United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Thursday, September 25, 2008

NUCLEAR SECURITY

Los Alamos National Laboratory Faces Challenges In Sustaining Physical and Cyber Security Improvements

Statement of Gene Aloise, Director
Natural Resources and Environment

Nabajyoti Barkakati, Chief Technologist
Applied Research and Methodology

Gregory C. Wilshusen, Director
Information Security Issues

GAO-08-1180T

September 25, 2008

NUCLEAR SECURITY

Los Alamos National Laboratory Faces Challenges in Sustaining Physical and Cyber Security Improvements

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-1180T, testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

Why GAO Did This Study

Los Alamos National Laboratory (LANL) is one of three National Nuclear Security Administration (NNSA) laboratories that designs and develops nuclear weapons for the U.S. stockpile. LANL employees rely on sensitive and classified information and assets that are protected at different levels, depending on the risks posed if they were lost, stolen, or otherwise compromised. However, LANL has experienced several significant security breaches during the past decade.

This testimony provides GAO's (1) views on physical security at LANL, as discussed in *Los Alamos National Laboratory: Long-Term Strategies Needed to Improve Security and Management Oversight*, GAO-08-694 (June 13, 2008); (2) preliminary observations on physical security at Lawrence Livermore National Laboratory; and (3) views on cyber security at LANL as discussed in *Information Security: Actions Needed to Better Protect Los Alamos National Laboratory's Unclassified Computer Network*, GAO-08-1001 (Sept. 9, 2008). To conduct this work, GAO analyzed data, reviewed policies and procedures, interviewed laboratory officials, and conducted site visits to the two laboratories.

To view the full product, including the scope and methodology, click on GAO-08-1180T. For more information, contact Gene Aloise at (202) 512-3841, or aloisee@gao.gov; Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov; and Nabajyoti Barkakati at (202) 512-6412 or barkakatin@gao.gov.

What GAO Found

Physical security at LANL is in a period of significant improvement, and LANL is implementing over two dozen initiatives to better protect its classified assets. However, while LANL's current initiatives address many physical security problems previously identified in external security evaluations, other significant security problems have received insufficient attention. In addition, the management approaches that LANL and NNSA intend to use to sustain security improvements over the long term are in the early stages of development or contain weaknesses. Furthermore, LANL's ability to sustain its improved physical security posture is unproven because (1) the laboratory appears not to have done so after a significant security incident in 2004, with another significant security breach in 2006, and (2) NNSA's Los Alamos Site Office—which is responsible for overseeing security at LANL—may not have enough staff or the proper training to execute a fully effective security oversight program. GAO's report made recommendations to help further improve physical security at LANL and ensure that these improvements are sustained over the long term.

As a result of poor performance on an April 2008 physical security evaluation conducted by the Department of Energy's (DOE) Office of Independent Oversight, GAO is reviewing physical security at Lawrence Livermore National Laboratory (Livermore). GAO's preliminary observations are that Livermore appears to experience difficulties similar to LANL's in sustaining security performance. Furthermore, it appears that NNSA has not always provided effective oversight of Livermore. Specifically, an NNSA security survey conducted only 6 months prior to the April 2008 DOE evaluation gave Livermore the highest possible rating on its security program's performance. These results differ markedly from those documented by DOE's Office of Independent Oversight.

LANL has implemented measures to enhance cyber security, but weaknesses remain in protecting information on its unclassified network. This network possesses sensitive information such as unclassified controlled nuclear information, export control information, and personally identifiable information about LANL employees. GAO found vulnerabilities in critical areas, including (1) identifying and authenticating users, (2) encrypting sensitive information, and (3) monitoring and auditing security policy compliance. A key reason for these information security weaknesses is that the laboratory has not fully implemented an information security program to ensure that controls are effectively established and maintained. Furthermore, deficiencies in LANL's policies and procedures raise additional concern, particularly with respect to foreign nationals' accessing the network from the laboratory and remotely. Finally, LANL cyber security officials told GAO that funding to address some of their security concerns with the laboratory's unclassified network has been inadequate. However, NNSA officials asserted that LANL had not adequately justified its requests for additional funds. GAO made 52 recommendations to help strengthen LANL's information security program and controls over the unclassified network.

