GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-08-1001, a report to congressional committees

September 2008

# INFORMATION SECURITY

## Actions Needed to Better Protect Los Alamos National Laboratory's Unclassified Computer Network

## Why GAO Did This Study

The Los Alamos National Laboratory (LANL), which is operated by the National Nuclear Security Administration (NNSA), has experienced security lapses protecting information on its unclassified computer network. The unclassified network contains sensitive information. GAO (1) assessed the effectiveness of the security controls LANL has in place to protect information transmitted over its unclassified computer network, (2) assessed whether LANL had implemented an information security program for its unclassified network, and (3) examined expenditures to protect LANL's unclassified network from fiscal years 2001 through 2007. To carry out its work, GAO examined security policies and procedures and reviewed the laboratory's access controls for protecting information on the unclassified network.

## What GAO Recommends

GAO recommends, among other things, that the Secretary of Energy and the Administrator of NNSA require the Director of LANL to (1) ensure that the risk assessment for the unclassified network evaluates all known vulnerabilities and is revised periodically and (2) strengthen policies with a view toward further reducing, as appropriate, foreign nationals'—particularly those from countries that DOE has identified as sensitive—access to the unclassified network. NNSA did not specifically comment on GAO's recommendations but agreed with the conclusions.

To view the full product, including the scope and methodology, click on GAO-08-1001. For more information, contact Gene Aloise at (202) 512-3841, or aloisee@gao.gov; Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov and Nabajyoti Barkakati at (202) 512-6412 or barkakatin@gao.gov.

## What GAO Found

LANL has implemented measures to enhance its information security, but weaknesses remain in protecting the confidentiality, integrity, and availability of information on its unclassified network. LANL has implemented a network security system that is capable of detecting potential intrusions. However, GAO found vulnerabilities in several critical areas, including (1) identifying and authenticating users, (2) encrypting sensitive information, and (3) monitoring and auditing compliance with security policies. For example, LANL had implemented strong authentication measures for accessing the network. However, once gaining this access, a user could create a simple password that would allow alternative access to certain sensitive information. Furthermore, LANL did not use encryption for authentication to certain internal services, which increased the risk that sensitive information transmitted over the unclassified network could be compromised.

A key reason for the information security weaknesses is that the laboratory has not implemented an information security program to ensure that controls are effectively established and maintained. For example, LANL did not adequately assess information security risks or develop effective policies and procedures to govern the security of its computing environment. LANL's most recent risk assessment for the unclassified network generally identified and analyzed vulnerabilities, but did not account for risks identified by internal vulnerability testing. Deficiencies in LANL's policies and procedures have been the subject of reports by the Department of Energy's (DOE) Office of Independent Oversight and the Los Alamos Site Office, including foreign nationals' access to the unclassified network. GAO found that, as of May 2008, 301 (or 44 percent) of 688 foreign nationals, who had access to the unclassified network, were from countries classified as sensitive by DOE, such as China, India, and Russia. In addition, a significant number of foreign nationals from sensitive countries were authorized remote access to LANL's unclassified network. The number of foreign nationals with access has raised concerns among laboratory and NNSA officials because of the sensitive information contained on the unclassified network. In response, the laboratory has taken some measures to limit foreign nationals' access.

From fiscal years 2001 through 2007, LANL spent approximately $51.4 million to protect its unclassified network. LANL cyber security officials told us that funding has been inadequate to address some of their security concerns. Specifically, there was a risk that unclassified network users would no longer receive cyber security training and that the laboratory would not be able to ensure that data containing sensitive unclassified information would be properly sanitized or destroyed. However, NNSA officials asserted that LANL has not adequately justified its requests for additional funds. NNSA is in the process of implementing a more systematic approach for developing budgets for cyber security activities across the nuclear weapons complex, including LANL.