
March 2009

NUCLEAR SECURITY

Better Oversight
Needed to Ensure
That Security
Improvements at
Lawrence Livermore
National Laboratory
Are Fully
Implemented and
Sustained



Highlights of GAO-09-321, a report to congressional committees

Why GAO Did This Study

In April 2008, the Department of Energy's (DOE) security inspection at Lawrence Livermore National Laboratory (LLNL) found significant weaknesses, particularly in LLNL's protective force's ability to assure the protection of weapons-grade (special) nuclear material. LLNL is overseen by the National Nuclear Security Administration (NNSA), a separately organized agency within DOE, and managed by a contractor. NNSA is planning to remove most of the special nuclear material from LLNL. GAO was asked to (1) characterize security deficiencies identified in the 2008 inspection; (2) determine the factors that contributed to these deficiencies; (3) identify LLNL's corrective actions to address security deficiencies; and (4) assess LLNL's plan to permanently remove the riskiest special nuclear material from its site. To conduct this work, GAO visited LLNL, reviewed numerous documents and plans, and interviewed LLNL and NNSA security officials.

What GAO Recommends

GAO recommends that the Administrator of NNSA improve and sustain federal oversight of security at LLNL by (1) developing a detailed plan and budget for training NNSA's Livermore Site Office (LSO) security staff and (2) providing financial incentives to LLNL's contractor to sustain security improvements. NNSA generally agreed with the report's findings and recommendations.

To view the full product, including the scope and methodology, click on [GAO-09-321](#). For more information, contact Gene Aloise at (202) 512-3841 or aloisee@gao.gov.

March 2009

NUCLEAR SECURITY

Better Oversight Needed to Ensure That Security Improvements at Lawrence Livermore National Laboratory Are Fully Implemented and Sustained

What GAO Found

DOE's Office of Independent Oversight found numerous and wide-ranging security deficiencies with LLNL's safeguards and security program. DOE gave the laboratory the lowest possible rating in two security areas: protective force performance and classified matter protection and control. The Office of Independent Oversight also reported that LLNL's physical security systems, such as alarms and sensors, and its security program planning and assurance activities needed improvement.

Weaknesses in LLNL's self-assessment program and LSO's oversight contributed to security deficiencies at the laboratory. LLNL's security self-assessment program and LSO's annual security survey failed to identify numerous security deficiencies before DOE's Office of Independent Oversight conducted its inspection. According to one DOE official, both programs were "broken" and missed even the "low-hanging fruit" of compliance-oriented deficiencies. More specifically, LLNL's self-assessment program should have identified the magnitude of technical problems with a key weapon system used at the laboratory. Furthermore, LSO's September 2007 security survey gave LLNL 100-percent satisfactory ratings in its security performance—differing markedly from the security performance DOE observed during its inspection a short time later. To address these issues, LSO is implementing a new program to better train security officials to perform security assessments and recognize deficiencies; however, according to LSO officials, LSO does not have a specific budget to implement this new security training program.

LLNL has developed corrective action plans to address the 54 security deficiencies identified by the Office of Independent Oversight, and both NNSA and DOE will oversee the plans' implementation. As of December 2008, LLNL reported having completed 74 percent of the milestones included in corrective action plans to address physical security deficiencies. DOE plans to re-inspect LLNL in April 2009 and focus on the effectiveness of corrective actions. In the past, LLNL has not sustained corrective actions to address similar security deficiencies. For example, in 1999 DOE reported that LLNL's capability to conduct vulnerability assessments was deficient. By 2000, this problem had been corrected. In 2008, DOE again noted deficiencies in LLNL's vulnerability assessment capability. NNSA has the opportunity to use its new performance-based management and operating contract to hold LLNL's contractor financially accountable for ensuring that security improvements resulting from corrective actions are sustained.

The plan to remove most of LLNL's special nuclear material by the end of fiscal year 2012 faces challenges because the plan's schedule depends on a number of factors, some of which LLNL does not control, such as the willingness and ability of other NNSA and DOE sites to receive the material, the timeliness of the effort, adequate funding, and the availability of specialized transport trucks operated by NNSA's Office of Secure Transportation to transfer material to other DOE sites.