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here today to discuss physical and cyber security at Los Alamos National Laboratory (LANL). LANL, located in Los Alamos, New Mexico, has a multibillion dollar annual budget and is one of three National Nuclear Security Administration (NNSA) laboratories responsible for designing and developing a safe, secure, and reliable nuclear weapons deterrent.[1] In fiscal year 2007, LANL budgeted nearly $200 million to provide the laboratory with physical and cyber security to protect the sensitive and classified assets on which laboratory employees rely to conduct their work. A successful physical or cyber attack on NNSA sites containing nuclear weapons, the material used in nuclear weapons, or information pertaining to the people who design and maintain the U.S. nuclear deterrent could have devastating consequences for the site, its surrounding communities, and the nation's security. Because of these risks, NNSA sites need effective physical and cyber security programs.

Over the last decade, LANL has experienced a series of high-profile security incidents in which sensitive assets and classified information were compromised. In October 2006, during a drug raid on a private residence, it was discovered that a LANL contract employee had transferred classified information to a USB "thumb drive" and removed the thumb drive, as well as a large number of classified documents, from the laboratory. The Department of Energy's (DOE) Inspector General reported that a serious breakdown in core laboratory physical and cyber security controls contributed to the October 2006 thumb drive incident.[2] More recently, in April 2008, DOE's Office of Independent Oversight conducted an evaluation of security at Lawrence Livermore National Laboratory (Livermore). The evaluation included a mock terrorist attack on a sensitive laboratory facility and concluded that Livermore's security program had significant weaknesses, particularly with respect to the performance of Livermore's protective force and the physical protection of classified resources.

[1]The other design and development laboratories are Lawrence Livermore National Laboratory in Livermore, California, and Sandia National Laboratories in Albuquerque, New Mexico, and Livermore, California. NNSA is a separately organized agency within the Department of Energy that is responsible for the management and security of the nation's nuclear weapons, nuclear nonproliferation, and naval reactors programs.

[2]U.S. Department of Energy, Office of Inspector General Office of Audit Services, *Special Inquiry Report to the Secretary: Selected Controls Over Classified Information at the Los Alamos National Laboratory*, OAS-SR-07-01 (Washington, D.C., Nov. 2006).

As a result of the October 2006 thumb drive incident and the congressional hearings that followed, the Committee asked us to review physical and cyber security at LANL. In addition, in June 2008, this Committee requested that we review the status of physical security at Livermore. Our testimony today discusses (1) physical security at LANL, (2) preliminary observations from ongoing work on physical security at Livermore, and (3) cyber security at LANL. This statement is primarily based on recently issued reports on physical and cyber security at LANL.[3] We conducted the performance audit work that supports this statement in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to produce 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 statements today.

Summary

Physical security at LANL is in a period of significant improvement, and LANL is implementing over two dozen initiatives to better protect its classified assets. However, while LANL's current initiatives address many security problems previously identified in external evaluations, other significant security problems have received insufficient attention. For example, at the time of our review, LANL had not implemented complete security solutions to address either the storage of classified nuclear weapons parts in unapproved storage containers or weaknesses in its process for ensuring that actions taken to correct security deficiencies are completed. Furthermore, management approaches that LANL and NNSA officials told us they would use to sustain security improvements over the long term were in the early stages of development or contained weaknesses. In addition, LANL's ability to sustain its improved physical security posture is unproven because (1) the laboratory appears not to have done so after a significant security incident in 2004, and (2) NNSA's Los Alamos Site Office—which is responsible for overseeing physical security at LANL on a daily basis—may not have enough staff or the proper training for these staff to execute a fully effective security oversight program. Our report on physical security at LANL made three recommendations to the Secretary of Energy and the Administrator of

[3]GAO, *Los Alamos National Laboratory: Long-Term Strategies Needed to Improve Security and Management Oversight*, GAO-08-694 (Washington, D.C.: June 13, 2008) and GAO, *Information Security: Actions Needed to Better Protect Los Alamos National Laboratory's Unclassified Computer Network*, GAO-08-1001 (Washington, D.C.: Sept. 9, 2008).

NNSA concerning long-term strategic security planning and the use of meaningful financial incentives for effective security performance. We believe these recommendations, if effectively implemented, would help further improve physical security at LANL and ensure that these improvements are sustained over the long term.

