U.S. Department of Energy
Office of Inspector General
Office of Audit Services

Audit Report

Security Over Wireless Networking Technologies

DOE/IG-0617

August 2003

Department of Energy
Washington, DC 20585

August 25, 2003

MEMORANDUM FOR THE SECRETARY

FROM: Greg Friedman
Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report on "Security Over Wireless Networking Technologies"

BACKGROUND

An increasing number of the Department of Energy's organizations are using wireless communications devices and networks. Such technologies enable the transmission of data without physical connection using radio frequency. Wireless technologies range from such complex systems as wireless local area networks, cell phones, and personal digital assistants to relatively simple devices that do not process or store information, such as wireless headphones, and microphones.

The trend toward wireless technology has many benefits, primarily in terms of operating efficiencies and effectiveness. However, the technology carries with it certain security implications which need to be addressed, especially when dealing with sensitive information. In fact, the National Institute of Standards and Technology (NIST) reports that risks in wireless networks are equal to the sum of the risk of operating a wired network plus the new risks presented by weaknesses in wireless protocols. As such, NIST recommends specific strategies to mitigate risks as wireless technologies are integrated into computing environments. We initiated this audit to determine whether the Department had taken actions to reduce the risks associated with its wireless networks.

RESULTS OF AUDIT

Four of six Department organizations we reviewed that had deployed wireless networks did so without assessing the risks associated with their use. We noted that most sites did not routinely implement or test the effectiveness of wireless security measures and that organizations had not focused sufficient attention on properly securing wireless networks or preventing the unauthorized use of such devices. In particular, they had not developed specific guidance or configuration management policies outlining approval, security, and wireless connection requirements. Lack of attention to wireless security placed the Department's information systems at risk of attack from internal and external sources and could ultimately result in the compromise of critical systems and information.

The Department has initiated an effort to require specific security actions regarding wireless devices. For example, management has drafted and circulated for comment specific policy for the use of wireless technologies and devices throughout the Department. Also, various organizations have procured and are piloting the use of certain wireless security tools. Despite these positive steps, we concluded that more needs to be done if the Department is to have in place a comprehensive wireless security strategy consistent with the *President's Management Agenda's* initiative regarding the use of information technology to improve Government operations. Consequently, we recommended a number of additional actions that should help improve the security and effectiveness of wireless technology.

Recently, the Secretary of Energy's Office of Independent Oversight and Performance Assurance completed a study of the use of wireless networking technologies at the Department. That study disclosed a number of concerns associated with the use of wireless networking technologies that parallel the findings in our report.

Due to security considerations, we have deleted from this report information that would identify specific programs and organizations reviewed as part of the audit. Cognizant officials were provided information on specific vulnerabilities identified during our audit fieldwork.

MANAGEMENT REACTION

Management agreed with our recommendations and noted that the Department's proposed policy "Cyber Security Requirements for Wireless Devices and Information Systems" will address many of our recommendations.

Management's comments are included as Appendix 3.

Attachment

cc: Deputy Secretary
Administrator, National Nuclear Security Administration
Under Secretary for Energy, Science and Environment
Assistant Secretary for Environmental Management
Chief Information Officer
Director, Office of Science

SECURITY OVER WIRELESS NETWORKING TECHNOLOGIES

TABLE OF CONTENTS

Mitigating the Risk of Wireless Networks

Appendices

Wireless Security

We evaluated wireless security strategies at 10 Department of Energy (Department) organizations. Six of the organizations we reviewed had implemented wireless networks without adequate protective measures. The remaining four sites reported that they did not permit wireless networks but had not taken periodic action to determine whether unauthorized connections existed. The sites reviewed also did not routinely implement or test the effectiveness of existing wireless protective measures.

Deployment and Access Issues

Department of Energy Order 205.1 (DOE O 205.1) requires that organizations have a program in place to test and evaluate security controls to ensure their continued effectiveness in the face of evolving risk. In addition, the National Institute of Standards and Technology (NIST) urges agencies to be aware that maintaining a secure wireless network is a continual process that requires more effort than that required for other networks and systems.