Contents

Letter		1
Background		4
DOE's Office of Independent Oversight Identified Several Significant Weaknesses in LLNL's Safeguards and Security Program		7
A Weak Laboratory Self-Assessment Program and Insufficient Federal Oversight Contributed to Security Deficiencies at LLNL		12
LLNL Has Developed Corrective Action Plans to Address 54 Identified Security Deficiencies, and Both NNSA and DOE Will Oversee Their Implementation		18
LLNL Faces Challenges in Implementing Plans to Complete De-inventory of Its Category I and II Special Nuclear Material by the End of Fiscal Year 2012		27
Conclusions		29
Recommendations for Executive Action		30
Agency Comments and Our Evaluation		30
Appendix I	Safeguards and Security Topics Covered in Office of Independent Oversight Inspections	32
Appendix II	Comments from the National Nuclear Security Administration	34
Appendix III	GAO Contact and Staff Acknowledgments	36
Tables		
Table 1: LLNL Security Deficiencies Identified by the Office of Independent Oversight, by Topical Area, April 2008		8
Table 2: LLNL's Required Protective Force Performance Assurance Testing		14
Figures		
Figure 1: LLNL Corrective Action Milestones by Security Topic, as of December 2008		19

Figure 2: Timeline for the Development and Final Approval of LLNL's Corrective Action Plans

23

Abbreviations

DBT	design basis threat
DOE	Department of Energy
LLNL	Lawrence Livermore National Laboratory
LLNS	Lawrence Livermore National Security, LLC
LSO	Livermore Site Office
NNSA	National Nuclear Security Administration

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.



Accountability * Integrity * Reliability

**United States Government Accountability Office
Washington, DC 20548**

March 16, 2009

The Honorable Henry A. 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 Department of Energy (DOE) has long recognized that a successful terrorist attack on a site containing nuclear weapons or the fissile material used in nuclear weapons—called special nuclear material—could have devastating consequences for the site and its surrounding communities. Lawrence Livermore National Laboratory (LLNL), located in Livermore, California, is one of three national laboratories responsible for designing, developing, and maintaining a safe, secure, and reliable nuclear weapons deterrent.¹ For these and other missions, LLNL stores and uses special nuclear material. Special nuclear material—including plutonium and highly enriched uranium—is considered to be Category I when it is weapons-grade and in specified forms and quantities. The risks associated with Category I special nuclear material vary but include theft, and the potential for sabotage in the form of radiological dispersal, also known as a “dirty bomb.” Because of these risks and LLNL’s location in California’s densely populated San Francisco Bay area, NNSA decided in October 2007

¹The other design and development laboratories are Los Alamos National Laboratory in Los Alamos, New Mexico, and Sandia National Laboratories in New Mexico and California.

to permanently remove, or “de-inventory,” all Category I nuclear material from LLNL.²

LLNL is overseen by the National Nuclear Security Administration (NNSA), a separately organized agency within DOE. DOE’s and NNSA’s safeguards and security program develops policies essential for preventing an unacceptable, adverse impact on national security. To manage potential risks, DOE has developed a classified policy that identifies the potential size and capabilities of terrorist forces against which facilities containing Category I special nuclear material—which at LLNL is the “Superblock” facility—must be prepared to defend.³ Additionally, LLNL must adhere to other DOE security requirements on the effective protection of classified assets, such as documents, removable electronic media, and nuclear weapons components. LLNL documents its ability to meet these requirements through its Site Safeguards and Security Plan.

On October 1, 2007, Lawrence Livermore National Security, LLC (LLNS) took over as the management and operating contractor of LLNL after more than 50 years of operation by the University of California.⁴ NNSA measures LLNL’s performance and determines LLNS’ management and operating incentive fee using annual performance evaluation plans that establish NNSA’s priorities for LLNL and ensure that contract requirements—such as effective security performance—are met.

To determine the overall effectiveness of LLNL’s implementation of DOE and NNSA security requirements—including its protection strategy to meet the DBT—two organizations periodically conduct comprehensive reviews of LLNL’s security performance. First, NNSA’s Livermore Site Office (LSO)—the on-site, federal office responsible for ensuring the secure operation of LLNL facilities and for accepting certain security risks

²LLNL also plans to de-inventory all of its Category II special nuclear material—smaller quantities of weapons-grade materials, such as highly enriched uranium and plutonium—that could be credibly aggregated into Category I quantities.