Though our observations on physical security at Livermore are preliminary, the laboratory appears to be experiencing difficulties similar to LANL's in sustaining physical security performance. In addition, Livermore's self-assessment and performance assurance programs appear to need improvement. For example, Livermore and NNSA security officials acknowledged that a lack of comprehensive performance assurance testing was a significant contributing factor to the poor performance of Livermore's protective forces during their April 2008 exercise. Finally, it appears that NNSA has not always provided effective security oversight of Livermore. Specifically, a 2007 NNSA security survey gave Livermore the highest possible rating on its security performance, differing markedly from what DOE observed during its evaluation in April 2008, only 6 months later. DOE identified multiple areas for significant improvement, and gave Livermore the lowest rating possible in two security performance areas.

Our review of cyber security at LANL found that the laboratory has implemented measures to enhance its information security, but weaknesses remain in protecting the confidentiality, integrity, and availability of information on its unclassified network.[4] LANL's unclassified network contains sensitive information, such as unclassified controlled nuclear information, export control information, and personally identifiable information about laboratory employees. LANL has implemented a network security system that is capable of detecting potential intrusions; however, we found vulnerabilities in several critical areas, including identifying and authenticating users; encrypting sensitive information; and monitoring and auditing compliance with security policies. For example, LANL has implemented strong authentication measures for accessing its unclassified network, but once access is initially gained, a user can work around the authentication measures to access certain sensitive information. A key reason for LANL's information security weaknesses is that the laboratory has not fully implemented an

[4]We are currently reviewing information security controls over LANL's classified network for this Committee.

information security program to ensure that controls are effectively established and maintained. For example, LANL's most recent risk assessment for its unclassified network generally identified and analyzed vulnerabilities, but did not account for risks identified by the laboratory's own internal vulnerability testing. Furthermore, we and other external security evaluators have reported concerns about LANL's policies for granting foreign nationals—particularly those from countries classified as "sensitive" by DOE—access to the unclassified network. Finally, LANL cyber security officials told us that funding to address some of their security concerns with respect to the laboratory's unclassified network has been inadequate. NNSA officials told us LANL has not adequately justified its request for additional funds, and NNSA is developing a process for developing cyber security budgets more systematically. We made 52 recommendations to the Secretary of Energy and the Administrator of NNSA that, if effectively implemented, would improve LANL's information security program and controls over its unclassified network. These recommendations address, among other things, ensuring that LANL's risk assessment for its unclassified network evaluates all known vulnerabilities and is revised periodically, and strengthening policies with a view toward further reducing, as appropriate, foreign nationals' access to the unclassified network.

Background

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. At LANL, these assets include Category I special nuclear material, such as plutonium and highly enriched uranium;[5] thousands of classified nuclear weapons parts and components; millions of classified documents; thousands of pieces of classified removable electronic media that contain nuclear weapon design information;[6] over 100 vaults and vault-type rooms that store classified assets; and computer networks and the hardware on which these

[5]Special nuclear material is considered to be Category I when it is weapons-grade, such as plutonium and highly enriched uranium, and occurs in specified forms and quantities.

[6]Some classified documents and pieces of removable electronic media, such as CDs and thumb drives, pose a security risk that requires maintenance of an accountability system to prevent unauthorized access or removal.

networks run that protect classified information as well as sensitive unclassified information.

LANL is subject to a series of DOE security orders that outline requirements for implementing effective physical and cyber security protection strategies. These orders include an assessment of the potential size and capabilities of terrorist forces that could physically attack a laboratory and against which a laboratory must be prepared to defend. The orders further describe different levels of physical protection for sensitive and classified assets, depending on the risk they would pose if they were lost, stolen, or otherwise compromised. Appropriate physical protection safeguards include locks and keys, fences, means to detect unauthorized entry, perimeter alarms, vehicle barriers, and armed guards.

In addition, the 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.[7] FISMA requires each agency to develop, document, and implement an agencywide 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. Examples of appropriate information security controls include user identification and authentication that allow computer systems to differentiate between users and verify their identities; cryptography that ensures the confidentiality and integrity of critical and sensitive information; configuration management that identifies and manages security features for all hardware, software, and firmware components of an information system and controls changes to them; and audit and monitoring controls that help establish individual accountability and monitor compliance with security policies.

