DOE F 1325.8
(08-93)
United States Government **Department of Energy**

Memorandum

DATE: September 28, 2007 Audit Report No.: OAS-L-07-25

REPLY TO
ATTN OF: IG-34 (A07TG028)

SUBJECT: Report on Audit of "Remote Access to the Department's Unclassified Information Systems"

TO: Administrator, National Nuclear Security Administration, NA-1
Under Secretary for Science, SC-1
Acting Under Secretary of Energy, NE-1
Chief Information Officer, IM-1

INTRODUCTION AND OBJECTIVE

To help accomplish its strategic goals and mission requirements, the Department of Energy (Department or DOE) utilizes numerous interconnected computer networks and individual systems, including ones accessed remotely. While remote access by authorized individuals can provide numerous advantages such as the capability to perform business-related functions, retrieve electronic mail, and access business applications while out of the office, allowing these capabilities can expose Department systems to an increased level of vulnerability to attack. For example, an authorized user working from his or her home computer system could inadvertently introduce a virus or allow an attacker access to the Department's networks and systems if the personally-owned system is not adequately protected.

In 2002, our report on *Remote Access to Unclassified Information Systems* (DOE/IG-0568, September 2002) identified that the Department had not adequately considered the risk associated with remote access to unclassified information systems, developed specific guidance for remote access security, or required protective measures such as personal firewalls and virus protection software. Because of the increasingly widespread use and evolving nature of risks regarding remote access, we initiated this audit to follow-up on our prior work and determine whether the Department had adequately secured its information and information systems from unauthorized remote access.

CONCLUSION AND OBSERVATIONS

Since our previous report the Department has taken a number of actions to secure its information and information systems from unauthorized remote access. For instance, Department-level policy was issued along with high-level guidance relating to remote access security. The Department has also focused heavily on protecting access to personally identifiable information (PII), which has, in turn, strengthened protections over remote access, such as the implementation of two-factor authentication tools.

Similarly, at the organizations visited, we observed that the actual practices for protecting remote access were generally adequate. However, we found that the actual practices noted above were generally ahead of efforts to ensure that the cyber security documentation was up-to-date and reflected these modernized protective practices.

Actions Taken to Secure Information Systems

In response to our prior report and changes in Federal requirements, the Department has taken a number of positive actions to improve remote access security. For instance, in February 2004, the Department's Office of Chief Information Officer (OCIO) issued Department of Energy Notice 205.11, which re-emphasized requirements set in Federal law to employ a documented risk-based approach and set forth minimum requirements for security of remote access to Department and contractor information systems. The Notice required the program offices to implement these requirements by May 2004.

The Department next issued Order 205.1A, which defined a Department-wide cyber security management program. The Order allows the OCIO to define the technical and management requirements (TMRs) to be implemented by each Under Secretary organization and requires each Under Secretary to document TMR implementation in Program Cyber Security Plans (PCSPs). The PCSPs serve as the overarching direction to organizations under each Under Secretary's purview for implementing program specific requirements and the requirements of the OCIO's TMRs. The sites and organizations having responsibilities to each Under Secretary must be able to demonstrate they have implemented requirements as set forth in the corresponding PCSP through their own cyber security planning documentation and related activities.

In January 2007, the OCIO issued a guidance memorandum on remote access that required senior Department managers to define – in their PCSPs – the policies, processes, and procedures for allowing remote access to their systems from outside of the systems' accreditation boundaries. The program offices were asked to incorporate the guidance in their program-level direction by April 19, 2007. Finally, the OCIO issued TMRs covering remote access and the use of external information systems in August 2007.

Updates to Cyber Security Documentation

While remote access practices at the organizations visited appeared to be generally adequate, the cyber security documentation at both the program and site levels had not yet been updated to reflect these efforts. In particular, the PCSPs issued by Headquarters organizations did not always include adequate direction or policies and procedures for allowing remote access to accredited systems. For example, the Office of Science's PCSP covered remote access at a high level, but did not provide all required guidance or direction to its program organizations or sites for implementing remote access controls. Similarly, the Office of Environmental Management's PCSP did not provide the essential guidance or direction to its program organizations or sites for implementing remote access controls.

Certification and accreditation documentation from six Department sites also did not specify requirements for remote access or for updating PII protections. Specifically, although the necessary management, operational, and technical controls relating to remote access appeared to be in place, they were not adequately outlined in the site-level cyber security program plans. Details describing security-related patching of operating system and application software, updates for anti-virus scanners, and minimum requirements for configuration on equipment used for remote access were also not included.

SUGGESTED ACTIONS

To ensure that remote access risks and associated protective measures can be adequately evaluated and implemented, we suggest that the Administrator, National Nuclear Security Administration, Under Secretary for Science, and the Under Secretary of Energy, in coordination with the Chief Information Officer, update PCSPs and requirements for governing remote access to accredited systems, consistent with the Department's technical and management requirements as well as guidance from the National Institute of Standards and Technology.

Since no formal recommendations are being made in this report, a formal response is not required. We appreciate the cooperation of your staff during this audit.

Rickey R. Hass
Assistant Inspector General
for Financial, Technology, and Corporate Audits
Office of Audit Services
Office of Inspector General

Attachment

cc: Chief of Staff
Team Leader, Audit Liaison, CF-1.2
Director, Policy and Internal Controls Management, NA-66
Audit Liaison, EM-33
Audit Liaison, FE-3
Audit Liaison, IM-10
Audit Liaison, HS-1.23
Audit Liaison, SC-32.1

SCOPE AND METHODOLOGY

SCOPE AND METHODOLOGY

Fieldwork on the follow-up audit of Remote Access to the Department of Energy's (Department) Unclassified Information Systems was performed between November 2006 and August 2007 at several Department locations. To accomplish the audit objective, we:

- Reviewed applicable laws, regulations, and guidance pertaining to remote access to information systems. We also reviewed relevant reports issued by the Office of Inspector General and the Government Accountability Office;

- Reviewed the *Government Performance and Results Act of 1993* and determined if performance measures had been established for remote access;

- Held discussions with Department officials and personnel from the field sites and obtained and reviewed relevant cyber security documentation regarding remote access practices; and,

- Examined configuration settings and practices for obtaining remote access to the Department's networks via selected systems.

The audit was performed 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 objective. Accordingly, we assessed significant internal controls and performance measures under the *Government Performance and Results Act of 1993* regarding management of remote access services. 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. We discussed the results of our audit with Department representatives on September 27, 2007.