³Until recently, this policy was known as DOE’s design basis threat (DBT). In 2008, DOE replaced the DBT with a Graded Security Protection policy that provides information that is similar to the information in the DBT but is tailored to risks at specific sites within the DOE nuclear weapons complex.

⁴LLNS is a limited liability corporation made up of Bechtel National, Inc.; the University of California; BWX Technologies, Inc. (now part of the Babcock & Wilcox Company); and the Washington Group International, Inc. The team also includes Battelle Memorial Institute, four small business contractors, and Texas A&M University.

on NNSA's behalf—conducts an annual survey and issues a report based on survey results, observations of security performance, and compliance with DOE and NNSA security directives. This survey is a means for LSO to oversee the laboratory's security performance and is intended to ensure that the security risks NNSA accepts are both known and mitigated to the extent practicable. Second, the Office of Independent Oversight, within DOE's Office of Health, Safety and Security, performs comprehensive, periodic security inspections at LLNL and other sites. These inspections may include performance assurance tests, such as "force-on-force" exercises that evaluate the ability of LLNL's protective force to successfully defend the Superblock facility against a mock terrorist group simulating a potential attacking force. All deficiencies—"findings"—identified during surveys and independent inspections require LLNL to take corrective actions; both LSO and the Office of Independent Oversight track the implementation of these actions. In addition, both LSO and DOE review the self-assessments LLNL conducts of its own security performance.

In April 2008, DOE's Office of Independent Oversight concluded a comprehensive inspection of security at LLNL. As a result of this inspection, LLNL earned the lowest possible rating—"Significant Weakness"—in two of seven security performance areas, including protective force performance. Two additional security performance areas were rated as "Needs Improvement."

In this context, you asked us to (1) characterize the security deficiencies identified by DOE's Office of Independent Oversight in its April 2008 inspection; (2) determine the factors that contributed to the deficiencies DOE's Office of Independent Oversight identified in its inspection; (3) identify corrective actions LLNL is taking to address identified security deficiencies and how these actions are being overseen; and (4) assess LLNL's plan for permanently removing Category I and II special nuclear material from its Superblock facility.

To address these questions, we visited LLNL and observed facilities included in the Office of Independent Oversight's inspection. We also reviewed applicable DOE safeguards and security policies, such as the DBT and DOE Manual 470-4.1, *Safeguards and Security Program Planning and Management*. Furthermore, we reviewed both the Office of Independent Oversight's inspection reports and LSO's security surveys of LLNL from 1999 to the present and analyzed trends in security performance, with a focus on the four of seven security areas for which the Office of Independent Oversight provided overall ratings of less than

effective performance in its 2008 inspection report. In addition, we analyzed LLNL's Site Safeguards and Security Plan for defending the site against the 2003 DBT as well as other key laboratory plans for ensuring that DOE security training and performance testing requirements are met. Furthermore, we reviewed LLNL's and LSO's interim and final corrective action plans to address security performance deficiencies identified by the Office of Independent Oversight. We also interviewed officials from DOE's Office of Health, Safety and Security; NNSA's offices of Defense Nuclear Security and of Nuclear Material Management Integration; LSO; and LLNL.

We conducted this performance audit from July 2008 to March 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.

Background

LLNL's inventory of special nuclear material consists predominantly of weapons-grade plutonium and highly enriched uranium. This inventory takes two forms: (1) metals, including weapons components and material machined into forms for use in weapons components; and (2) oxides and other compounds, such as salts. Some of LLNL's special nuclear material inventory has been determined to be "programmatic," or material that has been declared to be of national security value and that has an identified program use. Other special nuclear material in LLNL's inventory has been determined to be "excess," or material declared to be of national security value but that does not have an identified program use. Finally, LLNL's inventory includes waste material that does not have a national security value.