At six of the organizations we reviewed, we observed that wireless networks had been deployed and were an integral part of the site's business or operational network. Users were permitted, through the use of wireless access points, to access resources normally available only through their standard or "wired" network connection. While officials at some of these sites indicated that they had implemented protective measures such as encryption and authentication, they did not routinely test or scan wireless systems to determine the effectiveness of those measures – a routine and essential practice for "wired networks."

Sites stated, and performance testing by the Office of Independent Oversight and Performance Assurance (OA) confirmed, that a number of entities had installed and were operating unauthorized wireless devices. For example, at one site managed by the Office of Environmental Management, testing revealed that several wireless devices were transmitting data in an unencrypted "clear text" format that could be easily intercepted and read. Data such as passwords and user names – information that could permit access to a portion of a site network – could be readily discerned or decoded. At another site managed by the National Nuclear Security Administration, OA officials confirmed the existence of numerous unauthorized wireless devices. Additionally, site personnel determined that some unauthorized wireless devices were connected to operational networks.

Officials with three of the ten organizations we reviewed indicated that since they did not permit wireless devices there was no need to test for unauthorized use. A fourth site that did not permit wireless devices had started pilot testing for unauthorized connections. The remaining six organizations told us that they performed testing only on an ad hoc basis.

Security Plans and Risk Assessments

Despite Federal and Departmental requirements regarding risk mitigation strategies, four of the six sites we reviewed had implemented wireless networks without adequately considering associated risk factors. Specifically, only one had prepared and documented a risk assessment prior to installing wireless networks and none of the six had modified their cyber security program plan (CSPP). Some of the organizations did not consider the risk assessment to be a high priority and told us that they planned to perform it when they updated their CSPP. The CSPP is supposed to be updated when significant operational changes occur or at two-year intervals.

Management Focus and Resources

Department organizations had not focused sufficient attention on properly securing or preventing the unauthorized use of wireless devices. The sites we visited had not developed specific guidance or configuration management policies outlining approval, security, and wireless connection requirements. Officials at three of the sites believed that policy was unnecessary because they did not permit wireless. The rate of unauthorized use at other sites, however, demonstrates the need to specify connection and security policies. For the most part, organizations had also not developed sufficient site-specific guidance for areas such as device encryption or security capabilities, vulnerability testing, and required management approvals. It should be noted that DOE O 205.1, as recently issued, contains provisions requiring that risk management in security planning be addressed to include the use of wireless technology and personal electronic devices. The Office of Chief Information Officer (CIO) has also drafted additional policy specific to wireless devices requiring that the security of wireless technologies be implemented in a manner consistent with guidance by NIST.

Furthermore, the Department had not acquired the tools and training needed to address the wireless environment. Officials in the CIO stated that, unlike with the wired environment, the CIO had not taken action to acquire an enterprise license for a tool that would facilitate wireless vulnerability assessment. These officials indicated that they were evaluating the need for performance and vulnerability testing tools and may consider procuring and distributing them. Also, a CIO official at Headquarters indicated that the office lacked adequately trained personnel to perform wireless identification and vulnerability testing and that a configuration standard on which to base compliance had not been developed.

Unclassified Information Systems May Be At Risk

Inadequate protective measures exposed the Department's information and information systems to risk of attack from internal and external sources and could ultimately result in compromise of critical systems. Industry experts expect that 30 percent of enterprises will suffer serious security exposures from deploying wireless networks without implementing the proper security, and at least 20 percent of enterprises already have rogue wireless networks attached to their corporate networks. Within the Department, the compromise of a single wireless access point connected to an organization's business network could allow malicious users to access sensitive information residing on internal networks. Additionally, unauthorized users could exploit network vulnerabilities by launching a network attack on a third party (private party or other Government organization), thus exposing the Department to litigation.