LANL is managed and operated by a corporate entity, Los Alamos National Security LLC (LANS).[8] NNSA's Los Alamos Site Office serves as the primary federal overseer of laboratory security performance. Annually, the Site Office determines how much money LANS will earn for its

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

[8]LANS has been the management and operating contractor of LANL since June 2006. LANS is made up of the University of California, Bechtel National, Washington Group International, and BWX Technologies (which now operates under the name The Babcock & Wilcox Company).

management of the laboratory according to a maximum available performance-based fee established in the laboratory's contract. The Site Office bases its determination on the laboratory's success in meeting the goals laid out in performance evaluation plans. These plans allocate portions of the maximum available performance award fee to NNSA performance objectives, including measures related to both physical and cyber security.

In addition, two DOE organizations are required to periodically review physical and cyber security at LANL. NNSA's Los Alamos Site Office is required to conduct security surveys annually. These surveys are based on observations of performance, including compliance with DOE and NNSA security directives. In fiscal year 2008, the results of this survey are directly tied to NNSA's performance evaluation plan, and are therefore a factor in LANS' ability to earn the maximum available performance award fee. DOE's Office of Independent Oversight also conducts evaluations, typically every 18 months for facilities that store Category I special nuclear material. These evaluations identify weaknesses in the laboratories' security programs and produce findings that laboratory officials must take action to correct. The reviews overlap substantially, but each is required to provide a comprehensive assessment of the laboratory's security programs.

While Physical Security at Los Alamos National Laboratory Has Improved, Management Approaches to Sustain Security Improvements Are in the Early Stages of Development or Contain Weaknesses

Physical security at LANL is in a period of significant improvement, and LANL is implementing over two dozen initiatives to reduce, consolidate, and better protect its classified assets, as well as reduce the physical footprint of the laboratory by closing unneeded facilities. LANL officials believe that these initiatives will reduce the risk of incidents that can result in the loss of control over classified assets. For example, to reduce and consolidate classified assets and its physical footprint, as of March 2008, LANL had (1) reduced from nine to one the number of areas containing Category I special nuclear material; (2) reduced the amount of accountable classified removable electronic media from 87,000 pieces to about 4,300 and made information previously accessible on removable media available only through the laboratory's classified computer network; (3) eliminated about 30,000 classified nuclear weapon parts; and (4) reduced the number of vault-type rooms from 142 to 111. In addition, during fiscal year 2007, LANL reduced the physical footprint of existing facilities by over 500,000 square feet. In concert with these actions, LANL is implementing a series of engineered and administrative controls to better protect and control classified assets, [9] such as removing the functions from classified computers that enable them to create new pieces of removable electronic media and streamlining physical security procedures to make them easier to implement across the laboratory.

We found that DOE's Office of Independent Oversight and the Los Alamos Site Office identified significant physical security problems at LANL that the laboratory had not fully addressed. Specifically, while LANL's storage of classified parts in unapproved storage containers and its process for ensuring that actions to correct identified security deficiencies have been cited in external security evaluations for years, complete security solutions in these areas had not yet been implemented at the time of our review. In addition, external security evaluations had repeatedly identified concerns about the adequacy of LANL's assessments of its own security performance. The security self-assessment program provides LANL with the opportunity to self-identify security deficiencies and address them before they can be exploited. External security evaluations found that LANL's self-assessments were not comprehensive and did not include discussions of all internal findings. These evaluations also noted that findings identified through self-assessments were not always analyzed and

[9]Engineered controls are system-based controls that manage work processes and prevent employees from taking inappropriate action. Administrative controls are typically policies or procedures that govern the handling of classified resources.

addressed through corrective actions. At the time of our review, Los Alamos Site Office and DOE Office of Independent Oversight officials noted that LANL's self-assessment program was improving.

