other Government organizations who are supported by GSA, including those contractors, consultants, or other third parties who are specifically granted access to conduct business on behalf of or with GSA or other Government organizations supported by GSA.

b. Contracting Officers must include compliance with this policy in the Statement of Work for contract employees.

c. This policy applies to the Office of Inspector General (OIG) to the extent that the OIG determines it is consistent with the OIG's independent authority under the IG Act and does not conflict with other OIG policies or the OIG mission. This policy applies to the Civilian Board of Contract Appeals (CBCA) only to the extent that the CBCA determines it is consistent with the CBCA's independent authority under the Contract Disputes Act and does not conflict with other CBCA policies or the CBCA mission.

6. Policy.

a. All WLANs providing access to GSA enterprise resources must meet 802.11i requirements, as specified in 802.11-2016, for encryption using the Counter Mode with CBC-MAC (CCMP) protocol and AES as its encryption algorithm. In addition, it must use 802.1X port-based network access control for authorization and authentication (EAP).

(1) The minimum EAP authentication mechanism that must be used is Protected EAP (PEAP- MSCHAPv2). This passes MSCHAPv2 inside a Transport Layer Security (TLS) tunnel.

(2) It must also provide mutual authentication of the client and the authentication server.

(3) The implementation shall use the Federal Information Processing Standards (FIPS) 140-2 or FIPS 140-3 certified products to the greatest extent possible. Exceptions must be approved by the Information Systems Security Manager (ISSM -ISSM.Team@gsa.gov).

(4) EAP-TLS is also approved for use and is the preferred method of authentication. However, due to the client-side certificate required by EAP-TLS, it has yet to be used in GSA.

b. All GSA mesh connections (access points which do not have wired uplinks), such as building-to-building connectivity, shall use a minimum of 256 bit AES encryption.

c. All wireless remote access into the GSA network from hotel networks, home wireless networks, wireless hotspots, and similar, must use either the VPN client application or Virtual Desktop Interface to connect to and properly access the GSA network. Resources that are secured through web encryption, such as Google or Salesforce, can be accessed via their single sign-on infrastructure.

d. Dual connections are not allowed when connected to the network. Clients can connect *either* via Wi-Fi or a network cable - not both. GSA laptops are configured this way via group policy. Other devices (such as printers, servers, and Internet-of-things devices) need to be manually configured to be in compliance.

e. WLAN infrastructure devices, such as access points (APs) and Wireless LAN Controllers, may only be installed by network or security personnel and in locations approved by the appropriate Authorizing Official (AO). They must be placed in an isolated, controlled-access location and must use security hardening procedures from the following sources in order of preference:

(1) GSA technical guidelines;

(2) National Institute of Standards and Technology guidelines; and

(3) Industry best practice guidelines.

f. AP administrative traffic must be limited to the wired network interface to the greatest extent possible. Mesh WLANs are an example of an exception. Exceptions must be approved by ISSM by contacting ISSM.Team@gsa.gov.

g. Any suspected incident or compromise of a wireless device must be reported to the IT Service Desk or the appropriate Information Systems Security Officer (ISSO) (https://insite.gsa.gov/employee-resources/information-technology/security-and-privacy/it-security/report-it-security-incidents-and-suspicious-activity-immediately) as soon as possible. The ISSO will follow normal incident handling procedures.

h. Authorizing Officials (AOs) will ensure their LANs are scanned for unauthorized and unsecured WLAN devices quarterly. Contact the Information Systems Security Manager (ISSM - ISSM.Team@gsa.gov) for guidance on compliance.

i. Only GSA-owned and managed devices and GSA-furnished or Bring Your Own Device-approved devices, such as smartphones and tablets, are allowed to connect to the GSA enterprise WLAN. All other devices should connect to either the GSA Guest WLAN or to a public internet connection, such as a cellular internet provider or other public Wi-Fi network.

j. For Building Monitoring and Controls Systems, all wireless devices must be pre-approved by the Buildings Technology Services Division (BuildingsTechnologyServicesDivision@gsa.gov) prior to award. FIPS 140-2 or better is required for all wireless communication devices (FIPS 140-2 specifies 256 bit AES encryption). For details see the latest version of the Building Technologies Technical Reference Guide.

7. Nature of Revision.

a. Outdated references were removed or modified to reflect GSA IT's current approach; and

b. Updates were made to reflect current industry standards and modifications within GSA IT's own approach to Wi-Fi, including updating links to relevant web pages.

8. Deviations. All deviations from this policy shall be documented and approved by the appropriate AO with a copy of the approval forwarded to the Office of the Chief Information Security Officer.

9. Signature.

_____/S/_____
DAVID SHIVE
Chief Information Officer
Office of the Chief Information Officer