RECOMMENDATIONS

To enhance overall security for wireless networks to unclassified information systems, we recommend that the Chief Information Officer, in coordination with the Administrator, National Nuclear Security Administration and the Under Secretary for Energy, Science and Environment:

1. Establish Department-wide requirements for wireless device and network implementation;

2. Enforce the requirement for organizations to perform documented risk assessments and to develop and implement protective measures commensurate with the assessed level of risk; and,

3. Require that wireless security be evaluated during the security self-assessments required by the Federal Information Security Management Act of 2003.

To correct the specific vulnerabilities noted in this report, we recommend that the Administrator, National Nuclear Security Administration, and the Under Secretary for Energy, Science and Environment require the offices and organizations within their responsibility to:

1. Develop and implement protective measures commensurate with the assessed level of risks of wireless networks, including evaluating and acquiring wireless security technical tools that enable effective testing and monitoring of wireless devices and networks against associated risk;

2. Amend Cyber Security Program Plans prior to introduction of wireless technologies into their computing environment if it significantly changes the operational risk; and,

3. Issue clear guidance for wireless security, tailored to the particular operating environment, consistent with NIST guidance.

MANAGEMENT REACTION

Management generally concurred with our recommendations and made a number of technical comments that have been reflected in the report. The text of management's comments is included as Appendix 3.

OBJECTIVE

To determine whether the Department had taken actions to mitigate the risks associated with wireless networks.

SCOPE

The audit was performed between September 2002 and May 2003. We assessed whether the Department had taken actions to mitigate the risks associated with wireless networks. Our work did not include a determination of whether vulnerabilities found were actually exploited and used to circumvent existing controls.

METHODOLOGY

To accomplish our objective, we:

- Reviewed Federal regulations such as the Office of Management and Budget (OMB) Circular A-130, Departmental Directives, and guidance pertaining to wireless security. Generally, OMB Circular A-130 requires that organizations assess the risk associated with emerging technologies prior to their deployment. DOE O 205.1 also requires each organization to implement a Cyber Security Program commensurate with risk and to document the results in a CSPP. Further, the NIST recommends that agencies perform a risk assessment and develop a security policy before introducing wireless technologies.

- Reviewed relevant reports issued by the Office of Inspector General, the General Accounting Office, and Office of Independent Oversight and Performance Assurance.

- Held discussions with officials and staff at various organizations.

- Assessed organizational security policy and planning documentation.

The audit was conducted in accordance with generally accepted Government auditing standards for performance audits and included tests of internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objectives. Specific performance standards were not established for the area of wireless implementation and, therefore, we could not assess how they might have been used to measure performance. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our audit. We did not rely on computer-processed data to accomplish our audit objective.

Management waived the exit conference.

PRIOR AUDIT REPORTS

- Special Report on *Management Challenges at the Department of Energy* (DOE/IG-0580, December 2002). One of the most serious challenges faced by the Department is Information Technology (IT) Management. With its substantial annual expenditure for IT, it is essential that the Department develop and implement an effective IT management investment and control process. IT investment and development and cyber protection have suffered in the past from program management planning and execution weaknesses. While the Department had taken a number of positive steps to improve its unclassified cyber security program, many of its critical information systems remained at risk. The report noted that the Department had not consistently implemented a risk-based cyber security approach or adequately addressed configuration management and access control problems.

- *The Federal Energy Regulatory Commission's Unclassified Cyber Security Program 2002* (DOE/IG-0569, September 2002). While the Federal Energy Regulatory Commission (Commission) had implemented a number of protective measures, certain critical information systems remained at risk. Cyber protection efforts suffered from program management, planning, and execution weaknesses. Specifically, the Commission had not developed system specific security plans; adequately planned for contingency and disaster recovery; implemented a completely effective cyber security-training program; or adequately addressed configuration management and access control problems.

- *Remote Access to Unclassified Information Systems* (DOE/IG-0568, September 2002). The majority of the offices reviewed had not adequately protected information systems from unauthorized remote access. Inadequate protective measures over remote access placed the Department's critical unclassified information systems at risk of data tampering, fraud, disruptions in critical operations, and inappropriate disclosure of sensitive or Privacy Act information. As reported, the Department needs to better enforce requirements for risk assessments, provide additional guidance for security implementation and evaluation, and establish performance measures related to remote access risk mitigation.