LANL officials identified three management approaches that they asserted would sustain security improvements over the long term. However, these approaches were either in an early stage of development or contained important weaknesses that may impair their ability to ensure the sustainability of security improvements at the laboratory for the foreseeable future. First, LANL officials identified completing the management actions required by the Secretary of Energy's Compliance Order issued as a result of the October 2006 thumb drive incident as an approach to ensure that security improvements are sustained, yet the Compliance Order itself does not provide a mechanism to sustain security improvements over the long-term.[10] Second, LANL officials told us they will track the implementation of longer-term actions, including those required by the Compliance Order, by developing and implementing the Contractor Assurance System required under the LANS contract.[11] However, the extent to which LANL can rely on the Contractor Assurance System to ensure the long-term sustainability of security improvements is unclear. According to a Los Alamos Site Office official, the Contractor Assurance System will not be fully completed for 3 to 4 years and, thus, will not be fully implemented by the time actions under the Compliance Order are completed. Finally, according to LANL officials, the laboratory plans to realize security improvements by meeting the security-related performance incentives in the annual performance evaluation plans NNSA uses to measure performance and determine an award fee for LANS. However, the annual performance evaluation plans focus principally on

[10]The 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 corrective actions to remediate deficiencies that contributed to security violations. On July 12, 2007, the Secretary of Energy issued a compliance order to LANS as a result of the security incident discovered in October 2006. The Compliance Order directs LANS to take comprehensive steps to ensure that it identifies and addresses critical classified information and cyber security deficiencies at LANL. Violation of the Compliance Order would subject LANS to civil penalties of up to $100,000 per violation per day until compliance is reached.

[11]The Contractor Assurance System is intended to be a tool to increase accountability and improve laboratory management and performance. According to a LANL official, the Contractor Assurance System is an integrated performance-based management system that is available as a tool for federal oversight.

compliance with DOE requirements and do not sufficiently reward security program improvement. In that regard, according to a senior NNSA security official, compliance with current DOE requirements does not assure that LANL's security program is functioning effectively. Indeed, we found that all but $30,000 of the total $1.43 million fiscal year 2008 performance fee allocated to physical security was associated with LANL's achievement of compliance-oriented milestones, such as issuing plans, publishing policies, and completing equipment maintenance requirements.

The management attention dedicated to improving physical security following the October 2006 thumb drive incident mirrors the level of attention that followed LANL's 2004 shutdown, when over 3,400 safety and security deficiencies were identified for correction. This shutdown lasted up to 10 months for some laboratory activities and cost as much as $370 million.[12] Given how quickly LANL's security performance declined between the full resumption of laboratory activities in May 2005 and the discovery of the thumb drive on private property, LANL's ability to sustain the improved security posture it has recently achieved is unproven. Strong federal oversight will help ensure that these improvements are sustained. However, we reported that the Los Alamos Site Office suffers from a shortage of security personnel and lacks funding needed for training. Specifically, as of October 2007, the Los Alamos Site Office employed 13 security staff—enough for 1 person to oversee each of the topical areas the Site Office had to evaluate. This staffing level, officials said, was sufficient to cover only 15 percent of LANL's facilities. In April 2008, a senior security official at the Site Office said security staffing levels had decreased since October 2007. Furthermore, while NNSA had identified the need to train and certify Site Office security personnel in specific subject matters, according to Site Office officials no specific training funds had been made available.

We made three recommendations to the Secretary of Energy and the Administrator of NNSA that, if effectively implemented, will improve physical security at LANL and help ensure that improvements LANL has achieved are sustained over the long term. Specifically, we recommended that LANL be required to develop a comprehensive strategic plan for laboratory security that addresses all previously identified security

[12]GAO, *Stand-Down of Los Alamos National Laboratory: Total Costs Uncertain; Almost All Mission-Critical Programs Were Affected but Have Recovered*, GAO-06-83 (Washington, D.C.: Nov. 18, 2005).

weaknesses and focuses on improving security program effectiveness. Furthermore, we recommended that NNSA provide meaningful financial incentives in future performance evaluation plans for implementation of this comprehensive strategic plan for laboratory security.

