

October 2009

INFORMATION SECURITY

Actions Needed to Better Manage, Protect, and Sustain Improvements to Los Alamos National Laboratory's Classified Computer Network



GAO

Accountability * Integrity * Reliability



Highlights of [GAO-10-28](#), a report to congressional committees

Why GAO Did This Study

The Los Alamos National Laboratory (LANL), which is overseen by the National Nuclear Security Administration (NNSA), has experienced a number of security lapses in controlling classified information stored on its classified computer network. GAO was requested to (1) assess the effectiveness of security controls LANL used to protect information on its classified network, (2) assess whether LANL had fully implemented an information security program to ensure that security controls were effectively established and maintained for its classified network, and (3) identify the expenditures used to operate and support its classified network from fiscal years 2001 through 2008. To carry out this work, GAO examined security policies and procedures and reviewed LANL's access controls for protecting information on its classified network.

What GAO Recommends

GAO recommends, among other things, that NNSA direct LANL to (1) fully implement its information security program, (2) centralize management of the classified network, and (3) develop a sustainability plan that details how it plans to strengthen recent cyber security improvements over the long term.

NNSA generally agreed with a draft of this report.

[View GAO-10-28 key components.](#)

For more information, contact Gene Aloise at (202) 512-3841 or aloisee@gao.gov; Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov; or Gregory Wilshusen at (202) 512-6244 or wilshusen@gao.gov.

INFORMATION SECURITY

Actions Needed to Better Manage, Protect, and Sustain Improvements to Los Alamos National Laboratory's Classified Computer Network

What GAO Found

LANL has implemented measures to enhance its information security controls, but significant weaknesses remain in protecting the confidentiality, integrity, and availability of information stored on and transmitted over its classified computer network. The laboratory's classified computer network had vulnerabilities in several critical areas, including (1) uniquely identifying and authenticating the identity of users, (2) authorizing user access, (3) encrypting classified information, (4) monitoring and auditing compliance with security policies, and (5) maintaining software configuration assurance.

A key reason for the information security weaknesses GAO identified was that the laboratory had not fully implemented an information security program to ensure that controls were effectively established and maintained. Shortfalls in the program include, among other things, (1) the lack of comprehensive risk assessments to ensure that appropriate controls are in place to protect against unauthorized use, (2) not developing detailed implementation guidance for key control areas such as marking the classification level of information stored on the classified network, (3) inadequate specialized training for users with significant security responsibilities, and (4) not adequately developing and testing disaster recovery and contingency plans to mitigate the laboratory's chances of being unsuccessful at resuming normal operational standards after a service disruption. LANL's security plans and test plans were neither comprehensive nor detailed enough to identify certain critical weaknesses on the classified network. Furthermore, the laboratory's decentralized approach to information security program management has led to inconsistent implementation of policy, and although the laboratory has taken steps to address management weaknesses, its efforts may be limited because LANL has not demonstrated a consistent capacity to sustain security improvements over the long term.

Since fiscal year 2001, the laboratory has spent approximately \$433 million, in constant 2009 dollars, to operate and support its classified network. Between fiscal years 2001 and 2008, annual expenditures increased from about \$20 million to \$80 million. Expenditures for the core classified cyber security program, which serves as the foundation of LANL's protection strategy for the classified cyber security program, accounted for \$45 million of total expenditures over the period. According to LANL, funding for its core classified cyber security program has been inadequate for implementing an effective program during fiscal years 2007 and 2008. However, according to NNSA, it funded programs based on available resources and risk evaluations conducted at both the enterprise and site levels.

Contents

Letter		1
	Background	4
	Significant Information Security Control Weaknesses Remain on LANL's Classified Computer Network	7
	LANL Has Not Fully Implemented Key Elements of Its Information Security Program for Its Classified Computer Network	10
	LANL Has Spent More Than \$400 Million to Operate and Support Its Classified Computer Network Since Fiscal Year 2001, but LANL and DOE Officials Believe That Resources Are Inadequate to Mitigate Risks	20
	Conclusions	24
	Recommendations for Executive Action	25
	Agency Comments and Our Evaluation	27
Appendix I	Objectives, Scope, and Methodology	29
Appendix II	Comments from the National Nuclear Security Administration	32
Appendix III	GAO Contacts and Staff Acknowledgments	34
Figure		
	Figure 1: Annual Expenditures for LANL's Classified Computer Network, Fiscal Years 2001 through 2008	21

Abbreviations

DOE	Department of Energy
FISMA	Federal Information Security Management Act
FTE	full-time equivalent
LANL	Los Alamos National Laboratory
LANS	Los Alamos National Security, LLC
NIST	National Institute of Standards and Technology
NNSA	National Nuclear Security Administration
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
POAM	Plan of Actions and Milestones

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

October 14, 2009

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

The Honorable Bart Stupak
Chairman
The Honorable Greg Walden
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 Los Alamos National Security, LLC² for the National Nuclear Security Administration,³ has experienced a number of high-profile security lapses. Over the last decade, these lapses have included, but are not limited to, the

¹LANL, a multidisciplinary national security laboratory, conducts some of the nation's most sensitive activities, including designing, producing, and maintaining the nation's nuclear weapons; conducting efforts for other military or national security applications; and performing research and development in advanced technologies for potential defense applications. 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 about \$2 billion, with about \$1.5 billion devoted to nuclear weapons work.

²Los Alamos National Security, LLC (LANS) is a consortium of contractors that includes Bechtel National Inc.; the University of California; the Babcock and Wilcox Company; and the Washington Division of URS. In June 2006 LANS replaced the University of California, which had been the exclusive management and operating contractor of LANL since the 1940s.

³National Nuclear Security Administration (NNSA) was established in 2000 in response to management difficulties with DOE'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 DOE and is responsible for the nation's nuclear weapons, nonproliferation, and naval reactors programs.

inability to account for and control classified information. For example, in October 2006, evidence obtained during a drug-related investigation in Los Alamos, New Mexico, revealed that classified information—a “USB thumb drive” and several physical documents—had been improperly removed from the laboratory. This incident followed several others in 2003 and 2004, when LANL could not account for classified removable electronic media, such as compact disks and removable hard drives. In 2000, two pieces of this type of media containing nuclear weapon design information used by the Department of Energy’s (DOE) Nuclear Emergency Search Team were temporarily lost.⁴ Furthermore, in 1999, a LANL scientist transferred classified information from laboratory computer systems onto unmarked disks and removed the disks from the laboratory. Following the October 2006 event and an extensive investigation, DOE and National Nuclear Security Administration (NNSA) took formal enforcement actions against the University of California and Los Alamos National Security, LLC (LANS) for violations of classified information security requirements under their respective contracts.⁵ In addition to the assessment of civil penalties for both contractors, the Secretary of Energy issued a Compliance Order to LANS, which required the laboratory’s management and operating contractor to take 14 specific actions. These actions required LANS to, among other things, correct management deficiencies that contributed to the October 2006 incident and address long-standing deficiencies in the laboratory’s classified information and cyber security programs.⁶ The Los Alamos Site Office, which is a field component of

⁴The Nuclear Emergency Search Team provides technical capabilities to respond to potential and actual nuclear and radiological threats and incidents. See GAO, *Combating Nuclear Terrorism: Federal Efforts to Respond to Nuclear and Radiological Threats and to Protect Emergency Response Capabilities Could be Strengthened*, [GAO-06-1015](#) (Washington, D.C.: Sept. 21, 2006).

⁵Investigations revealed that management deficiencies of both contractors were a central contributing factor in a laboratory subcontractor employees unauthorized reproduction and removal of classified matter from the site.

⁶The Secretary of Energy has authority under 10 C.F.R. 824.4(b) of DOE’s Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations to issue compliance orders that direct management and operating contractors to take specific actions to remediate deficiencies that contributed to security violations. The July 2007 Compliance Order directed LANS to correct management deficiencies that contributed to the October 2006 incident and address long-standing deficiencies in the laboratory’s classified information and cyber security programs by December 2008. Violation of the Compliance Order would subject LANS to civil penalties of up to \$100,000 per violation per day until compliance was reached. In January 2009, NNSA’s Los Alamos Site Office formally validated that LANL successfully implemented all actions required by the Compliance Order in a timely manner and no additional civil penalties were levied.

NNSA and is responsible for day-to-day oversight of LANL cyber security activities, was responsible for ensuring that the laboratory satisfied the objectives of the Compliance Order.

At your request, we evaluated key elements of LANL's classified information security program for its classified computer network. Specifically, we (1) assessed the effectiveness of security controls used to protect information stored on and transmitted over its classified computer network, (2) assessed whether LANL had fully implemented an information security program to ensure that controls were effectively established and maintained for its classified computer network, and (3) identified the expenditure of funds used to operate and support the classified computer network from fiscal years 2001 through 2008. To accomplish these objectives, we examined the information security controls for five systems connected to the classified computer network at LANL that are critical to the laboratory's achievement of its nuclear weapon missions. In addition, we analyzed procedures and their implementation areas such as risk assessment, security awareness training, information security plans, security testing and evaluation, corrective action plans, and continuity of operations. Further, we identified and analyzed financial data provided by LANL that detailed classified computer network expenditures, and adjusted these expenditures to constant 2009 dollars.

We conducted this performance audit from November 2008 to July 2009 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.

This report summarizes shortcomings identified in information security controls on LANL's classified computer network. It does not contain specific examples of the weaknesses identified due to the sensitive nature of the information discussed. In a separate classified report, issued in July

2009, we provided specific examples and made recommendations to address the specific control weaknesses identified.⁷

Background

LANL is responsible for planning and executing all facets of the stockpile stewardship program, including assessing, refurbishing, and certifying nuclear weapons.⁸ To help carry out these critical missions, LANL uses its classified computing network to analyze results from nonnuclear experiments and to simulate the performance of nuclear weapons and their delivery systems to meet military requirements established by the Department of Defense. Due to the sensitivity of the information stored on and transmitted over the laboratory's classified computer network, LANL segregates this network from its other computer systems. The classified computer network consists of more than 3,900 computers and devices, serving about 3,800 users. The most restrictive information that can be processed on LANL's classified computer network is classified at the Secret-Restricted Data level, additionally controlled by Sigmas 1 through 13, 15, and 20.⁹ In addition, the following types of information can be stored on and transmitted over LANL's classified computer network: (1) open public unrestricted information, (2) unclassified protected information, (3) unclassified mandatory protected information, (4) confidential nonnuclear weapons information, (5) secret nonnuclear weapons information, and (6) confidential restricted data. However, all information stored on LANL's classified computer network is protected at the Secret-Restricted Data classification level.

⁷GAO, *Information Security: Actions Needed to Better Manage, Protect, and Sustain Improvements to Los Alamos National Laboratory's Classified Computer Network*, [GAO-09-745C](#) (Washington, D.C.: July 24, 2009).

⁸In the absence of nuclear testing, NNSA's Stockpile Stewardship Program was established to ensure that nuclear warheads and bombs in the U.S. nuclear weapons arsenal are safe, secure, and reliable. This effort uses several approaches, including test data and computer modeling, to detect any potential problems with nuclear weapons that affect their performance.

⁹The Secret-Restricted Data classification level generally protects nuclear weapon design information. Sigma categories provide additional need-to-know protections related to Restricted Data concerning the theory, design, manufacture, storage, characteristics, performance, effects, or use of nuclear weapons, nuclear weapon components, or nuclear explosive devices or materials. Sigma 14 or Top Secret data are not allowed to be received, processed, or stored on the laboratory's classified computer network. In addition, individuals that have access privileges to this type of information must possess the appropriate security clearances.

In July 2007, the Secretary of Energy issued a Compliance Order that directed LANS to implement specific action items by December 2008 to address long-standing deficiencies in the laboratory's classified information and cyber security programs, including the following:

- address organizational culture issues, including the lack of classified information protection by all employees and lack of leadership in classified information protection by LANL management;
- develop and implement an integrated corrective action plan for all previously identified classified information and cyber security issues;
- ensure full implementation of all NNSA cyber security requirements; and
- accredit all unclassified computer systems and reaccredit all classified computer systems.

A basic management objective for any organization is to protect the resources that support its critical operations from unauthorized access. To ensure the confidentiality, integrity, and availability of critical information and information systems used to support operations and assets of federal agencies, information security controls and complementary program activities are required. Effective controls are necessary to ensure the protection of information stored on 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.¹⁰

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

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

¹⁰For the purposes of this report, we are including LANL's classified cyber and computer network security programs as a key component of the laboratory's overall information security program.

-
- *Authorization* is the process of granting or denying access rights and privileges to a protected resource, such as a network, system, application, function, or file.
 - *Cryptography* underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information.
 - *Audit and monitoring controls* help establish individual accountability and monitor compliance with security policies.
 - *Configuration assurance* involves the (1) verification of the correctness of the security settings in the operating systems, applications, or computing and network devices and (2) maintenance of software in a secure fashion.

Information security program activities govern the security protections for the information and information systems that support the operations and assets of an 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) provides security awareness training to inform personnel of information security risks and of their responsibilities in complying with agency policies and procedures; (4) develops, documents, and implements plans to provide adequate information security for networks, systems, and facilities; (5) periodically tests and evaluates the effectiveness of information security policies, procedures, and practices relating to management, operational, and technical controls for every system; (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.

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.

In 2008, we issued two reports—a public version and a limited official use only version—regarding the effectiveness of the security controls protecting information stored on and transmitted over LANL’s unclassified computer network.¹¹ We made 11 recommendations to correct deficiencies identified in the public version of the report, including (1) ensuring that the risk assessment for the unclassified computer network evaluates all known vulnerabilities and is revised periodically and (2) strengthening 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. In a letter dated January 16, 2009, NNSA informed us that it concurred with all 11 recommendations in the public version of our report, noting that corrective action plans were either in place or being developed to address the identified deficiencies. We also made an additional 41 technical recommendations to improve specific computer security problems identified in our limited official use version of the report. NNSA informed us that it concurred with all 41 recommendations, noting that corrective actions were either in place or being developed in response to our report.

Significant Information Security Control Weaknesses Remain on LANL’s Classified Computer Network

While LANL had implemented measures to enhance the security controls protecting information stored on and transmitted over its classified computer network, significant security control weaknesses remain. LANL had vulnerabilities in several critical areas, including (1) identifying and authenticating the identity of users, (2) authorizing user access, (3) encrypting classified information, (4) monitoring and auditing compliance with security policies, and (5) maintaining software configuration assurance.

Strong Authentication Was Implemented but Was 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 a unique user account to a specific user, the system is able to distinguish one user from another—a process called identification. The system must also establish the validity of a user’s claimed identity by requesting some kind of information, such as a

¹¹GAO, *Information Security: Actions Needed to Better Protect Los Alamos National Laboratory’s Unclassified Computer Network*, [GAO-08-1001](#) (Washington, D.C.: Sept. 9, 2008) and GAO, *Information Security: Actions Needed to Better Protect Los Alamos National Laboratory’s Unclassified Computer Network*, [GAO-08-961SU](#) (Washington, D.C.: Sept. 9, 2008).

password, that is known only by the user—a process known as authentication. NNSA policy states that individuals must not share passwords except in emergency circumstances or when there is an overriding operational necessity, as described in the system’s approved security plan. In addition, the policy requires that passwords be changed at least every 6 months on systems where the consequence of loss of confidentiality or integrity for any information group is medium to high risk. Furthermore, LANL’s password policy requires that one-time passcodes—using token cards and personal identification numbers, that is, two-factor authentication—be used whenever possible or practical.

LANL did not always manage passwords securely on the classified computer network. As a result of this weakness, increased risk exists that insiders with malicious intent could guess the passwords of other individuals and use them to gain inappropriate access to classified information.

Weaknesses Existed in Authorizing User Access

Authorization is the process of granting or denying access rights and privileges to a protected resource, such as a network, system, application, function, or file. A key component of authorization and a basic principle for securing computer resources and data is the concept of least privilege. Least privilege means that users are granted access only to those programs and files that they need in order to perform their official duties. According to NNSA policy, LANL is required to provide access to classified information only to individuals with the appropriate access authorizations and a need-to-know to do their jobs. In addition, NNSA policy states that configuring computer systems only for necessary capabilities minimizes processes and services, and only required services should be enabled. LANL policy also recommends that only required services should be installed on computer systems and requires the configuration of computer systems only for necessary processes and services.

LANL provided users with more access than needed to perform their duties and configured classified systems with more capabilities and services than required. As a result, there is an increased risk that users could access classified data they do not need to perform their duties.

Cryptography Was Not Always Effectively Used

Cryptography underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information. One such mechanism is encryption. Encryption can be used to provide basic confidentiality and integrity of transmitted or stored data by transforming

plain text into cipher text using a special value, known as a key, and a mathematical process, known as an algorithm. NNSA requires that cryptographic services be used to ensure that information maintains an adequate level of confidentiality and integrity based on the sensitivity of the information to be protected and the threat environment.

Although LANL employed encryption mechanisms to protect data on its network and servers, it did not always comply with NNSA policy. As a result, weaknesses in encryption increased the risk of exposing data to unnecessary disclosure or misuse by unauthorized individuals.

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 what, when, and by whom specific actions are taken on a computer system. Organizations accomplish this by implementing system or security software that provides an audit trail of needed information in the desired format and locations, so they can use it to determine the source of a transaction or attempted transaction and to monitor users' activities. The way in which organizations configure system or security software determines the nature and extent of information that the audit trails can provide. A key aspect of this process is managing audit logs. Organizations should periodically review audit log design, review processes and procedures, and implement changes, as needed, to ensure that logs effectively detect security threats. NNSA policy requires that all user activities, and activities on behalf of the user, should be monitored and reviewed for actions that are detrimental to the confidentiality, integrity, and availability of the information or information systems. In addition, intrusion detection measures, which also enhance monitoring capabilities, must be taken to detect unauthorized attempts to penetrate the system and respond to detected incidents on the classified computer network.

Weaknesses existed in audit and monitoring controls for LANL's classified computer network, and although LANL was logging certain events such as failed and successful login attempts, other events were not being captured. These weaknesses increase the risk that unauthorized activity would not be effectively detected or investigated.

Weaknesses Existed in Software Configuration Assurance

Configuration assurance is the process of (1) verifying the correctness of the security settings in the operating systems, applications, or computing and network devices and (2) maintaining operations in a secure fashion. Organizations should maintain software configuration to ensure protection

against vulnerabilities. According to the National Institute of Standards and Technology (NIST), all organizations should have a systematic, accountable, and documented process for managing exposure to vulnerabilities. Proactively mitigating the vulnerabilities of computer systems can reduce or eliminate the potential for exploitations to occur. However, LANL did not effectively mitigate certain vulnerabilities on its systems, and as a result, data was unnecessarily vulnerable to compromise.

LANL Has Not Fully Implemented Key Elements of Its Information Security Program for Its Classified Computer Network

LANL's information security program for its classified computer network had not been fully implemented. Specifically, (1) risk assessments were not comprehensive, (2) specific guidance was missing from policies and procedures, (3) the training and awareness program did not adequately address specialized training needs for individuals with significant network security responsibilities, (4) system security plans were incomplete, (5) the system security testing and evaluation process had shortcomings, (6) corrective action plans were not comprehensive, and (7) contingency plans were incomplete and not tested. In addition, the laboratory's decentralized management approach has led to weaknesses in the effectiveness of its classified cyber security program. Although the laboratory has taken steps to address these weaknesses, its efforts may be limited because LANL has not demonstrated a consistent capacity to sustain security improvements over the long term. Until LANL ensures that the information security program associated with its computer network is fully implemented, the laboratory will have limited assurance that classified information is adequately protected against unauthorized disclosure.

Although Risk Assessments Were Complete, They Were Not Comprehensive

Identifying and assessing information security risks are essential steps in determining the security controls required to ensure the protection of information and information systems. The cornerstone of an information system's security program is the risk management process, which determines the protection requirements for information. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.

The Federal Information Security Management Act of 2002 (FISMA) requires each agency to develop, document, and implement an information security program that periodically assesses the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information

systems.¹² DOE and NNSA require that their organizations and contractors develop and implement a risk management process to protect classified information systems. DOE's risk assessment process includes detailed analysis of areas such as threat assessment, the effect of countermeasures, the remaining vulnerability (residual risk), and the protection requirements and value of the information being processed. Furthermore, risks must be reassessed when significant changes are made to computer systems or at least every 3 years. In January 2008, LANL issued a new risk management procedure, consistent with NNSA risk management policy, describing the framework to identify and manage risks for classified systems. In addition, the LANL policy requires that risk assessment results be incorporated into the system's security plans and be used in the development of information system controls.

Although LANL had strengthened its risk assessment program, shortcomings remained. To satisfy the July 2007 DOE Compliance Order, the laboratory reaccredited all classified computer systems. During 2008, as part of its reaccreditation process, LANL revised risk assessments for classified computer systems and included the results in the system security plans. The laboratory also developed a new risk assessment process that included related training and a comprehensive tool to aid in conducting risk assessments. However, of the five system security plans we reviewed, one plan's risk assessment did not adhere to the latest methodology and did not include evidence of a comprehensive threat analysis, as required by DOE. Furthermore, the remaining four plans noted that all known threats and vulnerabilities were not evaluated to determine risks. Without comprehensive risk assessments, risks to certain systems may be unknown and appropriate controls may not be in place to protect against unauthorized access to or disclosure of sensitive information, or disruption of critical systems and operations.

Detailed Implementation Guidance Did Not Exist for Certain Cyber Security Policies and Procedures

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

¹²FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2946 (Dec. 17, 2002).

primary mechanisms through which management communicates its 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. DOE and NNSA have also issued cyber security policies and related guidance to help implement security controls. In March 2007, DOE issued a *National Security Systems Manual* that established a framework for addressing technical, operational, and assurance controls such as security audits, management of user identifiers and authenticators, and configuration management. Although NNSA did not issue implementing guidance for this manual until May 2008, the Los Alamos Site Office instructed LANL to comply with NIST guidance in lieu of existing policies and procedures.

LANL had yet to develop detailed implementation guidance for certain areas. Although the laboratory has developed and documented many information security policies and procedures, it did not always have specific, detailed guidance for implementing federal and departmental requirements in the classified network environment. For example, the laboratory had neither developed detailed implementation guidance for the services allowed for computer systems connected to the classified network nor indicated whether encrypted protocols should be used. In addition, recertification and accreditation testing for four of the systems we reviewed identified a lack of up-to-date or formal institutional guidance for audit and accountability, system and information integrity, and contingency planning. Further, no specific policy existed for marking computer files within the classified network's directory system. As a result, LANL did not (1) mark the classification level of any individual documents stored on its classified computer network or (2) maintain an inventory of the numbers and types of classified documents stored on the network. Because classified documents in electronic form were not marked or inventoried, the laboratory did not know the numbers and types of information stored on its classified computer network or whether classified information is accessed by unauthorized individuals or misused by authorized individuals. This increases the risk that the laboratory may not be able to detect inappropriate activities or conduct comprehensive investigations of security violations on the network. Without effectively developing, documenting, and implementing detailed guidance, the laboratory has less assurance that the confidentiality, integrity, and availability of its systems and information were protected.

LANL's Classified Cyber Security Training and Awareness Program Did Not Adequately Address Specialized Training

People are often one of the weaker links in attempts to secure systems and networks. Therefore, an important component of an information security program is providing necessary training, so that users understand a system's security risks and their own role in implementing related policies and controls to mitigate those risks. 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 to train personnel with significant security responsibilities for information security. DOE policy requires the establishment of a training, education, and awareness program that develops and maintains cyber security competencies, and further states that, for classified information systems, users should be properly trained in system security by identifying their system-specific training needs and assigned personnel. LANL policy requires that all employees complete an initial computer security briefing prior to being granted access to the laboratory's classified information system resources, and it requires that employees complete annual refresher training. LANL's policy also states that cyber security specialists must maintain a record of their local training that includes the content of the training.

LANL had an annual awareness training program in place, but not all individuals with cyber security responsibilities had received specialized training. We examined the training records for 176 individuals, with significant security responsibilities, whom LANL had categorized as privileged users for the five computer systems we reviewed.¹³ All privileged users had completed the annual awareness training, which is a general course required for all classified computer users. However, more specialized training was not given to all privileged users. For example, system administrators, who are privileged users, were not required to take additional specialized training, despite having significant cyber security responsibilities on the classified computer network. Because the LANL cyber security training program does not adequately address the specialized training that users with significant security responsibilities require, LANL is at an increased risk of a security compromise if privileged users are not sufficiently trained to effectively perform their cyber security roles and responsibilities on the classified computer network.

¹³Privileged users may include system administrators, cyber security officers, and line managers responsible for security.

System Security Plans Were Incomplete

An information system security plan should provide a complete and up-to-date overview of a computer system's security requirements and describe the controls that are in place or planned to meet those requirements. DOE and NNSA policy require that each national security system be covered by a system security plan. Furthermore, DOE requires that the minimum set of security controls for the system be documented in plans, including any additional implementation information for the controls. The NNSA cyber security program policy outlines the contents for system security plans, including documentation of the system security requirements. According to NIST standards, there are three general classes of security controls—management, operational, and technical—that should be implemented to protect information systems. LANL policy reinforces these requirements, stating that system security plans will describe the management structure, the security environment, and the technical controls needed to protect the information on the system.

Although LANL had developed system security plans, it had not adequately addressed certain technical controls. This is especially significant since the controls documented in the security plans serve as the basis for security testing and evaluation to ensure that appropriate controls are functioning properly to protect information stored on and transmitted over LANL's classified computer network. All five system security plans that we reviewed generally documented management, operational, and technical controls, and described the management structure and security environment. However, these plans did not cover certain technical controls where weaknesses existed. Until the plans sufficiently address technical controls, LANL has limited assurance that appropriate controls are in place to protect its classified computer network.

LANL's Security Testing and Evaluation Process Had 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 agency 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. The frequency of this testing depends on the risk, but must be conducted at least 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. 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. In January

2008, the Los Alamos Site Office instructed LANL to use NIST guidance for documenting and testing security controls.

Although LANL annually tested the controls in its system security plans and conducted continuous automated testing to detect network vulnerabilities, these tests were not comprehensive. During our review, LANL conducted certification testing for its classified computer systems using NIST guidance. Nevertheless, our own independent tests identified numerous vulnerabilities and related control weaknesses that were not identified in LANL's tests. Further, LANL did not conduct comprehensive vulnerability scans of the classified computer network. Without appropriate tests and evaluations of system controls, the laboratory has limited assurance that policies and controls are appropriate and working as intended. As a result, the classified computer network is at increased risk that it could be compromised. Additionally, without these tests and evaluations, there is a higher risk that undetected vulnerabilities could be exploited.

Corrective Action Tracking Had Improved, but the Laboratory's Remedial Action Plans Were Not Comprehensive

Remedial action plans, which include plans known as Plans of Action and Milestones (POAM), can help set priorities and monitor progress in correcting identified security weaknesses. 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 POAM instructions set forth by the Office of Management and Budget, these action plans must describe classified and unclassified weaknesses from a variety of sources-internal assessments, the inspector general, and GAO-and should track progress for correcting each deficiency. A POAM should also detail the resources required to carry out the plan, any milestones in meeting the tasks, and scheduled completion dates for those milestones. DOE requires that POAMs serve as a management tool for tracking corrective actions associated with program and system-level weaknesses.

The laboratory had a management process for identifying, evaluating, and documenting security weaknesses and tracking corrective actions, but had not yet reported certain weaknesses in its POAM. LANL also used a new process for tracking and reporting weaknesses and the status of its corrective action plans, which provide specificity regarding remediation. The POAM that the laboratory created generally contained all required elements and included estimated resources required to correct ongoing weaknesses. However, findings related to the laboratory's internal

weaknesses or assessments were not in the POAM. In addition, LANL had not yet developed corrective action plans to address the 104 system-level weaknesses identified in its certification testing for the five computer systems we reviewed. According to a Los Alamos Site Office official, LANL is working to create corrective action plans for these weaknesses. Until LANL includes all weaknesses in its remedial action program, identified vulnerabilities may not be resolved in a timely manner, thereby allowing continuing opportunities for unauthorized individuals to exploit these weaknesses.