- *The Department's Unclassified Cyber Security Program 2002* (DOE/IG-0567, September 2002). While the Department had taken positive steps since the last review, many of its critical information systems were still at risk. Cyber protection efforts were hampered by weaknesses in program management, planning, and execution. The Department had not sufficiently strengthened its cyber security policy and guidance, implemented a cyber security performance measurement system, or established an effective self-assessment program. As a result, the critical systems were at risk of unauthorized or malicious use. Furthermore, the potential existed for compromise of sensitive operational and personnel-related data. Additional work in policy development and implementation is necessary to ensure that critical information technology resources are adequately protected.

- *Inspection of Cyber Security Standards for Sensitive Personal Information* (DOE/IG-0531, November 2001). The report concluded that the Department does not always meet the requirements of the Privacy Act of 1974, the Freedom of Information Act (FOIA), or the Computer Security Act of 1987 because the Department: (1) does not have a Department-wide baseline criteria for protecting Privacy Act/FOIA personal information; (2) does not group Privacy Act/FOIA personal information with other unclassified sensitive information for protection; and (3) allows individual sites and program offices to develop differing security measures for protection of Privacy Act/FOIA personal information.

- Special Report on *The Department of Energy's Implementation of the Clinger-Cohen Act of 1996* (DOE/IG-0507, June 2001). The report summarized 13 IT related Office of Inspector General reports. Cumulatively, these reports demonstrated systemic problems with the Department's approach to IT management and its method of addressing requirements of the Clinger-Cohen Act of 1996 (Act). Specifically, the Department had not satisfied major requirements of the Act to develop and implement an integrated, enterprise-wide, IT architecture, closely monitor policy implementation efforts, and acquire IT related assets in an effective and efficient manner. We attributed the problems identified, in part, to the Department's decentralized approach to information technology management and oversight and the organizational placement of the Chief Information Officer (CIO).

- *Virus Protection Strategies and Cyber Security Incident Reporting* (DOE/IG-0500, April 2001). The Department's virus protection strategies and cyber security incident reporting methods did not adequately protect systems from damage by viruses and did not provide sufficient information needed to manage its network intrusion threat. These problems existed because the Department had not developed and implemented an effective enterprise-wide strategy for virus protection and cyber security incident reporting.

Department of Energy
Washington, DC 20585

AUG 1 2003

MEMORANDUM FOR RICKEY R. HASS, DIRECTOR
SCIENCE, ENERGY, TECHNOLOGY, AND
FINANCIAL AUDITS
OFFICE OF INSPECTOR GENERAL

FROM: KAREN S. EVANS
CHIEF INFORMATION OFFICER

SUBJECT: Consolidated Comments on Draft Inspector General Report on *Security Over Wireless Networking Technologies*

The Office of the Chief Information Officer, as the designated primary action office, has prepared the attached response to the draft Inspector General Report on *Security Over Wireless Networking Technologies*. The attachment incorporates comments from the National Nuclear Security Administration, the Office of Science and the Office of the Assistant Secretary for Environmental Management.

If you have any questions, please contact Glenn Schlarman or Carol Bales on (202) 586-1090.

Attachment

Consolidated Comments on Draft Audit Report
Security Over Wireless Networking Technologies

__Comments on the MEMORANDUM FOR THE SECRETARY__

Results of Audit (p. 1)

__First paragraph, fourth sentence__: The draft text states that "Absent Departmental guidance, organizations had not focused sufficient attention on properly securing wireless networks or preventing the unauthorized use of such devices."
__Comment__: Where possible policy should not be technology specific. The Department of Energy (DOE) cyber security policies direct the continuous identification and management of risk regardless of the technology used.