Preliminary Observations on Physical Security at Lawrence Livermore National Laboratory

In June 2008, the Committee requested that we review the security status at Livermore. This request came as a result of an evaluation by DOE's Office of Independent Oversight in April 2008, in which Livermore received the lowest possible ratings for protective force performance and for physical protection of classified resources. The evaluation also identified issues in other areas, such as security sensors and alarms, and security program management. We are currently verifying the findings of the evaluation and Livermore's actions to correct security deficiencies. Specifically:

- *Self-assessment and performance assurance testing programs at Livermore need improvement.* DOE's Office of Independent Oversight evaluations and Livermore Site Office security surveys found shortcomings in Livermore's fiscal year 1999, 2000, 2002, and 2008 self-assessment programs. In addition, Livermore and NNSA security officials acknowledged that a lack of comprehensive performance assurance testing was a significant contributing factor to the poor performance of Livermore protective forces during their April 2008 exercise. Between December 2006 and April 2008, Livermore did not hold an integrated performance assurance test of its protective forces or operationally test equipment key to the laboratory's protective strategy. During our visit to the laboratory 2 weeks ago, Livermore officials told us they are finalizing corrective action plans to address deficiencies in their performance assurance and self-assessment programs and have already conducted a significant number of performance assurance tests with the protective force and on equipment since the completion of the Office of Independent Oversight's 2008 evaluation.

- *NNSA and the Livermore Site Office have not always provided effective security oversight.* Six months before the Office of Independent Oversight's 2008 evaluation, the 2007 Livermore Site Office's annual security survey gave the laboratory a 100-percent satisfactory rating on its security performance, the highest possible rating. The results of the Office of Independent Oversight inspection not only differed markedly, but also found that the Livermore Site Office survey was not comprehensive and the ratings provided did not reflect what was actually observed. The Livermore Site Office is currently in the process of fundamentally

rebuilding and restructuring its survey program and has embarked on a training program for its security personnel.

Though our observations are preliminary, Livermore appears to be experiencing difficulties similar to LANL's in sustaining physical security performance. For example, in 1999, DOE's Office of Independent Oversight identified significant weaknesses in Livermore's programs to secure the laboratory's Category I special nuclear material facility against a potential terrorist attack. Livermore then embarked on a major program to improve security and, according to the Office of Independent Oversight, addressed most issues by 2002. This improved level of security performance appears to have been sustained through 2006. Between December 2006—when Livermore's protective force performed well in an exercise—and April 2008, security performance at Livermore declined. In response to the negative results of the 2008 Office of Independent Oversight evaluation, Livermore appears to be refocusing management attention on security performance.

While our work is preliminary, we believe the actions taken by Livermore, the Livermore Site Office, and NNSA, if and when fully implemented, will address identified physical security issues. However, just as at LANL, sustaining attention on physical security performance will continue to be a challenge.

Los Alamos National Laboratory Has Implemented Measures to Enhance Cyber Security on Its Unclassified Network, but Weaknesses Remain

LANL has implemented measures to enhance its cyber 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 included 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.

A key reason for the information security weaknesses we identified is that LANL has not yet fully implemented an information security program to ensure that controls are effectively established and maintained. Although LANL has implemented a security awareness training program, we identified a number of shortcomings in its overall information security management program. For example, (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.

Many of LANL's cyber security deficiencies have been the subject of prior evaluations conducted by DOE's Office of Independent Oversight and the Los Alamos Site Office. 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 about 300 from countries identified as sensitive by DOE, such as China, India, and Russia.[13] 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.

[13]DOE identifies countries as sensitive based on national security, nuclear nonproliferation, or terrorism concerns.

NNSA and LANL have not agreed on the level of funding necessary for protecting the unclassified network. From fiscal years 2001 through 2007, LANL spent $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 made a series of recommendations to the Secretary of Energy and the Administrator of NNSA, 11 of which focus on improving LANL's information security program and determining resource requirements for the unclassified network. For example, we recommended that the Secretary of Energy and the NNSA Administrator require the Director of LANL 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' access to the unclassified network, particularly those from countries identified as sensitive by DOE. We made an additional 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 that we identified.

Mr. Chairman, this concludes our prepared statement. We would be happy to respond to any questions that you or Members of the Subcommittee may have at this time.

GAO Contacts and Staff Acknowledgements

For further information on this testimony, please contact Gene Aloise at (202) 512-3481 or aloisee@gao.gov; Nabajyoti Barkakati at (202) 512-6412 or barkakatin@gao.gov; and Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Jonathan Gill, Ed Glagola, Jeff Knott, and Glen Levis, Assistant Directors; Allison Bawden; Preston Heard; Tom Twambly; Ray Rodriguez; John Cooney; Carol Herrnstadt Shulman; and Omari Norman made key contributions to this testimony.

Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

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

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu