



United States
Department of
Agriculture

Office of the Chief
Information Officer

1400 Independence
Avenue SW

Washington, DC
20250

MAY 16 2008

TO: Agency Administrators
Agency Deputy Administrators
Chief Information Officers

FROM: Charles R. Christopherson
Chief Financial and Information Officer

SUBJECT: Wireless Network Security

**THIS MEMORANDUM SERVES AS A FINAL REMINDER OF THE STRICT
POLICIES AND REQUIREMENTS FOR WIRELESS ACCESS.**

The Office of the Chief Information Officer (OCIO) enthusiastically supports wireless networks that are configured correctly and are in full compliance with the requirements of the Department policy. Wireless networks that are configured correctly are secure and provide an economical solution to providing physical cabling to office buildings.

Wireless networks that do not comply with the Department wireless policies are considered to be a high risk to the network security of the Federal government. Improper management of wireless devices can allow employees, contractors, and outside individuals to quickly damage critical applications or capture sensitive information. Over the last six months, I have communicated to the agency Chief Information Officers that they have two core responsibilities. The first core responsibility is to insure the safety and security of the Federal Government's network. The second core responsibility is the support of mission area applications that assist in the delivery of core program requirements. The wireless network access falls within the first core responsibility.

OIG Wireless Audit. The Office of the Inspector General recently reviewed with my office an audit of wireless networks in the Department. The results of the audit concluded that the majority of the wireless networks in the USDA agencies did not meet the Department's policy requirements. The report states that many of the wireless networks did not meet the encryption standards or the systems did not delete the default administrator password. Not meeting the Department's policy for wireless networks put the USDA network and the agency network at a high risk of compromise.

OCIO Wireless Audits. The audit was also critical of the OCIO for not auditing the agency's wireless networks for compliance. While the first responsibility for the local office network currently resides with the agency CIOs, the Department's Office of the Chief Information Officer does have a responsibility to verify that the agencies are following the Department's policies. Within the Department policy, the Office of the Chief Information Officer (OCIO) is to audit the wireless networks for compliance. OCIO will allow the agencies 30 days from the date of this memorandum to communicate and comply with the Department's wireless policy. At that date, OCIO will begin random wireless audits without prior notification to the agencies.

Non-Compliance Equipment. While we expect that all wireless devices are in full compliance with Department policy, if wireless network equipment is found that is not meeting the Department policy, whether audited by the Office of the Inspector General or the Office of the Chief Information Officer; it will be promptly removed and the violation documented. The wireless equipment and a copy of the violation information are to be properly packaged and promptly delivered to the OCIO Cyber Security Policy Office in Washington, DC to mitigate the security risk.

Technology Management Personnel. The network administrator and/or other staff that did not comply with the Department policy for a wireless network device allowed a serious security weakness and network vulnerability for a Federal Government's network. The employees and managers that allowed the risk are to have their network access promptly cancelled and removed until the appropriate training can be completed for network management, wireless security, USDA policy, and Federal Government cyber security issues. Network access can once again be reestablished once the employee completes this training. This class will be available in Washington, DC at the Office of the Chief Information Officer.

OCIO fully supports the economies and flexibilities that are generated by a properly configured and documented wireless networks. We ask that all agency Administrators read this memorandum with their management teams including their agency CIOs. Agency CIOs need to read the Department policy very carefully to insure that they are in full compliance with all policy requirements. Wireless policies are attached to this document for your convenience.

Securing the Federal Government's network is very important. We appreciate your support in minimizing risk of unauthorized network access.