LANL's Network Contingency Planning Was Incomplete and Testing Was Not Consistently Performed Across the Components of the Classified Computer Network

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 is needed to detail 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, it is essential to test contingency plans in order to determine whether the plans will function as intended in an emergency situation.

Federal law and departmental guidance and policies call for the development and testing of contingency plans. LANL's policy also indicates that disaster recovery and contingency planning are essential parts of the laboratory's overall process for helping ensure that classified computer systems can be safely and securely managed during a crisis. This policy, which complies with NIST, DOE, and NNSA guidance, provides the framework to develop and implement disaster recovery and contingency plans, which should include a business impact analysis and test plan. Individual systems may be identified in the disaster recovery and contingency plan documentation, but the actual contingency planning process is performed at a higher level—addressing the contingency requirements of the network and its critical systems. Furthermore, according to LANL policy, disaster recovery and contingency plans should address (1) site policy; (2) business impact analysis; (3) preventive controls; (4) recovery strategies; (5) testing, training, and exercise; and (6) plan maintenance.

LANL did not have comprehensive disaster recovery and contingency plans in place for its classified computer network. Only one of the five plans reviewed had addressed all topics as required by LANL policy, including an up-to-date test plan and recent testing. Two others had contingency plans, but the plans were inadequate. For example, although

one plan addressed all topics, the plan is a procedural template and did not provide any specific information on the classified computer network. Furthermore, two plans did not include elements, such as a business impact assessment or appendices containing the points-of-contact notification list and standard operating procedures. With the exception of the one classified computer system plan that completed all topics of the disaster recovery and contingency planning process, none of the other four systems addressed contingency plan testing.

As a result, until LANL (1) identifies the essential processes that should be included in its contingency plans, (2) develops a contingency plan in accordance with its own policies for each of the systems on the laboratory's classified computer network, and (3) sufficiently tests each contingency plan, the laboratory faces higher risk that the classified network infrastructure will not be able to effectively recover and resume normal operations after a service disruption. LANL has recognized the shortcomings of its contingency planning for its classified computer network and has included the issues in its corrective action plans.

The Laboratory's Decentralized Management Approach Has Led to Weaknesses in the Effectiveness of Its Classified Cyber Security Program

LANL's decentralized approach to information security program management has led to inconsistent implementation of policy and contributed to both technical weaknesses and security program shortfalls. For example, the laboratory did not always use a consistent approach to implementing security fixes for the classified computer network. Specifically, LANL's central cyber security organization did not have the authority to enforce compliance with the laboratory's policies and procedures. Each operating division at the laboratory is responsible for managing and securing its computer systems that are connected to the classified computer network, and each division approaches cyber security differently. The result has been a patchwork of cyber security practices and procedures, which increases the risk of compromise and hampers the laboratory's ability to effectively secure information on its classified computer network. We have reported that establishing a central management focal point for cyber security is essential to spotting trends, identifying problem areas, and determining whether policies and administrative issues are handled in a consistent manner.¹⁴

¹⁴GAO, *Information Security Management: Learning from Leading Organizations*, GAO-AIMD-98-68 (Washington, D.C.: May 1998).

DOE's Office of Independent Oversight also found weaknesses with the laboratory's decentralized approach. In 2008, the Office of Independent Oversight reported that the laboratory's decentralized management approach was not fully effective in managing its classified cyber security program. For example, the Office of Independent Oversight reported that while LANL's Office of the Chief Information Officer cyber security group and LANL's central network group were integrated, LANL did not implement a consistent approach to managing its cyber security resources across the laboratory.¹⁵ In addition, the Office of Independent Oversight reported that some LANL organizations were allowed to run their cyber security functions for their computer systems autonomously and, in many cases, not as effectively as those whose cyber security was centrally managed.

Although LANL Took Actions to Address Weaknesses Governing Its Cyber Security Program, Sustainability Concerns Remain

Notwithstanding efforts to satisfy the July 2007 Compliance Order, DOE and NNSA officials told us they were concerned about LANL's ability to sustain security improvements over the long term. According to laboratory officials, the measures taken to address the Compliance Order facilitated the development of a solid foundation to monitor and sustain effective performance. Although actions taken by LANL have contributed to cyber security improvements over the short term, the assignment of financial penalties would no longer be available once it successfully completed the actions outlined in the Compliance Order, as we previously noted in our June 2008 report.¹⁶ In addition, LANL officials described two efforts that will form the basis for the sustainability of recent efforts over the long term, including (1) LANL's Contractor Assurance System and (2) NNSA's annual performance evaluation plans. However, as noted in the June 2008 report, these efforts have weaknesses and therefore do not form a solid foundation for sustainability.

Strengthening LANL's sustainability efforts requires federal oversight, specifically from NNSA and its Los Alamos Site Office. The Site Office is responsible for day-to-day oversight of LANL for NNSA and must conduct a comprehensive annual survey of LANL's cyber security performance to assure DOE and NNSA that the laboratory's cyber-related assets are

¹⁵LANL's Office of the Chief Information Officer cyber security group is responsible for security policies and program management.

¹⁶GAO, *Los Alamos National Laboratory: Long-Term Strategies Needed to Improve Security and Management Oversight*, [GAO-08-694](#) (Washington, D.C.: June 13, 2008).

adequately protected. These surveys must be validated through, among other things, document reviews, performance testing, and direct observation. To conduct these surveys, as well as to perform effective oversight, the Site Office must be appropriately staffed with well-trained personnel.

In our January 2007 report on the effectiveness of NNSA's management of its security programs, we reported that NNSA's site offices—including the Los Alamos Site Office—had a shortage of security personnel, lacked adequate training resources for Site Office security staff, and lacked data to determine the overall effectiveness of NNSA's security program.¹⁷ These factors, which contributed to weaknesses in NNSA's oversight of security at its laboratories and production facilities, persist. Specifically, as of February 2009, the Los Alamos Site Office employed two full-time equivalents (FTE) to oversee LANL's cyber security programs. According to NNSA officials, this staffing level is not sufficient to effectively oversee and ensure the sustainability of LANL's actions to satisfy the Compliance Order. In their view, the number of federal staff for cyber security oversight needs to be doubled to four FTEs. However, the site office had not conducted a comprehensive staffing review to determine the number of FTEs needed to conduct effective oversight and, according to the site office manager, additional federal cyber security staff is not needed.

¹⁷GAO, *National Nuclear Security Administration: Additional Actions Needed to Improve Management of the Nation's Nuclear Programs*, [GAO-07-36](#) (Washington, D.C.: Jan. 19, 2007).

LANL Has Spent More Than \$400 Million to Operate and Support Its Classified Computer Network Since Fiscal Year 2001, but LANL and DOE Officials Believe That Resources Are Inadequate to Mitigate Risks

LANL spent approximately \$433 million from fiscal years 2001 through 2008 (in constant 2009 dollars) to operate, maintain, protect, and procure equipment for its classified computer network. The laboratory receives funds for its classified computing operations from two primary sources: (1) NNSA's Advanced Simulation and Computing program, which supports stockpile stewardship by providing computer simulation capabilities to predict weapons' performance, safety, and reliability; and (2) NNSA's Office of the Chief Information Officer, which is responsible for leading the management of NNSA's information technology and adequately protecting its information technology systems and information.¹⁸

The \$433 million was used for four principal efforts:

- *High-performance computing* expenditures were for purchasing costs, hardware and software maintenance, and facility costs to house supercomputers that support the nuclear weapons stockpile.
- *Classified computer network* expansion expenditures were for the infrastructure that provides classified computing capabilities and includes the deployment of diskless technologies across the laboratory's classified computing environment.¹⁹
- *Core classified cyber security program* expenditures were for activities such as the implementation of NNSA policies and procedures, security plan development, perimeter protection, certification and accreditation, defense in depth, configuration management, and training.

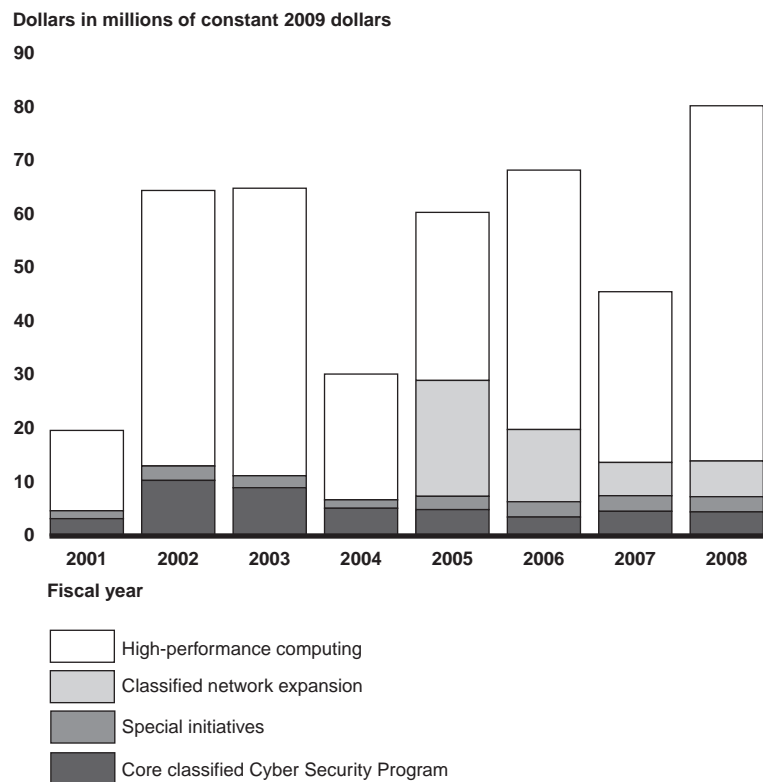
¹⁸Part of NNSA's mission to ensure the safety and reliability of the nuclear weapons stockpile, the Advanced Simulation and Computing program was established in 1995 to help shift from test-based certification of weapons in the nuclear stockpile to a simulation-based certification effort. The Advanced Simulation and Computing program provides supercomputing capabilities that run multi-dimensional codes to simulate all the physics involved in a nuclear detonation. These capabilities allow researchers to integrate past weapons test data, materials, studies, and current experimental data in simulations of unprecedented size. These capabilities leverage the computing expertise and resources of the three NNSA nuclear weapons laboratories (Los Alamos, Sandia, and Lawrence Livermore) and enable weapons scientists and engineers to gain a comprehensive understanding of the weapons' entire life cycle.

¹⁹LANL's classified computer network initially serviced a very specific area within the laboratory's boundaries, but because of the need to reduce the use of classified removable electronic media, such as compact disks and removable hard drives, the network was expanded across the laboratory's geographic area.

- *Special initiatives* expenditures were for the laboratory’s Integrated Cyber Security Initiative and Multi-Platform Trusted Copy program.²⁰

Figure 1 depicts LANL’s annual expenditures for each of the four efforts from fiscal years 2001 through 2008 in constant 2009 dollars.

Figure 1: Annual Expenditures for LANL’s Classified Computer Network, Fiscal Years 2001 through 2008



Source: GAO analysis of LANL expenditure data for the classified network.

As shown in figure 1, LANL’s annual expenditures for its classified computer network increased from about \$20 million to \$80 million between fiscal years 2001 and 2008. The largest expenditure for the

²⁰The Integrated Cyber Security Initiative provides a secure network infrastructure to support NNSA’s scientific, business, and engineering efforts related to the nuclear weapons stockpile. The Multi-Platform Trusted Copy is a cyber security software application that is used to sanitize documents for hidden, classified, or sensitive data before they are released to the public.

classified computer network was for high-performance computing, which accounted for \$322 million (or 74 percent) of total expenditures. For the period, expenditures for high-performance computing ranged from about \$15 million to \$66 million and included a marked reduction, more than 50 percent, in fiscal year 2004. This reduction occurred principally because of a \$29 million decrease in purchasing costs, which resulted from the lag between procurements of the next generation of high-performance computers used by the laboratory. In fiscal year 2006, high-performance computing costs significantly increased because LANL purchased the Roadrunner supercomputer, which provides a large computing resource for LANL's weapons simulations. Purchasing costs for this high-performance computer totaled approximately \$98 million, with \$51.5 million spent in fiscal year 2008.

LANL began to aggressively expand the classified computer network in fiscal year 2005, accounting for \$48 million (or 11 percent) of total expenditures during the fiscal year 2001 through fiscal year 2008 period. Since every high-profile security incident at the laboratory involved classified removable electronic media, LANL has reduced the volume of this media, transferring an ever-increasing volume of information to the classified computer network. Expansion of the classified computer network initially began in fiscal year 2003, using the laboratory's infrastructure funds. In fiscal years 2005 and 2006, Congress appropriated a total of \$40 million to assist in completing this effort.

Expenditures for special initiatives, such as the Integrated Cyber Security Initiative and Multi-Platform Trusted Copy program, accounted for \$19 million (or 4 percent) of total expenditures. These expenditures have remained relatively stable throughout period.

The core classified cyber security program, which serves as the foundation of LANL's protection strategy for the classified cyber security program, accounted for \$45 million (or 10 percent) of total expenditures over the

period.²¹ However, according to a LANL official, expenditures for the classified cyber security program have fluctuated significantly because of funding allocations.

Although total expenditures for the classified computer network increased from fiscal years 2001 through 2008, in the laboratory's view, funding for its core classified cyber security program, in particular, has been inadequate for implementing an effective 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 computing environment, while also reducing support for the unclassified computing networks. For example, in fiscal year 2007, LANL requested more than \$17 million to implement its classified and unclassified cyber security program operations but received \$15 million from NNSA. In fiscal year 2008, the laboratory requested \$27 million but received \$18 million from NNSA. According to LANL's analysis for fiscal years 2007 and 2008, the impacts of failing to fully fund the laboratory's classified cyber security program would limit the laboratory's ability to

- provide forensics capabilities in support of the laboratory's cyber security incident management capabilities,
- implement an effective inventory and patch management program,
- integrate two-factor authentication, and
- integrate identity management software with computer operating systems.

²¹ According to LANL officials, expenditures for classified cyber security program management—such as NNSA policy implementation planning, local policy development, self-assessments, and the development of corrective action plans in response to internal and external audits—were not included in the total expenditures because they could not differentiate between the amount of funds expended for the laboratory's classified and unclassified computer networks. The inability to differentiate between the amount of funds spent for classified and unclassified computer network protection makes it difficult to report on the actual amount of funds spent to protect the laboratory's classified computer network.

In 2007, DOE's Office of Independent Oversight reported that NNSA had not provided adequate funding for LANL's cyber security program because NNSA lacked a formal, risk-based process for allocating cyber security funds across the nuclear weapons complex. This contributed to weaknesses in LANL's overall cyber security program.

According to NNSA's Chief Information Officer, funding decisions for cyber security programs were based on available resources and risk evaluations conducted complex-wide and at individual sites, including LANL. As part of its budget process, NNSA determined that LANL's request exceeded available resources and, as a result, NNSA only partially funded the laboratory's cyber security budget requests.

Conclusions

Preventing the unauthorized disclosure of sensitive information stored on and transmitted over LANL's classified computer network is critical to national security. While the laboratory has taken steps to protect information on its classified computer network, a number of security weaknesses remain. These weaknesses include, among other things, (1) lack of an inventory of critical information stored on the classified computer network and (2) the inability to effectively monitor and maintain accountability for certain actions taken by individual users on the classified computer network. Identifying and inventorying documents on the classified computer network and monitoring user activities are essential to appropriately controlling the confidentiality, integrity, and availability of information stored on the classified computer network. Although the laboratory has taken steps to isolate the classified computer network from external access, the weaknesses we identified could be exploited by a knowledgeable insider, making it imperative that a number of steps be taken to strengthen the technical controls protecting the classified computer network.

Securing information on LANL's classified computer network requires that the laboratory effectively establish, implement, and enforce security policies, procedures, and guidance. The establishment of such policies and procedures lay the foundation for an effective and sustainable cyber security culture. LANL has instituted components of a laboratory-wide information security program for its classified computer network and has successfully implemented several NNSA cyber security policy requirements. However, key activities, such as the assessment of information security risks, the enforcement of compliance with the laboratory's policies and procedures, and the periodic testing of the effectiveness of information security policies and procedures, were not

fully implemented. Until LANL fully implements a laboratory-wide information security program for its classified computer network—including establishing practices for marking the classification level of information stored on the network, comprehensive risk assessments, security plan development and testing, and a continuity of operations process—it has limited assurance that information on the classified computer network will be adequately protected.

Regardless of the improvements the laboratory makes to strengthen the security controls protecting its classified computer network, the lack of centralized management will impede efforts to sustain improvements over the long term. Further, LANL cannot make these improvements on its own. This effort will require the laboratory to work in concert with its federal counterparts—NSA and the Los Alamos Site Office—to enhance implementation of its cyber security objectives. Federal oversight must include adequate staffing, training, and resources to provide effective oversight and reinforce program sustainability, including a comprehensive review of the laboratory’s implementation of the Compliance Order.

Recommendations for Executive Action

To improve LANL’s information security program for its classified computer network, we recommend that the Administrator for the National Nuclear Security Administration direct the Director of Los Alamos National Laboratory to take the following 12 actions:

- Ensure that the risk assessments for systems connected to the classified computer network evaluate all known threats and vulnerabilities.
- Ensure that cyber security policies and procedures applicable to the classified computer network are comprehensive and contain specific instructions on how to implement federal and departmental requirements.
- Develop and implement a policy to (1) mark the classification level of information in documents and files stored on the classified computer network and (2) develop and maintain an inventory of documents and files stored on the network.
- Implement specialized training requirements for all users with significant security-related responsibilities on the classified computer network.
- Ensure that security plans for systems connected to the classified computer network are revised to sufficiently document technical security controls.

-
- Strengthen the security testing and evaluation process for the systems connected to the classified computer network by conducting comprehensive vulnerability scans and expanding technical testing to cover new areas that might be vulnerable.
 - Ensure that plans of action and milestones include all system- and program-level cyber security weaknesses and required information so that they are an effective management tool for tracking security weaknesses and identifying budgetary resources needed to protect the classified computer network.
 - Develop comprehensive contingency plans for all computer systems connected to the classified computer network.
 - Annually test the contingency plans for the systems connected to the classified computer network to determine if the laboratory's proposed actions will function as intended during emergency situations.
 - Take steps to centralize security management of the classified computer network to enforce compliance with laboratory policies, procedures, and practices for each computer system connected to the classified computer network.
 - Develop a sustainability plan, in collaboration with NNSA, that details, among other things, (1) how the laboratory plans to maintain recent cyber security improvements, (2) how these improvements will be supported on a long-term basis, and (3) the resource requirements needed to sustain and improve on recent cyber security improvements.

To ensure sustainability efforts are properly implemented and effective federal oversight is provided, we recommend that the Administrator of the National Nuclear Security Administration take the following actions:

- Undertake a comprehensive review of federal cyber security staffing requirements at the Los Alamos Site Office to determine if additional staff is needed. Should a determination be made that additional federal cyber security staff is needed, actions should be taken by the Manager of the Los Alamos Site Office to acquire sufficient cyber security staff, ensure that staff receive adequate training, and maintain the skills necessary to perform adequate oversight and enforce compliance with NNSA cyber security requirements.
- Assess LANL's sustainability capabilities 12 months after it implemented the Compliance Order, and periodically review LANL's sustainability plan

in order to increase accountability for and improve performance of the laboratory's cyber security operations.

In a separate classified report, we also made 21 recommendations to correct specific weaknesses identified.

Agency Comments and Our Evaluation

In written comments on a draft of this report, the Associate Administrator for Management and Administration stated that NNSA generally agreed with the report and will provide its detailed corrective actions to the Committee on Energy and Commerce through its formal Management Decision process. The Associate Administrator also stated that the laboratory has shown improvement and that this change should be reflected in the report. However, at the time of our site visits, we determined that significant information security control weaknesses remained on LANL's classified computer network, and although NNSA states the laboratory has shown improvement, we did not test these reported corrective actions to determine whether they effectively resolved the weaknesses we identified. Therefore, these reported actions are not reflected in this report. Furthermore, the Associate Administrator stated that enough time has not passed since the implementation of the Compliance Order to properly assess LANL's sustainability measures, and requested that we add a recommendation directed to NNSA to assess the laboratory's sustainability capabilities 12 months after the laboratory implemented the Compliance Order. We agree that NNSA should reassess LANL's sustainability capabilities given the laboratory's historical inability to sustain information security improvements, and have modified our recommendation accordingly. NNSA's comments on our draft report are presented in appendix II. In addition, NNSA provided several technical comments, which we have incorporated as appropriate.

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 to the Secretary of Energy, the Administrator of NNSA, and the Director of LANL. Copies of the report will also be available to others at no charge on the GAO Web site at <http://www.gao.gov>.

