

September 2008

INFORMATION
SECURITY

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





Highlights of [GAO-08-1001](#), a report to congressional committees

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 aloise@gao.gov; Gregory Wilshusen at (202) 512-6244 or wilshusen@gao.gov and Nabajyoti Barkakati at (202) 512-6412 or barkakatin@gao.gov.

INFORMATION SECURITY

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

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.

Contents

Letter		1
	Results in Brief	6
	Background	9
	LANL Has Information Security Controls in Place to Protect Its Unclassified Network, but Weaknesses Remain	10
	LANL Has Not Fully Implemented Key Information Security Program Activities for Its Unclassified Network	14
	LANL Has Spent Approximately \$51.4 Million to Protect Its Unclassified Network from Fiscal Years 2001 through 2007, but Future Resource Requirements Need Better Justification	27
	Conclusions	32
	Recommendations for Executive Action	33
	Agency Comments and Our Evaluation	35
Appendix I	Objectives, Scope, and Methodology	37
Appendix II	Comments from the National Nuclear Security Administration	40
Appendix III	GAO Contacts and Staff Acknowledgments	42
Related GAO Products		43
Figures		
	Figure 1: Percentage of Foreign Nationals from Sensitive and Nonsensitive Countries at LANL with Unclassified Network Access, as of May 2008	26
	Figure 2: Annual Expenditures on LANL's Unclassified Network, Fiscal Years 2001-2007	29

Abbreviations

C&A	certification and accreditation
DAA	Designated Approving Authority
DOE	Department of Energy
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
FSU	former Soviet Union
IT	information technology
LANL	Los Alamos National Laboratory
LANS	Los Alamos National Security, LLC
LASO	Los Alamos Site Office
NIST	National Institute of Standards and Technology
NNSA	National Nuclear Security Administration
OMB	Office of Management and Budget
PIN	personal identification number
SANS	System Administration, Networking, and Security

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

September 9, 2008

The Honorable John D. Dingell
Chairman
The Honorable Joe Barton
Ranking Member
Committee on Energy and Commerce
House of Representatives

The Honorable Bart Stupak
Chairman
The Honorable John M. Shimkus
Ranking Member
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
House of Representatives

The Los Alamos National Laboratory (LANL),¹ which is operated by the National Nuclear Security Administration (NNSA),² has experienced a number of security lapses in protecting sensitive information. Over the last decade, these information security lapses have included, but are not limited to, the inability to accurately identify computer resources

¹The laboratory is a multidisciplinary national security laboratory whose core missions are to ensure the safety and reliability of the nuclear weapons stockpile and to conduct research and development that supports that mission and other homeland security-related initiatives. The laboratory covers 40 square miles, with 2,700 buildings covering 9.4 million square feet, employs more than 12,000 personnel, and has an annual operating budget of approximately \$2 billion. LANL operates 15 divisions that are responsible for carrying out its programmatic mission, including nuclear weapons engineering, nuclear weapons stockpile manufacturing and support, nuclear weapons physics, and nuclear weapons threat reduction. The laboratory also has a Chief Security Officer, Chief Information Security Officer, and Chief Information Officer who are responsible for overseeing information security, including protecting cyber security assets. In addition, federal oversight for information security at LANL, including cyber security, is provided by the Los Alamos Site Office.

²NNSA was established in 2000 in response to management difficulties with the Department of Energy's nuclear weapons programs. These difficulties included security programs at the department's national laboratories and significant cost overruns in the management of projects. NNSA is a separately organized agency within the department with the responsibility for the nation's nuclear weapons, nonproliferation, and naval reactors programs.

connected to the unclassified network and to identify and correct computer network vulnerabilities.

The unclassified network at LANL comprises over 25,000 devices, which does not include supporting devices, such as servers, printers, and scanners. It also contains about 51,000 active network ports, which serve as the interface between computers and other devices on the network, and provides service to over 13,000 users.

LANL's unclassified network is segmented into subnetworks and includes the (1) protected-unclassified network, which is the default location for unclassified computer systems at the laboratory and contains sensitive unclassified data and information; (2) unclassified-open network, which supports the laboratory's presence on the Internet and is to contain no sensitive information; (3) collaboration network, which supports external scientific collaboration involving high-performance computing; and (4) visitor network, which provides an outgoing connection to the Internet for visitors needing to check e-mail. This report focuses on LANL's protected-unclassified network because this network is designed to protect most of the laboratory's networks and systems from unauthorized access and is the clear target of sophisticated cyber attacks. For the purposes of this report, we will refer to this network as the "unclassified" network.

LANL's unclassified network has faced a number of security challenges. During 2007, according to LANL officials, the firewalls and other blocking mechanisms of the unclassified network deflected more than 10 million cyber probes every month. Cyber attacks include, among other things, the use of information exploitation tools, such as computer viruses, Trojan horses, and worms, that can destroy, intercept, and degrade the integrity of or deny access to information on a computer network. In addition, the unclassified network has voluminous e-mail traffic, which makes the network potentially vulnerable to malicious code designed to exploit e-mail services. The network receives approximately 2 million e-mails per month, plus approximately 50,000 to 500,000 spam e-mails every day, and LANL employees send approximately 1 million e-mails every month.

LANL's large unclassified computer network contains sensitive information, including business proprietary information; unclassified controlled nuclear information; naval nuclear propulsion information; export control information; nuclear reactor safeguards information; the military critical technology list; confidential foreign government information; and personally identifiable information, including names, aliases, Social Security numbers, and biometric records of employees,

contractors, and visitors. Owing to the nature of the research and development conducted at LANL, the information on the unclassified network presents a valuable target for foreign governments, terrorists, and industrial spies.

Recognizing the importance of securing information systems at federal agencies, Congress enacted the Federal Information Security Management Act (FISMA) in December 2002 to strengthen the security of information and information systems across the federal government.³ FISMA requires each agency to develop, document, and implement an agency-wide information security program that supports the operations and assets of the agency, including those provided or managed by another agency or contractor on its behalf.

To ensure the confidentiality, integrity, and availability of critical information and information systems used to support the operations and assets of federal agencies, information security controls and complementary program activities are required.⁴ Effective information security controls are necessary to ensure the protection of sensitive information contained and transmitted over computer networks. In addition, certain program management activities, such as the development, documentation, and implementation of policies and procedures, are required to govern the protection of information.⁵

Information security controls are put in place to prevent, limit, and detect unauthorized access, use, disclosure, modification, distribution, or disruption to computing resources, programs, and information. Examples of information security controls are as follows:

- *User identification and authentication* allows computer systems to differentiate between users so that activities on the system can be linked to specific individuals, and the claimed identity of users can be verified.

³FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2946 (Dec. 17, 2002).

⁴GAO has issued a series of reports that address federal agencies' information security programs and activities. See Related GAO products.

⁵For the purpose of this report, we are including LANL's "cyber" and computer network security programs as a key component of the laboratory's overall information security program.

-
- *Cryptography* underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information.⁶
 - *Audit and monitoring* controls help establish individual accountability and monitor compliance with security policies.
 - *Configuration management* involves the identification and management of security features for all hardware, software, and firmware components of an information system and systematically controls changes to that configuration throughout the development and operational life cycle of the system.
 - *Physical controls* restrict physical access to computer resources, usually by limiting access to the buildings and rooms in which the resources are housed and by periodically reviewing the access granted in order to ensure that access continues to be appropriate.

A comprehensive information security program is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. The program should establish a framework and continuous cycle of activities for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures.

Information security program activities govern the security protections for the information and information systems that support the operations and assets of the agency using a risk-based approach. These activities include ensuring that an agency (1) periodically assesses the risk and the magnitude of harm that could result from unauthorized access; (2) develops, documents, and implements risk-based policies and procedures to ensure that information security is addressed throughout the life cycle of each system and ensures compliance with applicable requirements; (3) develops, documents, and implements plans to provide adequate information security for networks, systems, and facilities; (4) provides security awareness training to inform personnel of information security risks and of their responsibilities in complying with agency policies and procedures; (5) periodically tests and evaluates the effectiveness of information security policies, procedures, and practices relating to

⁶Encryption can be used to provide basic data confidentiality and integrity by transforming plain text into cipher text using a special value known as a key and a mathematical process known as an algorithm.

management, operational, and technical controls for every system—the frequency of such tests should be based on risk but occur at least once per year; (6) has a process for planning, implementing, evaluating, and documenting remedial action to address deficiencies in information security policies, procedures, or practices; (7) has procedures for detecting, reporting, and responding to security incidents; and (8) documents, develops, and implements plans and procedures to ensure continuity of operations for information systems that support its operations and assets.

This report evaluates key elements of LANL’s unclassified information security program. Specifically, we (1) assessed the effectiveness of security controls LANL has implemented to protect information transmitted over its unclassified computer network, (2) assessed whether LANL had implemented an information security program to ensure that controls were effectively established and maintained for its unclassified computer network, and (3) examined the expenditure of funds used to protect LANL’s unclassified computer network from fiscal years 2001 through 2007.

We visited LANL to assess the effectiveness of security controls that the laboratory had implemented for its unclassified computer network, and we gained an understanding of the overall network control environment and identified its interconnectivity and control points. We performed vulnerability assessments to evaluate authentication and authorization controls, encryption mechanisms, network monitoring processes, and configuration management controls for the unclassified network. We also reviewed the effectiveness of physical security operations in preventing unauthorized access to cyber-related resources. In addition, we obtained views from and documentation on these issues from responsible security officials at the Department of Energy (DOE), NNSA, the Los Alamos Site Office (LASO), and LANL.