In accordance with DOE Manual 470.4-1, *Safeguards and Security Program Planning and Management*, NNSA must develop a safeguards and security program that ensures NNSA has the necessary protections in place to protect its security interests against malevolent acts, such as theft, diversion, sabotage, modification, compromise, or unauthorized access to nuclear weapons, nuclear weapons components, special nuclear material, or classified information. The safeguards and security program integrates NNSA's physical security efforts by protective guard forces, information and personnel security systems, and nuclear material control and accountability systems. Contractors that manage and operate NNSA laboratories—including LLNS—are required to comply with DOE

safeguards and security directives, as stated in their management and operating contracts.

Because LLNL contains Category I and II special nuclear material, DOE Manual 470.4-1 requires that it prepare a Site Safeguards and Security Plan, a classified document that identifies known vulnerabilities, risks, and protection strategies for the site and formally acknowledges how much risk the contractor and DOE are willing to accept. The protection measures identified in LLNL's approved Site Safeguards and Security Plan are developed in response to site-specific vulnerability assessments and become the basis for executing and reviewing protection programs at the Superblock. LLNL must annually review its Site Safeguards and Security Plan to ensure that implementation of the plan will provide effective security protection. This review includes a validation of the protective strategy, accomplished in part through an annual force-on-force exercise, which exercises LLNL's protective force against a mock adversary group simulating a potential attacking force. Force-on-force exercises are conducted using plausible attack scenarios. In addition, DOE Manual 470.4-3, *Protective Force*, requires that LLNL conduct other performance assurance tests throughout each year, including quarterly performance assurance tests of a more limited scope than full force-on-force exercises.

While most NNSA and DOE sites were required to meet DOE's 2005 DBT,⁵ LLNL has been declared "non-enduring" and is required to meet DOE's less-demanding 2003 DBT. Specifically, in a March 7, 2008, memorandum the Acting Deputy Secretary of Energy concurred with NNSA's October 2007 decision to declare LLNL a non-enduring Category I and II special nuclear material site because of plans to remove this material.⁶ Together with DOE, NNSA determined that the benefits of expediting the removal of Category I and II special nuclear material outweighed the risks associated with foregoing security upgrades, and funds that were to be spent on these upgrades were redirected to support the de-inventory of special nuclear material. In line with this decision, DOE also agreed with NNSA's decision to suspend planned security upgrades at LLNL's Superblock facility that would have brought LLNL's security posture to the level consistent with

⁵As noted earlier, DOE has now replaced the 2005 DBT (DOE Order 470.3A) with the Graded Security Protection plan (DOE Order 470.3B).

⁶Prior to this decision, NNSA had committed LLNL to meeting the 2005 DBT and had reported these plans to Congress in June 2006 as required by Section 3113 of the National Defense Authorization Act for Fiscal Year 2006 (Pub. L. No. 109-163, 119 Stat. 3136, 3543).

the larger adversary threat identified in DOE's 2005 DBT. However, DOE and NNSA are requiring LLNL to maintain a "denial-of-task" security strategy until de-inventory is complete. Under this strategy, any adversaries that gain hands-on access to special nuclear material must be neutralized. LLNL and NNSA documented the site's ability to meet the 2003 DBT through their approvals of LLNL's Site Safeguards and Security Plan, which had been revised and approved in January 2007, and through a validation force-on-force exercise conducted in December 2006.

To evaluate the effectiveness of sites' protection programs, DOE uses a three-stage evaluation model: laboratory self-assessment, federal site office security surveys, and Office of Independent Oversight inspections. In each stage of the evaluation model, the results of performance assurance tests are considered. All three stages are required to address laboratory safeguards and security programs comprehensively. More specifically:

- LLNL's self-assessment program is intended to provide the opportunity to self-identify security performance strengths and to address weaknesses internally before they can be exploited by a potential adversary. When security vulnerabilities are self-identified, these become the basis for federal decisions about how to mitigate them and what level of risk to accept. DOE requires that LLNL complete specific numbers and types of performance assurance tests to inform its self-assessments and assure DOE and NNSA that safeguards and security interests are being protected at their required levels.
- LSO security surveys are intended to confirm the availability and adequacy of safeguards and security programs, as implemented by LLNL. Surveys must be conducted annually and are based, in part, on direct observations of security performance, including compliance with DOE and NNSA security directives. LSO may also consider LLNL's security self-assessment as part of its annual survey as well as its performance assurance test results. To be comprehensive, LSO surveys cover eight topical areas and 33 subtopical areas and provide one of three ratings: satisfactory—the element being evaluated meets protection objectives or provides reasonable assurance that protection objectives are being met; marginal—the element being evaluated partially meets protection objectives or provides questionable assurance that protection objectives are being met; or unsatisfactory—the element being evaluated does not meet protection objectives or does not provide adequate assurance that protection objectives are being met. LSO may identify security deficiencies that are required to be addressed through corrective actions.

-
- The inspections by DOE's Office of Independent Oversight evaluate LLNL's and LSO's security performance. To determine the adequacy of security policy and the implementation of those policies, the Office of Independent Oversight conducts its own performance assurance tests of key security systems, observes security performance, and conducts interviews. Inspections result in reports, which may identify deficiencies that must be addressed through corrective actions. To be comprehensive, Office of Independent Oversight inspections cover eight topical areas and 36 subtopical areas⁷ (see app. I) and provide one of three ratings: effective performance—the system inspected provides reasonable assurance that the identified protection needs are met; needs improvement—the system inspected only partially meets identified protection needs or provides questionable assurance that the identified protection needs are met; or significant weakness—the system inspected does not adequately assure that identified protection needs are met.

DOE's Office of Independent Oversight Identified Several Significant Weaknesses in LLNL's Safeguards and Security Program

During the course of its April 2008 inspection, the Office of Independent Oversight found significant weaknesses in LLNL's protective forces' performance against the adversary threat identified in DOE's 2003 DBT, particularly during force-on-force scenarios and in other types of performance assurance testing. Deficiencies identified in LLNL's protection program management contributed to the protective forces' poor performance. In addition, the office identified deficiencies in LLNL's classified matter protection and control programs, which are intended to provide protection against unauthorized disclosure of classified matter, as well as in LLNL's physical security systems. LLNL's security performance in two other security topical areas—material control and accountability, and personnel security⁸—was rated effective.⁹ Table 1 describes the Office

⁷LSO and the Office of Independent Oversight categorize the topics and subtopics they cover differently. The Office of Independent Oversight also includes in its inspections subtopics covering safeguards and security at LSO.

⁸While the Office of Independent Oversight gave an effective performance rating to LLNL's personnel security program, in December 2008 DOE's Office of Inspector General found that LLNL did not fully adhere to DOE requirements regarding security clearance justifications and that no internal controls were in place to validate the justifications stated in security clearance requests. See U.S. Department of Energy, Office of Inspector General, Office of Inspections and Special Inquiries, *Security Clearances at Lawrence Livermore National Laboratory and Sandia National Laboratory-California*, INS-O-09-01 (Washington, D.C.: December 2008).

⁹The Office of Independent Oversight also inspected classified and unclassified cyber security at LLNL. Separately, we are reviewing cyber security across the DOE complex, including at LLNL, and therefore we did not include an assessment of cyber security findings at LLNL as part of this review.

of Independent Oversight's overall findings for LLNL. The office also identified 12 security deficiencies for LSO.

Table 1: LLNL Security Deficiencies Identified by the Office of Independent Oversight, by Topical Area, April 2008

Topical area	Number of findings	Overall rating
Protective force	13	Significant weakness
Classified matter protection and control	7	Significant weakness
Physical security systems	7	Needs improvement
Protection program management	7	Needs improvement
Personnel security	4	Effective performance
Material control and accountability	0	Effective performance

Source: Office of Independent Oversight.

Note: The Office of Independent Oversight identified an additional 16 security deficiency findings in cyber security that were outside the scope of our review.

LLNL's Protective Force Performed Poorly in an Exercise against the 2003 DBT

Despite an approved Site Safeguards and Security Plan and performance tests that validated LLNL's ability to defend against the 2003 DBT, DOE's Office of Independent Oversight identified 13 specific deficiencies in LLNL's protective force's performance; these deficiencies resulted in an overall rating of significant weakness, the lowest rating possible. These deficiencies became most apparent during force-on-force exercises designed to evaluate tactical response capabilities associated with the protection of LLNL's special nuclear material inventory, as well as limited scope performance tests to determine skill levels associated with routine and emergency duties. Specifically, the Office of Independent Oversight found the following:

- LLNL had not conducted an annual force-on-force exercise, as required by DOE Manual 470-4.3, *Protective Force*. Prior to the April 2008 exercise conducted during the Office of Independent Oversight's inspection, LLNL had not conducted a full force-on-force exercise since December 2006, when LLNL validated the site's ability to meet the adversary threat postulated by the 2003 DBT.
- Other quarterly performance assurance tests, also required by DOE Manual 470-4.1, were too limited in scope to meet performance testing

requirements. In addition, not all required quarterly performance assurance tests were completed.

- LLNL protective force members did not demonstrate proficiency in specific response capabilities, such as donning chemical masks in the required time.
- Communication among protective force members was poor during the force-on-force exercise and did not facilitate rapid and effective response to alarms and adversary movements.
- While protective force members performed well in individual qualification tests, the protective force did not demonstrate effective team tactics.
- Protective force commanders did not demonstrate sufficient command and control capabilities during the force-on-force exercise to effectively direct tactical units.
- Protective force members failed to respond to their fighting positions as required by LLNL's Security Incident Response Plan.
- LLNL's mobile weapon platform—an armored vehicle that carries a mounted M-134D Dillon multi-barreled machine gun and that was identified in the laboratory's approved Site Safeguards and Security Plan as key to the site's security—failed to competently support the protection mission. Numerous technical problems were noted with the weapon system's operation, and officers were unable to perform operational tests of the weapon at the Superblock because of safety and security concerns. Furthermore, officers were not allowed to train with the weapon at LLNL's nearby training range because of environmental concerns.
- LLNL experienced "controller errors" when those running the exercise failed to communicate critical information on simulated events—such as explosions—that might have affected the exercise's outcome. Office of Independent Oversight and LLNL officials agreed that errors of this nature can be attributed to a lack of practice in conducting force-on-force exercises.

In several instances, LLNL security officials knew of the deficiencies identified by the Office of Independent Oversight before the April 2008 inspection, but had not committed to corrective actions. For example, LLNL security officials were aware of some mechanical problems with the mobile weapon platform before April 2008. Officials said the full extent of the problems was not known because the platform had not been sufficiently tested in an operational environment. Officials explained that

performance tests of the mobile weapon platform did not include tests of how effectively the weapon would function in different attack scenarios, but rather tested officers' response times for getting to the weapon and positioning it. Nevertheless, a review of LLNL's quarterly performance assurance testing reports to LSO shows that LLNL reported completing 100 percent of required performance tests on all essential protection strategy elements, including the mobile weapons platform. These reports do not include the results of the performance assurance tests; they only state that the tests were conducted. LLNL has since taken steps to improve the reliability of the mobile weapon platform, and a complete review of the electrical and mechanical systems is underway. Similarly, in 2006, LSO found that LLNL had not conducted its annually-required force-on-force exercise. There was an 18-month gap between a June 2005 exercise at LLNL and the one conducted in December 2006 to validate LLNL's protection strategy against the 2003 DBT.

Deficiencies in LLNL's protection program management also contributed to the protective forces' poor performance. The Office of Independent Oversight found seven security deficiencies in the area of protection program management—LLNL's security program planning and assurance activities—and rated this security topic as needing improvement. The seven findings were focused on three areas of security planning and feedback: vulnerability assessment, self-assessment, and performance assurance testing. More specifically, the office found the following:

- The evidence files to support the vulnerability assessments underpinning LLNL's Site Safeguards and Security Plan were incomplete and raised questions about the scope and methodology used to prepare vulnerability assessments.
- LLNL's security self-assessment program was not comprehensive and individual assessments of security elements lacked the breadth and depth to provide management with information necessary to make meaningful decisions.
- The list of essential security program elements LLNL had included in its performance assurance test plan was incomplete and the performance assurance tests did not always include measures that would test the effectiveness of these elements.