__Comments on *SECURITY OVER WIRELESS NETWORKING TECHNOLOGIES*__

Security Plans and Risk Assessment (p. 2)

__First paragraph, last sentence__: Some of the organizations did not consider the risk assessment to be a high priority and told us that they planned to perform it when they updated their CSPP, a process that is supposed to occur before significant operational changes or at two year intervals.
__Comment__: DOE Order 205.1 *Department of Energy Cyber Security Management Program*, paragraph 4.d states that "PCSPs and CSPPs must be reviewed in accordance with the Federal Information System Management Act (FISMA) and updated as needed when operational consideration (e.g. risks, threats, general support system configuration, vulnerabilities, or DOE cyber security directives) change significantly, but not less frequently than every 2 years." It does not specify that the Cyber Security Program Plan (CSPP) update must be completed before the changes are implemented.

Recommendations (p. 3)

To enhance the overall security for wireless networks to unclassified information systems, we recommend that the Chief Information Officer, in conjunction with the Acting Administrator, National Nuclear Security Administration:

__Recommendation 1__: Establish Department-wide requirements for wireless devices and network implementation.

__Response__: Concur with Comment

The Office of the Chief Information Officer (OCIO) has drafted and circulated for comment specific policy for the use of wireless technologies and devices throughout the Department. This draft policy, DOE Notice 205.5, *Cyber Security Requirements for Wireless Devices and Information Systems*, explicitly requires the security of wireless technologies be implemented in a manner consistent with guidance issued by the National

Institute for Standards and Technology (NIST) (NIST Special Publication 800-48, *Wireless Network Security*). The OCIO has discussed this draft policy with program officers and representatives of the Office of the Inspector General (IG). These discussions have made clear the program offices' wireless use must be consistent with NIST guidance as mandated by Office of Management and Budget (OMB) policy.

The requirement to follow NIST wireless guidance was also specifically emphasized by OCIO representatives at DOE's annual security conference in April 2003.

Recommendation 2: Enforce the requirement for organizations to perform documented risk assessments and to develop and implement protective measures commensurate with the assessed level of risk.

Response: Concur with Comment

Current law and policy clearly require documented risk assessments as part of security planning and system certification processes and DOE Order 205.1 includes these requirements. Implementing manuals will further specify the approaches necessary perform and document risk assessments. Implementing protective measures commensurate with the level of risk and magnitude of harm is a key principle integrated into Order 205.1.

It is also important to note that while the OCIO concurs that enforcement is necessary, it is a shared responsibility. The Federal Information Security Management Act of 2002, like the Government Information Security Reform Act of 2000 before it, makes clear that implementation of security controls is first and foremost a program responsibility. As with any management activity, enforcement and accountability must primarily take place at that level. Any approach that removes local accountability sends the incorrect signal that security is not the program official's responsibility. Officials of the current and past Administrations have explicitly made this point in policy statements to the agencies and in testimony before Congress.[1]

The OCIO does agree that it has an oversight responsibility and its current program of collecting performance measurement data and corrective action plans and milestones are the primary vehicles by which oversight is performed. We are improving that process to include quarterly reporting of performance measures and providing feedback to the programs as to the areas of weakness.

[1] OMB M-01-08, Memorandum for the Heads of Executive Departments and Agencies, Jack Lew, Director, *Guidance on Implementing the Government Information Security Reform Act*, January 16, 2001. Testimony of the Honorable John T. Spotilla, Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget, *Computer Security: Cyber Attacks- War without Borders*, July 26, 2000. Statement of Mark A. Forman, Associate Director for Information Technology and Electronic Government, Office of Management and Budget before the Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, U.S. House of Representatives, November 9, 2001.

As directed by OMB, these performance measures and corrective action plans are tools primarily intended for line management to continually assess their security performance and make necessary adjustments. Waiting for or relying solely on the OCIO to identify and alert program offices as to weaknesses is an incorrect shift in responsibility and accountability and will degrade security performance not improve it.