To assess whether LANL had implemented an information security program to ensure that controls were effectively established and maintained for its unclassified computer network, we determined whether policies and procedures adhered to NNSA, DOE, and the National Institute of Standards and Technology (NIST) guidance, in areas such as security awareness training, risk assessment, information security plans, security testing and evaluation, corrective action plans, and continuity of operations for information systems. In addition, we obtained the views of and documentation on these issues from officials responsible for information security management at DOE, NNSA, LASO, and LANL. We

also met with officials from DOE's Office of Independent Oversight and its Office of Inspector General, regarding any related prior, ongoing, or planned work in these areas.

To determine the expenditure of funds used to protect LANL's unclassified computer network from fiscal years 2001 through 2007, we obtained and analyzed documentation detailing program expenditures and met with LANL officials to discuss the data. We chose this time period because, beginning in fiscal year 2001, NNSA assumed programmatic responsibility for the nuclear weapons complex. We obtained responses to a series of data reliability questions, from responsible LANL officials, covering issues such as data entry access, internal control procedures, and the accuracy and completeness of the data. In addition, we obtained written responses from LANL officials to clarify discrepancies in the data we received. We determined that the data were sufficiently reliable for the purposes of this report.

We conducted this performance audit from May 2007 to September 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. A more detailed description of our objectives, scope, and methodology is contained in appendix I.

Results in Brief

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. In particular, LANL has implemented a network security system that is capable of detecting potential intrusions on the network. However, LANL has vulnerabilities in several critical areas, including (1) identifying and authenticating users of the network, (2) encrypting sensitive information, (3) monitoring and auditing compliance with security policies, (4) controlling and documenting changes to a computer system's hardware and software, and (5) restricting physical access to computing resources. For example, although LANL had implemented strong authentication measures for accessing the network, these measures were not always used. Once a user successfully accessed the network, the user could create a separate simple password that would allow alternative access to certain sensitive information. Furthermore, LANL neither conducted comprehensive vulnerability scans of the unclassified network nor did it include sensitive

applications in these scans, thus leaving the network at increased risk of compromise or disruption. In addition to these weaknesses, LANL's computing facilities had physical security weaknesses and could be vulnerable to intentional disruption. Specifically, we observed lax restriction of vehicular traffic entering the laboratory and inadequate fencing.

The laboratory has not yet implemented an information security program to ensure that controls are effectively established and maintained—the absence of such a program is a key reason for the information security weaknesses we identified. Although LANL has implemented an effective security awareness training program, we identified a number of shortcomings in its overall information security management program. 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 current risk assessment for the unclassified network, completed in June 2007, generally identified and analyzed vulnerabilities but did not account for risks identified by internal vulnerability testing. We also identified shortcomings in other information security policies and procedures. For example, LANL's information security policies and procedures lacked specific implementation guidance. Furthermore, LANL does not have a formal contingency plan for its unclassified network that conforms to current federal requirements to ensure continuous network operations. Many of these cyber security deficiencies have been the subject of prior reports by DOE's Office of Independent Oversight and LASO. The most recent reports, covering fiscal years 2006 and 2007, documented significant weaknesses with LANL's unclassified information security program, including foreign nationals' access to the laboratory's unclassified network. As of May 2008, LANL had granted unclassified network access to 688 foreign nationals, including over 300 from countries identified as sensitive by DOE, such as China, India, and Russia. A country is identified as sensitive based on national security, nuclear nonproliferation, or terrorism concerns. In addition, foreign nationals from sensitive countries have been authorized remote access to LANL's unclassified network. The number of foreign nationals who have access to the unclassified network has raised security concerns among some laboratory and NNSA officials because of the sensitive information contained on the network. According to LANL, the percentage of foreign nationals with authorized remote access to the unclassified network has steadily declined over the last 5 years.

From fiscal years 2001 through 2007, LANL spent about \$51.4 million to protect and maintain its unclassified network. Although LANL cyber

security officials told us that funding has been inadequate to address some of their security concerns, NNSA officials raised questions about the basis for LANL's funding request for cyber security. NNSA's Chief Information Officer told us that LANL has not adequately justified requests for additional funds to address the laboratory's stated shortfalls. In addition, NNSA officials informed us that LANL's past budget requests were prepared on an ad hoc basis and were not based on well-defined threat and risk assessments. In response to these concerns, in fiscal year 2006, NNSA implemented a more systematic approach to developing cyber security budgets across the nuclear weapons complex, including LANL. This effort, however, does not provide guidance that clearly lays out funding priorities. Furthermore, NNSA does not consistently document resource allocation decisions and identify how funding shortfalls affect critical cyber security issues.

To help strengthen information security controls over LANL's unclassified network, we are making a series of recommendations to the Secretary of Energy and the Administrator of NNSA that require the Director of the Los Alamos National Laboratory to, among other things, (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 countries identified as sensitive by DOE—access to the unclassified network. We also are making 41 recommendations in a separate report with limited distribution. These recommendations consist of actions to be taken to correct the specific information security weaknesses related to identification and authentication, cryptography, audit and monitoring, configuration management, and physical security.

We provided NNSA with a copy of this report for review and comment. NNSA did not specifically comment on our recommendations. However, NNSA agreed with our general conclusion that LANL has taken steps to protect sensitive information and acknowledged that there was considerable work yet to be done. NNSA also stated that LANL is currently responding to a DOE Secretarial Compliance Order requiring the laboratory contractor to take comprehensive steps to ensure that it identifies and addresses, among other things, critical cyber security deficiencies. The July 2007 Compliance Order requires LANL to submit an integrated corrective action plan to address critical security issues. These steps must be completed by December 2008. NNSA noted that responding to the issues identified in this report—as well as more technical issues included in a limited official use only version of this report—will extend beyond the completion of the Compliance Order since the actions we

recommend are more complex. We would expect that our recommendations, when implemented, would complement and be consistent with other remedial actions taken to improve LANL's cyber security posture as part of the Secretarial Compliance Order.

Background

LANL is responsible for planning and executing all facets of stockpile stewardship, including assessing, refurbishing, and certifying nuclear weapons. The laboratory operates and manages numerous nuclear facilities. Critical activities include plutonium, uranium, and tritium processing; research and development on special nuclear material; high-energy radiography; radiation measurement; packaging of nuclear materials; and the management of radioactive and hazardous waste. To help carry out these critical missions, LANL uses its unclassified and classified computer networks to manage its business operations, conduct nonnuclear experiments, and analyze nuclear weapons and their delivery systems to meet requirements established by the Department of Defense.

Protecting the computer systems that support LANL's operations has never been more important. Government officials are increasingly concerned about attacks from individuals and groups with malicious intent, such as terrorists and foreign intelligence agencies. These concerns are well-founded for a number of reasons, including the dramatic increase in the reports of security incidents in the United States and the steady advance in the sophistication and effectiveness of attack technologies. As the nation's defense and intelligence communities increasingly rely on commercially available information technology, the likelihood increases that information attacks will threaten vital national interests.

A basic management objective for any organization is to protect the resources that support its critical operations from unauthorized access, use, destruction, or disruption. Organizations accomplish this objective by designing and implementing controls that are intended to, among other things, prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities. Inadequate security controls diminish the reliability of computerized information and increase the risk of unauthorized disclosure, modification, and destruction of sensitive information and disruption of service. Security controls include those related to user identification and authentication, cryptography, audit and monitoring, configuration management, and physical security.

LANL Has Information Security Controls in Place to Protect Its Unclassified Network, but Weaknesses Remain

LANL has implemented measures to enhance its information security, but weaknesses remain. In particular, LANL has implemented a network security system that can detect potential intrusions on the network. However, LANL has vulnerabilities in several critical areas, including (1) identifying and authenticating users, (2) encrypting sensitive information, (3) monitoring and auditing compliance with security policies, (4) controlling and documenting changes to a computer system's hardware and software, and (5) restricting physical access to computing resources.

Strong Authentication Was Implemented but Not Always Used

A computer system must be able to identify and authenticate different users so that activities on the system can be linked to specific individuals. When an organization assigns unique user accounts to specific users, the system is able to distinguish one user from another—a process called identification. The system also must establish the validity of a user's claimed identity by requesting some kind of information, such as a password, that is known only by the user—a process known as authentication. The combination of identification and authentication—such as user account/password combinations—provides the basis for establishing individual accountability and for controlling access to the system. As NIST notes, multifactor authentication schemes are stronger than single factor authentication.⁷ In keeping with this standard, LANL's password policy requires that one-time passcodes (using token cards and personal identification numbers (PIN), i.e., two-factor authentication) be used whenever possible or practical. It further states that users are not to share passwords and that vendor-supplied default passwords must be changed immediately.

LANL had implemented a strong authentication solution for its network through the use of two-factor authentication with a one-time password—use of a token (cryptocard); a PIN; and a one-time number code. However, strong authentication was not always used. Once a user successfully

⁷According to NIST, authentication mechanisms can be based on three categories of information or "factors": something the user knows, such as a password; something the user possesses, such as a token; and some physical characteristic (biometric) of the user, such as a fingerprint. Authentication methods employing a token or biometric can provide a significantly higher level of security than passwords alone. Multifactor authentication mechanisms, such as those involving tokens and biometric data are considered strong authentication mechanisms.

accessed the network, the user could create a separate login password that would allow alternative access to sensitive information on the unclassified network. Such access was allowed for file sharing and e-mail. Furthermore, users shared default identifications and passwords for managing certain network devices. As a result, LANL was at increased risk that unauthorized users could access sensitive information in files and e-mails, as well as obtain access to network devices.