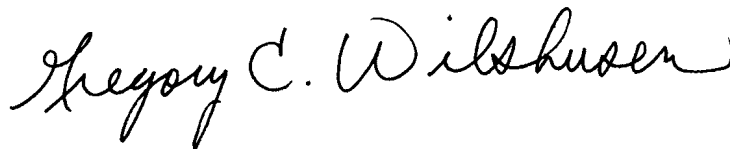
If you or your staffs have any questions about this report, please contact Gene Aloise at (202) 512-3841, or aloise@gao.gov; Nabajyoti Barkakati at (202) 512-641 or barkakatin@gao.gov; or Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributors to this report are included in appendix III.



Gene Aloise
Director, Natural Resources
and Environment



Nabajyoti Barkakati
Director, Center for Technology
and Engineering



Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to (1) assess the effectiveness of security controls Los Alamos National Laboratory (LANL) used to protect information stored on and transmitted over its classified computer network, (2) assess whether LANL had fully implemented an information security program to ensure that controls were effectively established and maintained for its classified computer network, and (3) identify the expenditure of funds used to support LANL's classified computer network from fiscal years 2001 through 2008.

To determine the effectiveness of security controls that the laboratory had implemented for its classified computer network and to identify interconnectivity and key control points, we gained an understanding of the overall network control environment of LANL. Our evaluation is based on our *Federal Information System Controls Audit Manual*, which provides guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized information.¹ Using National Institute of Standards and Technology (NIST) standards and guidance, and Department of Energy (DOE) and National Nuclear Security Administration (NNSA) policies, procedures, and standards, we focused our review on five computer systems connected to the classified computer network. We focused on these five computer systems because they are critical to the laboratory's achievement of its nuclear weapons missions. We performed vulnerability assessments on these computer systems to evaluate authentication and authorization controls, encryption mechanisms, network monitoring processes, and configuration management controls for the classified computer network. In addition, we obtained the views of, and analyzed documentation on these issues from cognizant security officials at DOE, NNSA, the Los Alamos Site Office, and LANL.

To assess whether LANL had fully implemented an information security program to ensure that controls were effectively established and maintained for its classified network, we determined whether LANL's security procedures and their implementation adhered to NNSA, DOE, and other federal guidance in areas such as risk assessment, security awareness training, information security plans, security testing and

¹GAO, *Federal Information System Controls Audit Manual*, [GAO-09-232G](#) (Washington, D.C.: February 2009).

evaluation, corrective action plans, and continuity of operations. Specifically, we

- reviewed LANL's risk assessment process and risk assessments for the classified computer network to determine whether risks and threats were documented consistently with federal guidance;
- analyzed LANL's policies on securing information stored on information systems connected to the classified computer network to determine if they provided sufficient guidance to personnel responsible for security information and information systems;
- examined training records for personnel with significant security responsibilities to determine if they received training commensurate with those responsibilities;
- analyzed security plans for systems connected to the classified computer network 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 classified computer network to determine whether management, operational, and technical controls were tested at least annually and whether the controls tested were based on the risks posed if they were to fail;
- examined corrective action plans to determine whether they addressed vulnerabilities identified in LANL's security testing and evaluations; and
- examined disaster recovery and contingency plans for the classified network to determine whether those plans had been tested or updated.

We also met with key security representatives and officials responsible for information security management at DOE, NNSA, the Los Alamos Site Office, and LANL and discussed 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, to discuss any related prior, ongoing, or planned work in these areas.

To identify the expenditure of funds used to operate and support LANL's classified computer network from fiscal years 2001 to 2008, we determined and analyzed financial data detailing classified cyber security program expenditures in constant 2009 dollars. We chose this time period because, beginning in fiscal year 2001, NNSA assumed programmatic responsibility

for the nuclear weapons complex. In addition, we met with cyber security officials from NNSA, the Los Alamos Site Office, and LANL. To assess the reliability of expenditure data, we (1) reviewed existing documentation related to the data sources; (2) performed basic reasonableness checks of the data; and (3) assessed responses to a series of data reliability questions from responsible LANL officials related to data entry, internal control procedures, and the accuracy and completeness of the data. We determined that the data were sufficiently reliable for the purposes of this report.

We conducted this performance audit from November 2008 to July 2009 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



October 2, 2009

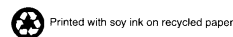
Gregory C. Wilshusen
Director, Information Security Issues
Government Accountability Office
Washington, D.C. 20548

Dear Mr. Wilshusen:

The National Nuclear Security Administration (NNSA) appreciates the opportunity to review the Government Accountability Office's (GAO) draft report, GAO-10-28, *INFORMATION SECURITY: Actions Needed to Better Manage, Protect, and Sustain Los Alamos National Laboratory's Classified Computer Network*. This is a series of reports requested by the House Committee on Energy and Commerce to determine the issues associated with the Los Alamos National Laboratory's (LANL) cyber security program. We understand that this report is the public version to the classified report that GAO issued in July 2009.

NNSA generally agrees with the report. However, we believe that LANL has shown improvement and this change should be reflected in the report. During the GAO evaluation of the Los Alamos National Laboratory's classified computer infrastructure, it was noted by GAO that a number of weaknesses remain in LANL's ability to provide confidentiality, integrity, and availability of information stored on and transmitted over its infrastructure. Many of these weaknesses had already been identified by NNSA Headquarters, Los Alamos Site Office and LANL during their implementation of the Secretary Compliance of Energy's Order issued in FY 2007. To the LANL's credit, during the implementation of the Compliance Order a number of key technical issues and policy implementation concerns have been or are currently being addressed with Correction Action Plans. Although LANL capability to sustain security improvements over the long-term has been in question in the past, there has not been enough time to measure sustainability after the implementation of the Compliance Order to determine if the problem has been resolved. We believe it would be helpful if GAO would recommend to NNSA leadership that 12 months after the implementation of the Compliance Order, NNSA should again assess LANL sustainability capability. Enclosed are further comments for your consideration.

Because of the extent of the recommendations contained in this draft report, NNSA will provide its detailed corrective actions to the Committee on Energy and Commerce through our formal Management Decision process. Los Alamos has made significant progress in correcting the issues you identified and most actions have been completed.



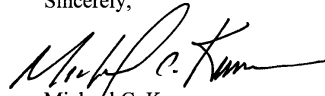
**Appendix II: Comments from the National
Nuclear Security Administration**

2

NNSA continues to exercise its leadership to correct deficiencies noted and to implement a dynamic framework of controls and processes that can be implemented complex-wide. These processes and controls will provide a level of confidence that NNSA is successfully managing risk.

Should you have any questions about this response, please contact JoAnne Parker, Acting Director, Policy and Internal Controls Management at 202-586-1913.

Sincerely,



Michael C. Kane
Associate Administrator
for Management and Administration

Enclosure

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gene Aloise, (202) 512-3841 or aloisee@gao.gov

Nabajyoti Barkakati, (202) 512-6412 or barkakatin@gao.gov

Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov

Staff Acknowledgments

In addition to the individuals named above, Glen Levis; Jeffrey Knott; Edward M. Glagola, Jr.; Duc Ngo; Harold Lewis (Assistant Directors); Preston S. Heard; Jennifer R. Franks; John A. Spence; and Eugene Stevens were key contributors to this report. Allison B. Bawden, Omari Norman, Rebecca Shea, and Carol Hermstadt Shulman also made key contributions to this report.

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 afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

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