Finally, program offices and sites need not wait for OCIO feedback. Through the IG and DOE's Office of Independent Oversight and Performance Assurance (OA) reviews, self-assessments, peer-reviews, etc., program officials currently have ample feedback and the means to understand, implement, and enforce all necessary security controls.

Recommendation 3: Require that wireless security be evaluated during the security self-assessments required by the Federal Information Security Management Act of 2003.

Response: Concur with Comment

Order 205.1 requires that Heads of Departmental Elements prepare a Program Cyber Security Plan (PCSP) that includes addressing the risk of using wireless technology within their IT infrastructure. While the IG recommends adding wireless as a data collection point, the draft does not assert that wireless outweighs any of the risks and findings presented in previous IG reports for which specific review has not been suggested, nor are wireless technologies and devices specifically called out in NIST Special Publication 800-26 *Security Self-Assessment Guide of Information Technology Systems*. The OCIO agrees that wireless technology, as well as other technology areas, should be assessed by all sites as a general Risk Assessment responsibility. If it is a greater risk to the Department overall, it should be stated in the report.

Comments on the Recommendations

To correct the specific vulnerabilities noted in this report, we recommend that the Acting Administrator, National Nuclear Security Administration, and the Under Secretary for Energy, Science, and Environment require the offices and organizations within their responsibility to:

Recommendation 1: Develop and implement protective measures commensurate with the assessed level of risk of wireless networks including evaluating and acquiring wireless security technical tools that enable effective testing and monitoring of wireless devices and networks against associated risk.

Response: Concur.

The OCIO has prepared DOE Notice 205.5, *Cyber Security Requirements for Wireless Devices and Information Systems*. This notice must be implemented at all organizational levels with requirements and responsibilities flow down, as appropriate, to subordinate organizational levels. As part of this flow down process, Heads of Departmental Elements must develop and maintain PCSPs that address, among other things, risk management, including the use of wireless and personal electronic devices, consistent with NIST Special Publication 800-48. This notice also requires, per the PCSP, inclusion within applicable CSPPs of the specific technical, operational and management controls for wireless devices and information systems necessary to maintain risk at an acceptable level. This Notice is expected to be published 4th quarter FY03.

Evaluation and acquisition of wireless security tools will be commensurate with the evaluation of risk that wireless networks and devices present at the local site.

Recommendation 2: Amend Cyber Security Program Plans prior to introduction of new technologies into their computing environment if it significantly changes the operational risk.

Response: Concur.

DOE Notice 205.5, *Cyber Security Requirements for Wireless Devices and Information Systems* requires Departmental Elements to identify, within their PCSPs, requirements regarding the incorporation of wireless technology. It further requires that Sub-elements include wireless networks and devices in their CSPPs. CSPPs must be updated as needed when operational considerations change significantly, but at least every 2 years and system security plans must be completed annually. Introducing wireless technologies into a legacy application or system may constitute a significant change to operational risk. If so, system-level security plans must be updated to reflect the use of wireless technologies. If not, officials responsible for updating the CSPPs must document their conclusion that a change to operational risk has not occurred.

Overall requirements for a DOE organization's CSPPs are documented in its PCSP. As noted previously in our comments on Security Plans and Risk Assessments, we do not agree with the assumption in the draft report that a CSPP update is "supposed to occur before significant operational changes."

Recommendation 3: Issue clear guidance for wireless security, tailored to the particular operating environment, consistent with NIST guidance.

Response: Concur.

DOE Notice 205.5, *Cyber Security Requirements for Wireless Devices and Information Systems*, requires DOE Elements to use a documented risk-based approach, consistent with NIST Special Publication 800-48, *Wireless Network Security*. This Notice is expected to be published during the 4th quarter FY03. Further, Departmental Element's PCSPs must document roles, responsibilities, processes, and requirements for operating wireless devices and networks and for interconnecting them to DOE LAN/WAN systems.

IG Report No.: DOE/IG-0617

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the audit would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in this report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name ____________________________ Date _________________________

Telephone ________________________ Organization ___________________

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Wilma Slaughter at (202) 586-1924.