Cryptography Was Not Always Effectively Used

Cryptography underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information. A basic element of cryptography is encryption. The National Security Agency recommends disabling protocols that do not encrypt information, such as user identification and password combinations transmitted across the network.

Although LANL had implemented cryptography, it was not always effective or used in transmitting sensitive information. LANL integrated Kerberos with its authentication process.⁸ Kerberos is designed to provide strong authentication for client/server applications by using secret-key cryptography so that each party can prove its identity across an insecure network connection. However, the laboratory relied on a Kerberos implementation that uses a weak and outdated encryption algorithm. Furthermore, LANL neither uses encryption to protect certain network management connections, nor requires encryption for authentication to certain internal services. Instead, the laboratory used clear text protocols (i.e., unencrypted) to manage key network devices, such as internal firewalls and switches. As a result, sensitive data transmitted through the unclassified network is at an increased risk of being compromised.

Network Monitoring Was Performed Regularly but Was Not Comprehensive

To establish individual accountability, monitor compliance with security policies, and investigate security violations, it is crucial to determine who has taken actions on the system, what these actions were, and when they were taken. According to NIST, when performing vulnerability scans, greater emphasis should be placed upon systems that are accessible from the Internet (e.g., Web and e-mail servers); systems that house important or sensitive applications or data (e.g., databases); or network

⁸Kerberos is a widely used authentication protocol developed at the Massachusetts Institute of Technology.

infrastructure components (e.g., routers, switches, and firewalls). In addition, according to commercial vendors, running scanning software in an authenticated mode allows the software to detect additional vulnerabilities. NIST also states that the use of secure software development techniques, including source code review, is essential to preventing a number of vulnerabilities from being introduced into items such as a Web service.

Although LANL regularly monitored its unclassified network for security vulnerabilities, the monitoring is not comprehensive. LANL frequently scans its network using multiple software tools that search for known vulnerabilities on various network devices. However, the scans were not comprehensive. For example, at the time of our review, the laboratory's vulnerability scan neither included sensitive applications such as databases, nor did it run in an authenticated mode. In addition, LANL did not conduct source code reviews. As a result, the laboratory may not detect certain vulnerabilities, leaving the network at increased risk of compromise or disruption.

Although LANL Uses Innovative Techniques for Configuration Management, It Does Not Consistently Implement Software Patches

The purpose of configuration management is to establish and maintain the integrity of an organization's work products. Organizations can better ensure that only authorized applications and programs are placed into operation by establishing and maintaining baseline configurations and monitoring changes to these configurations. Configuration management involves ensuring the correctness of the security settings in the operating systems, applications, or computing and network devices, and securely maintaining operations. Patch management, a component of configuration management, is important for mitigating software vulnerability risks. When software vulnerabilities are discovered, the software vendor may develop and distribute a patch or work-around to mitigate the vulnerability. NIST recommends that organizations have an explicit and documented patching policy and a systematic, accountable, and documented process for installing and testing patches. In addition, LANL policy requires that all Windows-based systems on the unclassified network participate in a patch management system. In addition to patch management, to further protect an organization's systems, such as from malicious e-mails, NIST states that organizations should determine which types of attachments to allow and to block potentially dangerous ones.

Although LANL had implemented innovative techniques to maintain its system configuration and install patches, shortcomings existed in the patch process. The laboratory used an automated tool to configure and

maintain its Unix servers, and deployed a tool to its Windows systems to track and implement patches on the majority of systems we reviewed. It also used its vulnerability scanning tools to verify the latest patch levels of Windows systems. However, LANL did not always consistently implement or appropriately test these patches. For example, LANL had not applied a critical operating system patch or patches for a number of general third-party applications. As a result, LANL cannot ensure that all needed patches are applied to critical system resources or that untested patches will not have unintentional consequences, increasing the risk of exposing critical and sensitive unclassified data to unauthorized access. Furthermore, although the laboratory had configured its e-mail system to prevent many common cyber attacks, it was still vulnerable to attack because the system allowed various file types as e-mail attachments. These files could be used to install malicious software onto an unsuspecting user's workstation, potentially compromising the unclassified network.

Physical Security Controls May Leave the Unclassified Network Vulnerable to Disruption

Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. These controls restrict physical access to computer resources, usually by limiting access to the buildings and rooms in which the resources are housed and by periodically reviewing the access granted in order to ensure that it continues to be appropriate. NIST requires that federal organizations control all physical access points (including designated entry/exit points) to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and verify individual access authorizations before granting access to the facilities. In addition, NIST requires that federal agencies control physical access to information system transmission lines to prevent eavesdropping, in-transit modification, disruption, or physical tampering, and that these agencies protect power equipment for information systems from damage or destruction. Furthermore, LANL policy requires that access to exclusion areas that house sensitive information technology (IT) resources and the equipment that supports these resources be limited to authorized personnel.

LANL has various protections in place for its IT resources. It effectively secures many of its sensitive areas and computer equipment and takes other steps to provide physical security. For example, LANL issued electronic badges and employed hand geometry devices to help control access to many of its sensitive and restricted areas. It also maintains liaisons with law enforcement agencies to help ensure additional backup

security if necessary and to facilitate the accurate flow of timely security information among appropriate government agencies.

However, LANL's computing facilities may be vulnerable to attack because of weaknesses in its controls over physical access points, including the lax control of vehicular traffic, inadequate fencing, unsecured buildings housing computer network equipment, and signs visible from the street that indicate what these buildings contain. In addition, LANL did not effectively control access to a (1) telecommunications room that houses transmission lines and equipment and (2) utility room that provides heating and air conditioning for sensitive IT equipment. These weaknesses in physical security increased the risk that sensitive computing resources and data could be inadvertently or deliberately misused or destroyed. In response to our observations, LANL corrected the control issues associated with the telecommunications and utility rooms before the end of our site visits. Regarding control of vehicular traffic, LANL's former Chief of Security told us that the laboratory was willing to accept the level of risk because it was infeasible to check every car entering the laboratory.

LANL Has Not Fully Implemented Key Information Security Program Activities for Its Unclassified Network

The information security weaknesses in LANL's unclassified network that we identified have occurred, in large part, because the laboratory has not yet fully implemented an information security program to ensure that controls are effectively established and maintained. Although LANL has implemented an effective security awareness training program, we identified a number of shortcomings in its overall information security management program, including risk assessments, policies and procedures, network security plan, security testing and evaluation, remedial action plans, and contingency planning and testing. Many of these cyber security deficiencies have been the subject of prior reports by DOE's Office of Independent Oversight and LASO. The most recent report, issued by the Office of Independent Oversight in February 2008, also documented significant weaknesses with LANL's unclassified information security program, including foreign nationals' access to the unclassified network. During our review, we found that LANL had granted over 300 foreign nationals access to its unclassified network from countries identified as sensitive by DOE, including China, India, and Russia. Some LANL and NNSA officials raised security concerns about the level of access given to foreign nationals from sensitive countries because of the valuable scientific and technological information contained on the laboratory's unclassified network.

Security Awareness Training Program Is in Place

People are one of the weakest links in attempts to secure systems and networks. Therefore, an important component of an information security program is providing required training so that users understand a system's security risks and their own role in implementing related policies and controls to mitigate those risks. As defined by the System Administration, Networking, and Security (SANS) Institute,⁹ security awareness training is designed to educate users on the appropriate use, protection, and security of information; individual users' responsibilities; and ongoing maintenance necessary to protect the confidentiality, integrity, and availability of information assets, resources, and systems from unauthorized access, use, misuse, disclosure, destruction, or disruption. FISMA requires each agency to develop, document, and implement an information security program that includes security awareness training to inform personnel of information security risks and of their responsibilities in complying with agency policies and procedures, as well as training personnel with significant security responsibilities for information security. LANL policy requires that all employees complete an initial computer security briefing prior to being granted access to the laboratory's information system resources, and it requires that employees complete annual refresher training. According to laboratory officials, each employee is required to have a training plan highlighting all of the training courses the employee is to receive for his or her job function.

According to LANL officials, there are several controls in place to ensure that individuals receive adequate computer security awareness and training that will help them develop and maintain their technical skills. For example, according to LANL officials, if employees do not complete their security awareness training on an annual basis, LANL suspends their access to security areas until they have taken the required training. LANL officials stated the badge identification system is linked to the security awareness course, and those individuals who return to the laboratory each succeeding year must take the annual computer security refresher so that they can retain access to building facilities. If individuals do not complete the course by their renewal date, LANL deactivates their badge, denies their access to LANL facilities, and directs them to report to the badge office to retake the computer security refresher course. The laboratory has also ensured that all employees have and complete training plans unique to their specific roles and responsibilities within the organization. For example, of the 20 training plans for organizational unit administrators we

⁹SANS was established in 1989 as a cooperative research and education organization.

reviewed, all had completed their computer security training courses, and their training plans were up to date. Because LANL has established a security awareness and training program, the unclassified network is at decreased risk that individual employee's responsibilities for the safety and security of the information system will be unclear, misunderstood, or improperly implemented.

Information Security Program Activities Have Numerous Shortcomings

LANL's information security program has not been fully implemented. Specifically, (1) its risk assessment was not comprehensive, (2) specific guidance was missing from policies and procedures, (3) the network security plan was incomplete, (4) system testing had shortcomings, (5) remedial action plans were incomplete and corrective actions were not always timely, and (6) the network contingency plan was incomplete and inadequately tested. Until LANL ensures that the information security program associated with its unclassified network is fully implemented, it will have limited assurance that sensitive data are adequately protected against unauthorized disclosure or modification or that network services will not be interrupted.

Although a Risk Assessment Was Completed, It Was Not Comprehensive

Identifying and assessing information security risks are essential steps in determining what controls are required. Moreover, by increasing awareness of risks, these assessments can generate support for the policies and controls that are adopted in order to help ensure that these policies and controls operate as intended. FISMA requires each agency to develop, document, and implement an information security program that includes periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. NIST guidelines state that the identification of risk for an IT system requires an understanding of the system's processing environment, including data and information, system and data criticality, and system and data sensitivity. Furthermore, according to NIST, risk management should identify threats and vulnerabilities, set priorities for actions to reduce risks, identify new controls or countermeasures, and determine risks remaining after implementing the new control, also known as residual risk. Office of Management and Budget (OMB) Circular A-130, appendix III, prescribes, as does DOE policy, that risk be reassessed when significant changes are made to computerized systems—or at least every 3 years.

Although the laboratory updated its risk assessment in June 2007 for the unclassified network, this assessment was not comprehensive but provided a general identification and analysis of threats, vulnerabilities,

and countermeasures and included a residual risk for most vulnerabilities. However, it did not fully characterize risks to the network. For example, the risk assessment did not identify risks for vulnerabilities exposed by previous DOE internal findings and LANL vulnerability testing. Also, we found vulnerabilities during our analysis that LANL had not previously addressed in its risk assessment. For example, strong authentication was often not required for internal network services such as e-mail and database logins. Risks associated with this vulnerability were not assessed. Without comprehensive risk assessments, risks to certain systems may be unknown and appropriate controls may not be in place to protect against unauthorized access or disclosure, or system disruption.

LANL is taking steps to strengthen its risk management program that improves identification and assessment of potential threats, vulnerabilities, assets, and information system controls. For example, in January 2008, LANL issued a new risk management procedure describing the detailed methodology. In addition, LANL developed a new comprehensive methodology to aid in conducting risk assessments and provided training on this new methodology. According to LANL officials, this new program is in compliance with both NIST and NNSA policies and guidance.

Policies and Procedures Have Shortcomings

Another key task in developing an effective information security program is to establish and implement risk-based policies, procedures, and technical standards that govern security over an agency's computing environment. If properly implemented, policies and procedures should help reduce the risk that could come from unauthorized access or disruption of services. Because security policies and procedures are the primary mechanisms through which management communicates views and requirements, it is important that these policies and procedures be established and documented. FISMA requires agencies to develop and implement policies and procedures to support an effective information security program. NIST issued security standards and related guidance to help agencies implement security controls, including appropriate information security policy and procedures. The DOE Chief Information Officer has also issued guidance on management, operational, and technical controls implementing the NIST security control requirements.

Shortcomings existed in LANL's information security policies and procedures. Although the laboratory developed and documented many information security policies and procedures, it did not always have specific guidance for implementing federal and departmental requirements in the network environment. The laboratory had issued a local cyber

security policy describing the cyber security program framework and an implementation procedure describing roles, responsibilities, authorities, and accountability. Furthermore, it had issued specific guidance on user passwords, use of nongovernmental computers on the network, and the configuration of computers using Microsoft Windows that are connected to the network. However, the cyber security guidance the laboratory used did not follow guidance issued by DOE's Chief Information Officer or NIST standards and guidance for categorizing information systems and developing minimum security controls. In addition, the policy was not always comprehensive. For example, LANL implemented a policy requiring centralized configuration management for its Windows environment, but the policy did not address other systems the laboratory uses, such as Macintosh and Linux. At the time of our site visits, the laboratory had drafted, but not issued, specific policies and procedures on topics such as cyber security risk management, certification and accreditation, access control, and incident management. Without effectively developing, documenting, and implementing timely policies, procedures and standards, the laboratory has less assurance that its systems and information are protected from unauthorized access.

LANL was making an effort to improve its information security policies and procedures. During our site visits, the laboratory's Cyber Security group was undertaking a policy development and publication effort to review, revise, and issue policies as necessary to ensure compliance with DOE and NNSA policy. However, until LANL completes this effort, its information security program will not be fully effective.

Network Security Plan Was Incomplete

An information system security plan should provide a complete and up-to-date overview of a system's security requirements and describe the controls that are in place or planned to meet those requirements. OMB Circular A-130 specifies that agencies develop and implement system security plans for major applications and for general support systems and that these plans address policies and procedures for providing management, operational, and technical controls. In addition, NIST recommends that security plans include, among other topics, existing or planned security controls, the individual responsible for the security of the system, description of the system and its interconnected environment, and rules of behavior. NIST also requires federal agencies to document minimum security controls. Furthermore, DOE and NNSA policy requires that LANL develop an overall cyber security program plan, and specific system security plans as part of its certification and accreditation (C&A) process. NNSA policy further states that all documentation relevant to the system C&A should be referenced or included in the system security plan;

this includes the risk assessment results, security test and evaluation plan, and procedures and contingency plan(s).

The laboratory had documented an overall cyber security program plan and a security plan for the unclassified network infrastructure, but the network security plan was incomplete and not up-to-date. The laboratory-wide plan followed DOE policy guidance, and the network security plan addressed certain security controls recommended by NIST, such as the description of individuals responsible for security and rules of behavior. However, the network security plan had not been updated to address many of the controls NIST recommended. For example, the network security plan only partially addressed access controls and system communication protection controls and was incomplete because it did not include or reference some key security activities, such as the risk assessment results and security test plans, as stated in NNSA policy guidance.

Although DOE had issued guidance implementing FISMA and related NIST requirements, a laboratory cyber security official said LANL was waiting on detailed implementation instructions from NNSA and that it intends to revise the security plan by October 2008 to use controls from NIST guidance. Unless it uses the most current guidance on security controls, the laboratory cannot ensure that appropriate controls are documented in a security plan and in place to protect its systems and critical information.

Security Testing and Evaluation Process Has Shortcomings

Another key element of an information security program is testing and evaluating system controls to ensure they are appropriate and effective and comply with policies. FISMA requires each agency to develop, document, and implement an information security program that includes periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, performed with a frequency depending on risk, but no less than annually. The program is to include testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems. NIST provides guidance to agencies for assessing security control effectiveness and for performing network security testing, and states that security test results should be appropriately documented. Similarly, DOE guidance specifies that all controls identified in the security plan are subject to assessment procedures, and that the breadth and depth of testing activities should be documented.

The laboratory had various initiatives under way to test and evaluate system controls in its unclassified network at the time of our review, but

we found shortcomings in the testing process. In fiscal year 2007, LANL conducted a self-assessment of the unclassified security program using NIST's specified security controls. However, most controls were not assessed at a very detailed level—with only 3 of the 17 control areas being assessed in more detail using certain questions and security performance tests derived from NIST guidance. The laboratory also annually tests the controls in the security plan and conducts continuous automated testing to detect network vulnerabilities. However, this testing was limited because the controls identified in the security plan were not developed using NIST guidance. For example, the NIST control for configuration settings was not documented in the network security plan. Furthermore, although testing requirements were stated in the test documentation, officials said that the breadth and depth of the testing, as well as the results of the tests, were not always documented and available for examination. Furthermore, the automated testing was not comprehensive. LANL did not use an automated scanning tool to detect vulnerabilities in databases, and virtual web hosts or source code. Our tests identified vulnerabilities such as outdated database software and unpatched third-party applications. Without appropriate tests and evaluations of system controls, the laboratory has limited assurance that policies and controls are appropriate and working as intended. Additionally, without these tests and evaluations, there is a higher risk that undetected vulnerabilities could be exploited to allow unauthorized access to sensitive information.

Remedial Actions Were Not Taken in a Timely Manner and Plans Were Incomplete

Remedial action plans, also known as plans of actions and milestones, can help agencies identify and assess security weaknesses in information systems and set priorities and monitor progress in correcting them. FISMA requires each agency to develop, document, and implement an information security program that includes a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in its information security policies, procedures, or practices. According to OMB Circular A-123, agencies should take timely and effective action to correct deficiencies that they have identified through a variety of information sources. To accomplish this, agencies should develop remedial action plans and track progress for correcting each deficiency. A plan should detail the resources required to carry out the plan, any milestones in meeting the tasks, and scheduled completion dates for those milestones. OMB also states that the resource estimates should include the anticipated source of funding and whether the reallocation of resources or a request for new funding is anticipated. DOE requires that plans of action and milestones serve as a management tool for tracking corrective actions associated with program and system-level weaknesses.

Although the laboratory had a management process for identifying, evaluating, and documenting issues and tracking corrective actions, it did not always take actions in a timely manner and the plans were incomplete. For example, the laboratory's plan of actions and milestones addressed findings for eight weaknesses identified by DOE's Office of Independent Oversight in December 2006 by establishing 63 milestones. In August 2007, LANL's tracking report showed that tasks associated with 26 of these milestones were past due. Although a tracking report completed a month later indicated that only 11 milestones were still past due, evidence had not been submitted to validate that the recently completed milestones had been satisfactorily met. An additional 6 milestones had no completion dates in these tracking reports so their status could be determined and effectively monitored. In addition, the plans did not include estimated resources required to correct weaknesses. Finally, several findings from the laboratory's self-assessment were not included in the plan. Without an effective remediation program, identified vulnerabilities may not be resolved in a timely manner, thereby allowing continuing opportunities for unauthorized individuals to exploit these weaknesses to gain access to sensitive information and systems.

Network Contingency Plan Was Incomplete and Testing Was Inadequate

Contingency planning is a critical component of information protection. If normal operations are interrupted, network managers must be able to detect, mitigate, and recover from service disruptions while preserving access to vital information. Therefore, a contingency plan details emergency response, backup operations, and disaster recovery for information systems. It is important that these plans be clearly documented, communicated to potentially affected staff, and updated to reflect current operations. In addition, testing contingency plans is essential to determine whether the plans will function as intended in an emergency situation.

FISMA, NIST, DOE, and NNSA require contingency plans. FISMA requires each agency to develop, document, and implement an information security program that includes plans and procedures to ensure continuity of operations for information systems that support the agency's operations and assets. NIST requires that all agencies' systems have a contingency plan and that the plans address, at a minimum, identification, and notification of key personnel, plan activation, system recovery, and system reconstitution. In addition, the process should include a business impact assessment to determine what recovery strategies should be implemented to ensure availability and to fully characterize the system's requirements, processes, and interdependencies to determine contingency requirements and priorities. Furthermore, NIST requires that the plan be reviewed for

accuracy and completeness at least annually and that testing occur annually and when significant changes are made to the IT system, supported business processes, or the contingency plan. DOE and NNSA also require contingency plans to ensure that the department can continue to perform and support functions in the event of a service disruption, and these plans must be updated and tested annually.

The contingency plan LANL has implemented for its unclassified network is incomplete, outdated, and testing is inadequate. The laboratory had drafted a disaster recovery and contingency planning procedural document that details how the laboratory should prepare a contingency plan and testing procedures, and it notes the importance of contingency planning and testing. However, at the time of our site visits, the document had not been made final or provided to employees for review. In addition, at the time of our site visits, the most current contingency plan was over 4 years old and did not include key elements, such as identification and notification of key personnel, plan activation, system recovery, and system reconstitution. Also, LANL had not completed a business impact assessment to determine what recovery strategies should be implemented at the laboratory to ensure availability of system resources during a service disruption. LANL had also not tested the contingency plan annually. Furthermore, the test plan that was used was inadequate. The test plan was a checklist of regulatory questions that were checked-off and then signed and dated by an approving official. This generic checklist laid out several areas to review and provided an associated testing procedure, but did not adequately follow the contingency plan. Until LANL identifies the essential processes that should be included in a contingency plan and sufficiently tests the plans, it faces higher risk that the unclassified network infrastructure will not be able to effectively recover and resume normal operations after a disruption.

DOE Assessments Have Identified Significant Management Weaknesses Governing the Unclassified Network

DOE's Office of Independent Oversight and LASO have prepared reports identifying weaknesses with the management of LANL's unclassified cyber security program. These reports have surfaced numerous problems that can be traced to management deficiencies at NNSA, LASO, and the laboratory itself. The most recent reports, covering 2006 and 2007, identified problems in several specific areas: risk assessment; leadership; certification and accreditation; security testing; and policies and procedures. Key findings in each of these areas included the following:

- *Risk assessment.* LANL's risk assessment methodology is not comprehensive enough to address system-specific risks and does not

provide LASO with an appropriate appraisal of the risk in the unclassified environment. It also does not identify residual risks for acceptance or the development of appropriate mitigation strategies. As a result, the threats, vulnerabilities, and consequently the risks to LANL's unclassified systems cannot be quantified.

- *Leadership.* NNSA has not exercised management and oversight responsibilities so that LANL ensures effective implementation of the unclassified cyber security program. Furthermore, LASO has not exercised its oversight responsibilities for managing and accepting risks for the laboratory's unclassified cyber security program and has not provided sufficient leadership to resolve LANL performance problems and establish a clear set of management priorities. Finally, LANL has not exercised sufficient leadership within the unclassified program to ensure effective implementation of management and technical processes. In a 2007 follow-up report, the Office of Independent Oversight found that NNSA and/or the contractor, Los Alamos National Security, LLC (LANS),¹⁰ had taken steps to improve leadership, including (1) hiring a new Chief Information Officer at LANL who reports directly to the laboratory Director, (2) allocating additional funding to establish increased federal oversight activities at LASO, and (3) creating cyber security advisors to assist the laboratory's directorates.
- *Certification and accreditation.* LANL's C&A process is significantly deficient and cannot certify that unclassified systems and information are appropriately protected. The current process is based on security directives and guidance that are obsolete, rather than on NNSA, DOE, or national policies. In addition, neither the LANL unclassified network security plan nor any other security plan addresses the accreditation of servers, workstations, firewalls, routers, and other IT resources that LANL personnel use to process all levels of unclassified information. Furthermore, the laboratory's cyber security program plan gives a broad range of the possible number of systems on the unclassified network (25,000 to 35,000) on a daily basis, which contributes to the perception that LANL cannot accurately identify its unclassified assets. According to the Office of Independent Oversight's most recent assessment, LANL has made little or no progress to correct the identified deficiencies.

¹⁰LANS, LLC is a consortium of contractors that includes Bechtel National, Inc.; the University of California; BWX Technologies, Inc.; and the Washington Group International, Inc. In June 2006, LANS replaced the University of California, which had been the exclusive management and operating contractor of LANL since the 1940s.

-
- *Security testing.* LANL’s security testing and evaluation is not robust enough to ensure the security of the unclassified network. While security tests have been prepared, there is little actual testing of the controls associated with the unclassified network. Rather, individual tests are used to validate security plan statements. As a result, the security testing process does not demonstrate that the management, operational, and technical controls function as intended.
 - *Policies and procedures.* LANL’s policies and procedures have not been updated to address changing management, operational, and technical needs in the unclassified environment. While the unclassified cyber security program had been implemented within the framework of overarching policy provided by DOE, a serious weakness of LANL’s unclassified cyber security program is that its policies were based on obsolete directives and had not fully implemented all NNSA and DOE policies concerning cyber security. In addition, LANL has not established a comprehensive set of policies, plans, and procedures for managing cyber security within LANL organizations. According to the Office of Independent Oversight, most aspects of weaknesses relating to formal cyber security policies, plans, and procedures have yet to be resolved, which places sensitive unclassified information at greater risk.

DOE’s Office of Independent Oversight and LASO Have Also Raised Concerns about Foreign Nationals’ Access to LANL’s Unclassified Network

DOE’s Office of Independent Oversight and LASO also reported that LANL had not fully implemented DOE policies and procedures for protecting sensitive but unclassified information from foreign nationals who have access to information technology resources.¹¹ The Office of Independent Oversight and LASO noted, among other things, that

- foreign nationals’ use of this information has not been fully evaluated for risk or information sensitivity. As a result, the laboratory does not have adequate assurance that foreign nationals pose no risk to sensitive unclassified computer systems;
- the only risk assessment specific to foreign nationals’ access to the site pertains to “benefit of work to home country;”
- LANL does not have specific procedures that describe policies and processes for managing foreign nationals’ access and a method to allow

¹¹According to LANL, a foreign national is anyone who is not a U.S. citizen. Immigrant aliens are considered foreign nationals.

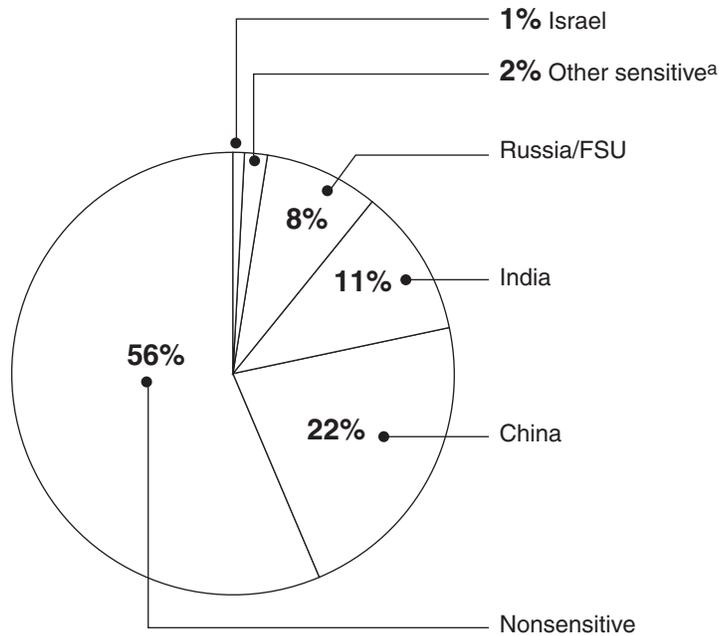
LANL's cyber security site manager to know what foreign nationals are on the network; and

- LANL has installed an additional 10 firewalls and improved firewall rules to enhance network segmentation, which allows better control of foreign nationals who have access to the unclassified network. However, LANL still needs to strengthen controls to further restrict access of those foreign nationals who are “scattered across the (unclassified) network and cannot be controlled by firewalls.”

We reviewed the status of foreign nationals' access to LANL's unclassified network. LANL policy states that foreign nationals working at the laboratory may have access to the information and administrative controls needed to perform authorized work. However, this policy has resulted in foreign nationals having widespread access to LANL's unclassified network and has raised concerns among some laboratory and NNSA officials about potential security risks. As of May 2008, LANL reported that 688 foreign nationals from 64 countries were authorized access to the unclassified network in their capacity as visitors, postdoctoral students, or permanent staff. Of the 688 foreign nationals, 301 (or 44 percent) were from countries classified as sensitive by DOE.¹² As figure 1 shows, 22 percent of all foreign nationals at the laboratory who were authorized access to the unclassified network were from China—one of the sensitive countries. Foreign nationals from other sensitive countries that had access to the unclassified network included India, Russia and other countries of the former Soviet Union (FSU), and Israel.

¹²A country is identified as sensitive based on national security, nuclear nonproliferation, or terrorism concerns.

Figure 1: Percentage of Foreign Nationals from Sensitive and Nonsensitive Countries at LANL with Unclassified Network Access, as of May 2008



Source: GAO analysis of LANL data.

^aAlgeria, Hong Kong, and Taiwan comprise the “other sensitive” category.

In addition, a significant number of foreign nationals from sensitive countries have been authorized remote access to LANL’s unclassified network.¹³ LANL’s Chief Information Officer told us that the security risks associated with granting this level of access to foreign nationals from sensitive countries has been far too great in the past and had reached an unacceptable level because of the valuable scientific and technological information contained on the laboratory’s unclassified network. As a

¹³Access to computer systems is granted using a standardized form that enables the approving official—either a laboratory Associate Director or Deputy Director—to authorize the type of computer resources provided to the foreign national such as unclassified network, visitor network, or remote unclassified network. In those instances where the laboratory division sponsoring the foreign national wants the individual to have remote access, the division must provide a justification statement. LANL policy, effective January 30, 2004, states that ample and sufficient justification for remote access must be provided to allow a cognizant laboratory group leader, division leader, and Associate Director to approve or disapprove.

result, LANL has reduced the number of foreign nationals from sensitive countries that have been granted remote access.

LANL's former Chief of Security and LANL's Chief Information Officer told us they were concerned about the large number of foreign nationals at the laboratory who have access to the unclassified network through remote or other means. In particular, the former Chief of Security asserted that it was a "bad idea" to have foreign nationals on the unclassified network. NNSA's Deputy Chief of Information Security questioned why any foreign nationals were authorized access to the network. In his view, all of their work should be done in a highly controlled cyber environment, with exceptions being granted on a very selective case-by-case basis.

LANL officials told us that unclassified network access for foreign nationals from both sensitive and nonsensitive countries is "a given." Foreign nationals employed at the laboratory require access to the unclassified network in order to carry out their duties and meet mission requirements. In fact, the foreign nationals in certain cases possess unique skills in science that cannot easily be found in the United States. The laboratory has seen a significant increase in foreign nationals' visit and assignment activities over the past 10 years. According to LANL, much of this increase in foreign national population is due to an increase in the foreign student population in U.S. graduate programs and a marked increase in foreign postdoctoral students, which is the laboratory's key source of its technical staff.

LANL Has Spent Approximately \$51.4 Million to Protect Its Unclassified Network from Fiscal Years 2001 through 2007, but Future Resource Requirements Need Better Justification

From fiscal years 2001 through 2007, LANL spent approximately \$51.4 million to protect its unclassified network. Nevertheless, LANL cyber security officials told us that funding has been inadequate to address some of their security concerns, such as the potential compromise or modification of sensitive unclassified data and a shutdown of computer systems and networks processing sensitive unclassified data. In response, NNSA's Chief Information Officer told us that LANL has not adequately justified its request for additional funds to address the laboratory's stated shortfalls. NNSA is now implementing a more systematic approach for developing information security budgets at LANL.

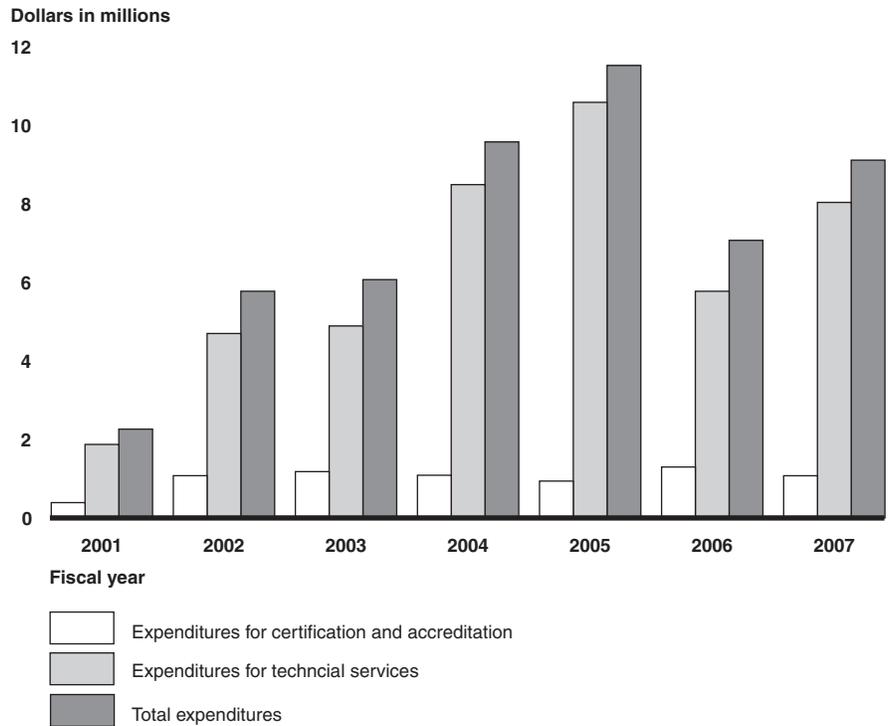
LANL Officials Assert That Resources Are Inadequate to Protect the Unclassified Network

LANL spent approximately \$51.4 million from fiscal years 2001 through 2007 to protect and maintain the unclassified network.¹⁴ The unclassified network expenditures have primarily been directed toward C&A and technical activities. LANL's C&A costs for the unclassified network cover such items as security plan development and maintenance, self-assessments, training, education, and awareness, media, and oversight of foreign nationals' access to the unclassified network. Technical costs involve items such as intrusion detection systems, network monitoring, antivirus services, e-mail monitoring, evaluating and testing security software before deployment, and incident cleanup.¹⁵ Figure 2 depicts LANL expenditures for the unclassified network over the period. As shown, LANL's overall security expenditures for the unclassified network increased from about \$2.3 million to \$9.1 million between fiscal years 2001 to 2007, with a peak of approximately \$11.5 million in fiscal year 2005. A reduction in spending occurred in fiscal year 2006, followed by a modest increase again in fiscal year 2007. The unclassified network expenditures for C&A activities have remained relatively stable around \$1 million from fiscal years 2002 to 2007, with the majority of unclassified network funds going toward technical activities.

¹⁴According to LANL, the laboratory spent approximately \$87.7 million from fiscal years 2001 through 2007 to protect and maintain the classified network.

¹⁵LANL officials explained to us that the cyber security budget is also broken down into C&A and technical activities for the classified network as well.

Figure 2: Annual Expenditures on LANL's Unclassified Network, Fiscal Years 2001-2007



Source: GAO analysis of LANL budget data.

Although cyber security expenditures increased from fiscal years 2001 to 2007, LANL officials told us this funding has been inadequate to protect the unclassified network and overall cyber security program. In a September 27, 2006, letter to the NNSA Administrator, the Directors of LANL, Lawrence Livermore National Laboratory, and Sandia National Laboratories stated that proposed reductions in the cyber security budget would expose the laboratories and NNSA to an unacceptable level of security and operational risk. The laboratory Directors emphasized that the inevitable effect of cuts in cyber security funding would be to forgo improvements in the classified network while also reducing support for the unclassified network. The lack of funding would be particularly harmful to the unclassified network because it is essential to productivity, a key factor in transforming the nuclear weapons complex, and is clearly a target for external attack. According to LANL's fiscal year 2008 budget request to NNSA, the laboratory needed approximately \$1 million more than the \$7.7 million it was allocated to implement an effective program

for its unclassified network. NNSA's allocation and LANL's request represent an approximate 11 percent difference for the unclassified network in fiscal year 2008. According to a LASO analysis identifying the impacts of failing to fully fund the LANL cyber security program, the shortage of funding exposes the unclassified network to several potential risks, including the following:

- the compromise, inappropriate access, or modification of sensitive unclassified data;
- a shutdown of computer systems and networks processing sensitive unclassified data, without additional systems or networks being approved to process these data;
- placement of LANL in noncompliance with DOE guidance;
- a significant gap in the laboratory's information protection capabilities (i.e., virus scans and firewalls);
- the severe hampering of laboratory efforts to identify the devices and levels of sensitivity of information on the unclassified network;
- impaired ability to verify the secure configuration of systems on the unclassified network; and
- the hampering of the laboratory's efforts to follow up on computer compromises.

LANL officials also told us that due to staffing and funding constraints, the laboratory could not provide all of the security measures that it determined necessary for an effective cyber security program, and, therefore, individuals or groups might be able to penetrate LANL's networks and gain access to sensitive information. In its analysis of the potential consequences of unfunded unclassified network activities for fiscal year 2007, LANL asserted that because of a lack of funding to perform self-assessments, there was a risk that the laboratory's ability to discover and address cyber deficiencies would be weakened. In addition, there was a risk that unclassified network users could not receive cyber security training, which creates serious potential for user-introduced vulnerabilities to the unclassified network. Moreover, there was risk that LANL could not ensure that media (e.g., disks) containing sensitive unclassified information would be properly sanitized or destroyed.

NNSA officials told us that they strongly disagreed with LANL's assertion that the laboratory does not have adequate funding for unclassified network activities. According to NNSA's Chief Information Officer, LANL's requests for additional funds to meet the laboratory's stated shortfalls have not been adequately justified. NNSA also found the claims made by the laboratory Directors about funding shortfalls in their 2006 letter to be unsubstantiated. In addition, NNSA officials stated that the laboratories were inconsistent in how they reported cyber security funding requests to NNSA. For example, prior to fiscal year 2006, LANL produced budget requests using terminology not sanctioned or used by NNSA budget processes by categorizing funding levels for cyber security activities as "minimal," "effective," and "essential." Furthermore, NNSA officials stated that LANL's past cyber budget requests were prepared on an ad hoc basis and were not based on well-defined threat and risk assessments.

NNSA Is Attempting to Implement a More Systematic Approach for Developing Information Security Budgets at LANL

Since 2006, NNSA has been developing a more systematic approach for developing cyber security budgets at LANL and the other national laboratories. NNSA officials in the Chief Information Office told us that because of the shortcomings in LANL's cyber security budget preparation process, NNSA has developed standard budget guidance and terminology. NNSA and the laboratories worked together to create a standard budget template—a work breakdown structure—for the laboratories to use in requesting and allocating cyber security funding. The work breakdown structure is to be used for both the classified and unclassified networks. More specifically, NNSA cyber security officials told us that this structure provides a framework for LANL to use in determining what cyber security activities it will fund, how much it will give to each activity, and how it will set priorities for funding activities and assessing unfunded activities.¹⁶ In addition, NNSA's Chief Information Office has identified a Designated Approving Authority (DAA), a federal official at each national laboratory site office, to determine site risks and approve budgets. Individual program officials at each laboratory provide budget information and risk assessments to their respective DAA to weigh the risks and weaknesses of the cyber security program to determine how to allocate funds.

¹⁶LANL officials told us that the laboratory began tracking cyber security financial figures toward the work breakdown structure in fiscal year 2006, but added that the unclassified network funding figures cannot be broken down into all the cyber security program activities listed in the work breakdown structure because some expenditures, such as "program management" and "incident response" cover both the classified and unclassified networks.

Nevertheless, NNSA officials could not provide us with guidance documenting how the laboratories should set budget priorities for cyber security activities. An NNSA official acknowledged that the agency has not yet produced any guidance on how to set funding priorities for the unclassified network but that NNSA is working on a plan to document the methodology it uses to approve and deny funding requests based on comprehensive assessments of risks and threats for specific work breakdown structure activities. Furthermore, NNSA does not consistently document its resource allocation decisions for cyber security or identify how funding shortfalls affect critical cyber security issues. NNSA cyber security officials stated that the laboratories estimate the impact of the failure to fund cyber security activities but acknowledged the need for NNSA to develop a process to better track activities that do not receive funding. NNSA officials believe that implementing a complex-wide approach to documenting budget decisions will help the agency develop a more systematic, transparent approach for determining appropriate cyber security funding levels.

Conclusions

Ensuring the confidentiality, integrity, and availability of sensitive information transmitted over LANL's unclassified network is a national security priority because the unauthorized disclosure of sensitive information or data from the unclassified network could have serious consequences. While the laboratory has taken steps to protect sensitive information, a number of weaknesses in security controls raise concerns. These weaknesses include, among other things, keeping information on the unclassified network out of the reach of unauthorized users.

Securing sensitive information on LANL's unclassified network requires that the laboratory's management establish, implement, and reinforce policies, procedures, and guidance for its employees to follow. In our view, these policies and procedures lay the foundation for an effective and sustainable security culture. While LANL has instituted components of a laboratory-wide information security program, key activities, such as the assessment of information security risks, and the development of policies and procedures that adhere to federal requirements, were not fully implemented or were absent. Furthermore, until LANL fully implements a laboratory-wide information security program that includes comprehensive risk assessments, risk-based policies and procedures, security plans, and a continuity of operations process, it has limited assurance that its sensitive data on the unclassified network will be adequately protected. For example, the large number of foreign nationals—particularly those from countries identified as sensitive by

DOE—who have access to the laboratory’s unclassified network raises serious security concerns. While there can be a legitimate need for foreign nationals to have access to LANL’s unclassified network to carry out mission-related responsibilities we believe it is prudent to control and restrict this level of access, whenever possible. To that end, we believe the laboratory has taken a positive step by significantly reducing the number of foreign nationals from sensitive countries that are authorized to have remote access to the unclassified network.

Establishing a comprehensive information security program requires a well thought out process for determining resource requirements, based on risk. We are concerned that neither NNSA nor LANL has developed a satisfactory approach to address this matter. In our view, the lack of a systematic process for identifying and allocating resources for those areas deemed to be highest risk can be traced directly to the absence of well-documented procedures and guidelines. Without a rigorous and disciplined approach, it is difficult to determine what the laboratory’s true resource requirements are to implement a comprehensive information security program for the unclassified network.

Recommendations for Executive Action

To improve LANL’s information security program for its unclassified network, we recommend that the Secretary of Energy and the Administrator of NNSA require the Director of Los Alamos National Laboratory to take the following eight actions:

- Ensure that the risk assessment for the unclassified network evaluates all known vulnerabilities and is revised periodically;
- Strengthen policies with a view toward further reducing, as appropriate, foreign nationals’—particularly those from countries identified by DOE as sensitive—access to the unclassified network;
- Ensure that the new set of cyber security policies and procedures applicable to the unclassified network are comprehensive, including centralized configuration management for all types of systems, and contain specific instructions on how to implement federal requirements and guidance;
- Ensure that the network security plan for the unclassified network is revised to document security controls using federal guidance and that this plan also includes or references key security activities, such as risk assessment development and the evaluation of security test results;

-
- Strengthen the security test and evaluation process for the unclassified network by expanding technical testing to cover new areas that might be vulnerable, such as those disclosed in our report, and ensure that testing adequately considers federal guidance for evaluating security controls and determining their effectiveness;
 - Ensure that milestones in corrective action plans are met or that new milestones are established to remediate security weaknesses for the unclassified network in a timely manner.
 - Ensure that the related plan of action and milestones used for FISMA reporting includes all LANL security weaknesses and required information so that it is an effective management tool for tracking security weaknesses and identifying budgetary resources needed to protect the unclassified network; and
 - Develop and maintain a comprehensive continuity of operations plan that addresses the current unclassified network environment and periodically test the plan for restoring operations.

To ensure that NNSA has a clear and consistent strategy to determine resource requirements for the laboratory's unclassified network, we recommend that the Secretary of Energy and the Administrator of NNSA take the following three actions:

- Develop, document, and implement a process that clearly links resource requirements and funding decisions to risk assessments for the unclassified network;
- Implement a process that provides a rationale for approving or denying resource requests for the unclassified network; and
- Establish and implement procedures to monitor critical program activities that are unfunded or underfunded in order to improve management accountability and transparency in determining how best to fund the most critical program requirements.

We are also making 41 detailed recommendations in a separate report with limited distribution. These recommendations consist of actions to be taken to correct the specific information security weaknesses related to identification and authentication, cryptography, audit and monitoring, configuration management, and physical security.

Agency Comments and Our Evaluation

We provided NNSA with a copy of this report for review and comment. NNSA did not specifically comment on our recommendations. However, NNSA agreed with our general conclusion that LANL has taken steps to protect sensitive information and acknowledged that there was considerable work yet to be done. NNSA also stated that LANL is currently responding to a DOE Secretarial Compliance Order requiring the laboratory contractor to take comprehensive steps to ensure that it identifies and addresses, among other things, critical cyber security deficiencies. The July 2007 Compliance Order was issued after a subcontractor employee removed classified information from LANL without authorization. The Order requires LANL to submit an integrated corrective action plan to address critical security issues. These steps must be completed by December 2008, and violations of the Compliance Order would subject the laboratory's contractor to civil penalties of up to \$100,000 per violation per day until compliance is reached.

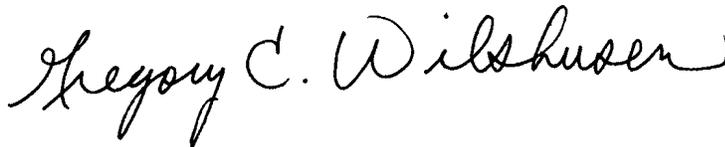
NNSA noted that responding to the issues identified in this report—as well as more technical issues included in a limited official use only version of this report—will extend beyond the completion of the Compliance Order since the actions we recommend are sufficiently more complex. We would expect that our recommendations, when implemented, would complement and be consistent with other remedial actions taken to improve LANL's cyber security posture as part of the Secretarial Compliance Order. Furthermore, NNSA stated that it will exercise the leadership necessary to correct the deficiencies identified in our report and will implement controls and processes complex-wide to demonstrate that it is successfully managing risk. NNSA's comments on our draft report are presented in appendix II.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to interested congressional committees; the Secretary of Energy; the Administrator of NNSA; the Director of LANL; and other interested parties. We will also make copies available to others upon request. In addition, this report will be made available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact Gene Aloise at (202) 512-3841 or aloisee@gao.gov; Greg Wilshusen at (202) 512-6244 or wilshuseng@gao.gov; or Nabajyoti Barkakati at (202) 512-6412 or barkakatin@gao.gov. Contact points for our Office of Congressional Relations and Public Affairs may be found on the last page of this report. Major contributors to this report are included in appendix III.



Gene Aloise
Director, Natural Resources and Environment



Gregory C. Wilshusen
Director, Information Security Issues



Nabajyoti Barkakati
Director, Center for Technology and Engineering

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to (1) assess the effectiveness of the security controls the Los Alamos National Laboratory (LANL) has implemented to protect information transmitted over its unclassified computer network; (2) assess whether LANL had fully implemented an information security program to ensure that controls were established and maintained for its unclassified computer network; and (3) examine the expenditure of funds used to protect LANL's unclassified network from fiscal years 2001 through 2007.

To determine the effectiveness of the security controls LANL had implemented to protect information transmitted over its unclassified computer network, we gained an understanding of the overall network control environment and identified its interconnectivity and control points. Our evaluation was based on our Federal Information System Controls Audit Manual (FISCAM),¹ which provides guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized information.

Using National Institute of Standards and Technology (NIST) standards and guidance, and Department of Energy (DOE) and National Nuclear Security Administration (NNSA) policies, procedures, practices, and standards, we

- developed an accurate understanding of the overall network architecture and examined routers, network management servers, switches, and firewalls;
- analyzed the effectiveness of controls used to establish individual accountability and control network access;
- observed methods for providing secure data transmissions across the unclassified network to determine whether sensitive data was being encrypted;
- evaluated controls intended to limit, detect, and monitor electronic access to sensitive computing resources and the effectiveness of these controls in protecting computing resources from unauthorized disclosure and modification;

¹GAO, Federal Information System Controls Audit Manual, [GAO/AIMD-12.19.6](#) (Washington, D.C.: January 1999).

- evaluated control configurations of selected servers and database management systems to assess the management of security features for network components; and
- observed and tested physical access controls to determine if computer facilities and resources were being protected from espionage, sabotage, damage, and theft;

In addition, we obtained views and documentation on these issues from security officials at DOE, NNSA, the Los Alamos Site Office (LASO), and LANL.

To assess whether LANL had fully implemented an information security program to ensure that controls were established and maintained for its unclassified computer network, we used the requirements identified by FISMA, which establishes key elements for an effective information security program. We

- examined training records for personnel with significant security responsibilities to determine if they received training commensurate with those responsibilities;
- reviewed LANL's risk assessment process and risk assessments for the unclassified network to determine whether risks and threats were documented consistent with federal guidance;
- analyzed LANL's policies, procedures, practices, and standards to determine their effectiveness in providing guidance to personnel responsible for securing information and information systems;
- analyzed security plans to determine if management, operational, and technical controls were in place or planned and that security plans were updated;
- analyzed security testing and evaluation results for the unclassified network to determine whether management, operational, and technical controls were tested at least annually and based on risk;
- examined remedial action plans to determine whether they addressed vulnerabilities identified in LANL's security testing and evaluations; and
- examined contingency plans for the unclassified network to determine whether those plans had been tested or updated.

We also discussed with key security representatives and officials responsible for information security management at DOE, NNSA, LASO, and LANL, whether information security controls were in place, adequately designed, and operating effectively. In addition, we met with officials from DOE's Office of Independent Oversight and its Office of Inspector General, regarding any related prior, ongoing, or planned work in these areas.

To determine the amount of funds LANL spent to protect its unclassified network from fiscal years 2001 to 2007, we obtained and analyzed documentation on the LANL cyber security program and budget, such as the LANL Cyber Security Program Office Roles and Responsibilities; LASO's Annual Cyber Survey Report Activity for fiscal year 2007; National Nuclear Security Administration's cyber security policies; and LANL risk assessments. We also obtained and analyzed financial data on LANL's cyber security program and unclassified network from fiscal years 2001 to 2007. In addition, we met with cyber security officials from NNSA, LASO, and LANL. To assess the reliability of funding data, we (1) reviewed quality control procedures used to report funding information; (2) interviewed knowledgeable officials; and (3) based on document reviews, ensured that we had received all available information. We determined that the data were sufficiently reliable for the purposes of this report.

We conducted this performance audit from May 2007 to September 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the National Nuclear Security Administration



Department of Energy
National Nuclear Security Administration
Washington, DC 20585

August 19, 2008

OFFICE OF THE ADMINISTRATOR

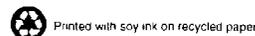
Mr. Gene Aloise
Director, Natural Resources
and Environment
Government Accountability Office
Washington, D.C. 20548

Dear Mr. Aloise:

The National Nuclear Security Administration (NNSA) appreciates the opportunity to review the Government Accountability Office's (GAO) draft report, GAO-08-1001, "INFORMATION SECURITY: Actions Needed to Better Protect Los Alamos National Laboratory's Unclassified Computer Network." We understand that this report is the result of an audit requested by the House's Committee on Energy and Commerce and the Subcommittee on Oversight and Investigations to determine security controls effectiveness, implementation of programs, and expenditures at Los Alamos.

NNSA agrees with the draft report's conclusion that in general, the Laboratory has taken steps to protect sensitive information but that more work needs to be done. As you are aware, the Laboratory is responding to a Secretarial Compliance Order that is designed to address a majority of the issues identified in this report and a subsequent report more technically focused. Responding to these reports will extend beyond the completion of the Secretarial Compliance Order requirements since the GAO's recommendations are sufficiently more complex.

NNSA will exercise the leadership necessary to correct deficiencies noted and to implement a dynamic framework of controls and processes that can be implemented complex-wide that will provide a level of confidence that NNSA is successfully managing risk. NNSA will provide detailed corrective actions to Congressional Committees through our formal Management Decision process.



**Appendix II: Comments from the National
Nuclear Security Administration**

2

Should you have any questions about this response, please contact Richard Speidel, Director, Policy and Internal Controls Management. He may be contacted at 202-586-5009.

Sincerely,



William C. Ostendorff
Principal Deputy Administrator

cc: Robert Smolen, Deputy Administrator for Defense Programs
David Boyd, Senior Procurement Executive
Bradley Peterson, Chief, Defense Nuclear Security
Donald Winchell, Revitalization Manager, Los Alamos Site Office
Linda Wilbanks, Chief Information Officer
Karen Boardman, Director, Service Center

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gene Aloise, (202) 512-3841, or aloisee@gao.gov
Gregory C. Wilshusen, (202) 512-6244, or wilshuseng@gao.gov
Nabajyoti Barkakati, (202) 512-6412, or barkakatin@gao.gov

Staff Acknowledgments

In addition to the individuals named above, Edward R. Alexander, Jr.; West E. Coile; Edward M. Glagola, Jr.; Jeffrey L. Knott; Glen Levis; Duc M. Ngo (Assistant Directors); Debra Conner; Kirk J. Daubenspeck, Jennifer R. Franks; Eugene H. Gray; Rosanna Guerrero; Preston S. Heard; Lisa N. Henson; Nicole Jarvis; John A. Spence; and Christopher J. Warweg made key contributions to this report. Other technical assistance was provided by Omari A. Norman, Rebecca Shea, and Carol Herrnstadt Shulman.

Related GAO Products

Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks. [GAO-08-526](#). Washington, D.C.: May 21, 2008.

Information Security: Progress Reported, but Weaknesses at Federal Agencies Persist. [GAO-08-571T](#). Washington, D.C.: March 12, 2008.

Information Security: Securities and Exchange Commission Needs to Continue to Improve Its Program. [GAO-08-280](#). Washington, D.C.: February 29, 2008.

Information Security: Although Progress Reported, Federal Agencies Need to Resolve Significant Deficiencies. [GAO-08-496T](#). Washington, D.C.: February 14, 2008.

Information Security: IRS Needs to Address Pervasive Weaknesses. [GAO-08-211](#). Washington, D.C.: January 8, 2008.

Information Security: Selected Departments Need to Address Challenges in Implementing Statutory Requirements. [GAO-07-528](#). Washington, D.C.: August 31, 2007.

Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses. [GAO-07-837](#). Washington, D.C.: July 27, 2007.

Information Security: Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US-VISIT Program. [GAO-07-870](#). Washington, D.C.: July 13, 2007.

Information Security: Homeland Security Needs to Enhance Effectiveness of Its Program. [GAO-07-1003T](#). Washington, D.C.: June 20, 2007.

Information Security: Agencies Report Progress, but Sensitive Data Remain at Risk. [GAO-07-935T](#). Washington, D.C.: June 7, 2007.

Information Security: Federal Deposit Insurance Corporation Needs to Sustain Progress Improving Its Program. [GAO-07-351](#). Washington, D.C.: May 18, 2007.

Information Security: FBI Needs to Address Weaknesses in Critical Network. [GAO-07-368](#). Washington, D.C.: April 30, 2007.

Related GAO Products

Information Security: Persistent Weaknesses Highlight Need for Further Improvement. [GAO-07-751T](#). Washington, D.C.: April 19, 2007.

Information Security: Further Efforts Needed to Address Significant Weaknesses at the Internal Revenue Service. [GAO-07-364](#). Washington, D.C.: March 30, 2007.

Information Security: Sustained Progress Needed to Strengthen Controls at the Securities and Exchange Commission. [GAO-07-256](#). Washington, D.C.: March 27, 2007.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548