United States Department of Agriculture
Marketing and Regulatory Programs
Grain Inspection, Packers and Stockyards Administration

Directive GIPSA 3140.5 11/30/06

WIRELESS LOCAL AREA NETWORK (WLAN) IMPLEMENTATION

1. PURPOSE

This Directive defines the security requirements for Wireless Local Area Network (WLAN) implementation. WLAN equipment includes but is not limited to: hubs, routers, switches, workstations, and servers.

2. REPLACEMENT HIGHLIGHTS

This Directive replaces GIPSA Directive 3140.5, dated 6/8/05.

3. REFERENCES

a. Office of Management and Budget (OMB) Circular A-130, Security of Federal Automated Information Resources, Appendix III.

b. Public Law 100-235, Computer Security Act of 1987.

c. National Institute of Standards and Technology (NIST) Special Publication, 800-48, Wireless Network Security.

d. The Privacy Act of 1974.

e. Federal Information Processing Standard Publication 140-2, Security Requirements for Cryptographic Modules.

f. OMB Memorandum M06-16 (Clay Johnson memo).

g. U.S. Department of Agriculture, Office of the Chief Information Officer Memorandum, dated 7/13/2006 (Lynn Allen memo).

4. BACKGROUND

Wireless devices and technology save countless hours and have changed the way in which many Federal agencies do business. These devices make staying in touch easy, offer flexibility and portability, can offer dramatic cost savings, and interact easily with other computer resources.

However, as a group, they represent serious security threats to the U.S. Department of Agriculture (USDA) agencies and staff offices. Transmissions using wireless devices are unprotected; sensitive information could be compromised, malware could be spread, or these devices could be used as a back door to the GIPSA or USDA networks. Wireless networks have all of the vulnerabilities of wired networks and introduce new technology "risks." The airwave medium for these networks makes the loss of confidentiality, integrity, and denial of services attacks easier than ever before.

5. POLICY

a. All GIPSA facilities will follow the Agency approach for the implementation of WLAN. Staff offices wishing to use WLAN must coordinate with the GIPSA Information Technology (IT) staff first; there are no exceptions. This strategy will consider recommendations contained in the:

(1) TSAC USDA Wireless Strategy Report, dated March 2003,

(2) NIST Interagency Report 6981, dated April 2003, and

(3) Special Publication 800-48, Wireless Network Security.

b. All GIPSA facilities will follow policy guidance from **CS-034** Cyber Security Guidance Regarding Portable Electronic Devices (PED) and Wireless Technologies.

c. All implementations of wireless technology require that a formal risk assessment be conducted in the environment where this technology will operate prior to deployment of the WLAN.

d. Staff offices will plan and execute measures to safeguard their systems and lower security risks to a manageable level using the Procedures in this Directive, and Checklists provided by the USDA Cyber Security Office.

e. Strong encryption and authentication techniques will be used in the transmission and storage of sensitive information. All GIPSA WLAN implementation will use the assumption that sensitive but unclassified (SBU) data is being transmitted.

f. The GIPSA IT Staff will be responsible for the development of a formal Wireless Plan that documents use of this technology and planned implementations. Elements of this plan will also be documented and submitted to the Agency Information Systems Security Program Manager (ISSPM) for the Overall Agency Security Plan, including funding levels and countermeasures employed.

6. PROCEDURES

All GIPSA facilities will follow the procedures below for use of wireless connectivity.

a. Internal GIPSA Wireless Connectivity (WLAN).

(1) GIPSA internal wireless networks will only be accessed by GIPSA purchased and approved equipment—no personal/non-GIPSA equipment will be used in any wireless connectivity including both networked and non-networked GIPSA equipment, and any GIPSA supplied access point. To ensure a secure internal environment these devices will be locked down at the Media Access Control (MAC) address level.

(2) Additions/modifications to MAC addresses will be accomplished via the GIPSA Network Account Management procedures and must include a Network User Modification Form.

(3) WLAN devices will be configured to a specific use. In addition, WLAN connectivity devices will only be configured for access by a GIPSA IT Network Administrator. Any unauthorized connectivity to any GIPSA wireless device is strictly prohibited.

(4) GIPSA IT will grant WLAN connectivity only for specific machines, specific purposes, and/or at specific times, through single points of access only (i.e., no ‘roaming’ configurations).

(5) USDA, Office of Cyber Security, requires all agencies and staff offices to conduct wireless technology risk assessments and complete the appropriate checklists found in **CS-034,** Cyber Security Guidance Regarding Portable Electronic Devices (PED) and Wireless Technology to assess the security posture and countermeasures necessary to ensure all security requirements are satisfied. The risk assessment and checklists must be completed by the wireless requester prior to any wireless implementation.

b. External wireless connectivity to the GIPSA WAN.

GIPSA allows wireless laptop connectivity to the GIPSA network, using non-GIPSA wireless connections (such as hotels, or home wireless networks), with the following stipulations:

(1) GIPSA users will use the connection for GIPSA business ONLY.

(2) A secure, encrypted connection must be used to reduce the risk of unauthorized monitoring of data (GIPSA currently uses VPN encryption for all of its remote connections to the GIPSA WAN). GIPSA laptop users are strictly forbidden to connect a GIPSA laptop to a non-GIPSA connection without the use of VPN.

(3) Full connection to the GIPSA LAN (including log in and network drives) is required for all wireless connectivity using GIPSA computers. On a very limited basis, users may connect a GIPSA laptop to a wireless connection without fully connecting (logging in) to the GIPSA network. However, all GIPSA laptops must be connected fully to the network on a regular basis to ensure that automatic patching, updates, and anti-virus requirements are fulfilled.

7. RESPONSIBILITIES

a. Agency Management and the Chief Information Officer will:

(1) Implement applications of WLAN in accordance with policy and procedures;

(2) Ensure that Agency guidelines are developed, implemented, and followed to include requirements for technology plans, risk assessments, and strict physical accountability;

(3) Require that the appropriate Wireless Technology Checklist be completed prior to installations, strict security controls be employed, and standardized configurations be established and monitored;

(4) Ensure that encryption, authentication, and VPN Technology are employed, where appropriate;

b. The Agency Information Systems Security Program Manager (ISSPM) will:

(1) Coordinate and manage the security control required for WLAN;

(2) Assist Agency managers in completing the appropriate checklists, as required;

(3) Routinely monitor Agency implementation of these devices and technology to ensure that policy and procedures are followed; advise Agency managers in cases of lax security controls or improper use;

(4) Ensure the completion of the development of technology implementation plans; and

(5) Update the Overall Agency Security Plan to reflect the funding and planned implementation of WLAN.

c. The Agency Systems or Network Administrators will:

(1) Provide appropriate administrative access and permissions for WLAN based job requirements;

(2) Install encryption, VPN Technology, and require strong authentication for these devices. All GIPSA WLAN implementations will be considered to be handling SBU data and all instances will be configured as SBU;

(3) Install standardized configurations, strict security features, profiles, and disable modems;

(4) Verify appropriate security controls are in place using the appropriate checklists.

8. EXCEPTIONS

There are no exceptions to this policy.

9. COMPLIANCE AND SANCTIONS

All Federal personnel who work with GIPSA Information System resources are individually and personally responsible for applying the appropriate security measures and for complying with Federal, USDA, and GIPSA policies and procedures on the subject. Willful failure to comply may result in punishment, including dismissal, under the Computer Fraud and Abuse Act and other appropriate Federal statutes.

10. INQUIRIES

a. Direct inquiries or requests for changes to this policy to the GIPSA ISSPM at (202) 690-0044.

b. This Directive is available on the Internet at ***http://www.aphis.usda.gov/library/gipsa/GIPSA.html***

/s/
James E. Link
Administrator