DOE Concluded That LLNL's Protection and Control over Classified Matter Was Deficient

DOE Manual 470.4-4, *Information Security*, lays out the classified matter protection and control requirements that are intended to prevent the unauthorized disclosure of classified matter. Protection strategies include properly marking classified documents and media to make visible their classification level and other information; using security containers (or safes), vaults, and vault-type rooms for classified matter storage; having accountability systems that use unique identification numbers for controlling access to and movement of certain classified matter; and having access barriers, such as combination locks. Other physical security systems—such as alarms and sensors to detect unauthorized access to rooms storing classified matter—are considered separately during Office of Independent Oversight inspections.

According to DOE officials, in the area of classified matter protection and control, none of the seven individual findings of security deficiencies would independently have resulted in a rating of significant weaknesses; however, in total, the deficiencies identified led officials to question the overall effectiveness of LLNL's classified matter protection and control program. More specifically, the Office of Independent Oversight found the following classified matter protection and control deficiencies:

- LLNL failed to comply with basic security requirements, such as the frequency of changes to safe combinations when individuals' needs for access to safes have changed; repeated errors in classified document marking; weaknesses in the timely completion of classification reviews for working papers; and errors in location records for all safes containing classified matter.
- Individual LLNL directorates' policies for storing accountable classified removable electronic media after hours were inconsistent and conflicted with DOE requirements.

DOE Identified Additional Areas of LLNL's Security Program That Needed Improvement

The Office of Independent Oversight also reported that LLNL's physical security systems needed improvement. The office identified seven security deficiencies, including the adequacy of the alarm systems' redundancy; the quality of lighting for, and images from, closed circuit television monitoring systems; the extent to which protective force posts needed repairs; and the protection strategy for security keys. Two of the office's findings involved the security of vault-type rooms in which classified matter is stored.

The personnel security and material control and accountability security areas received effective performance ratings from the Office of Independent Oversight in April 2008. However, four security deficiencies were found in the personnel security area. All four related to aspects of LLNL's Human Reliability Program, a program designed to ensure that individuals who occupy positions affording access to special nuclear and explosive materials meet the highest standards of reliability and physical and mental suitability.

A Weak Laboratory Self-Assessment Program and Insufficient Federal Oversight Contributed to Security Deficiencies at LLNL

Neither LLNL's security self-assessment program nor LSO's annual security survey identified the security performance deficiencies that DOE's Office of Independent Oversight found. According to one DOE official, both programs were "broken" and missed even the "low-hanging fruit" of compliance-oriented deficiencies that LLNL must now take actions to correct. More specifically, LLNL's self-assessment program did not identify security deficiencies in the laboratory's classified matter protection and control program or the performance assurance program established to test the operability and effectiveness of elements essential to LLNL's protective strategy. Furthermore, LSO's September 2007 annual security survey, completed only 6 months before the Office of Independent Oversight's inspection, resulted in 100-percent satisfactory ratings for the laboratory's security performance. The Office of Independent Oversight found LSO's survey program was not comprehensive, and LSO security officials said site office employees who conduct surveys need more subject matter training.

LLNL's Self-Assessment Program Did Not Identify the Security Deficiencies Identified by DOE's Office of Independent Oversight

DOE's safeguards and security orders require that self-assessments comprehensively cover all topical and subtopical areas in order to assure the adequacy and effectiveness of security programs and their implementation. However, LLNL's self-assessment program failed to identify the security deficiencies identified by DOE's Office of Independent Oversight because the program (1) was not comprehensively implemented and (2) not supported by an effective performance assurance testing regime. In terms of implementation, the office reported that LLNL's and LSO's collaborative approach to selecting high-priority security topical areas for self-assessment each year benefited the self-assessment program by making efficient use of limited resources; however, it also reported that several subtopic areas were not evaluated annually as required. Specifically:

-
- There had not been a comprehensive, site-wide assessment of safes containing classified matter for 3 years.
 - LLNL's self-assessments were not broad and deep enough to provide laboratory management with sufficient information to make meaningful decisions about security performance. For example, self-assessments completed in fiscal year 2007 did not describe the evaluation criteria used to perform the assessments.

DOE requires that all essential elements of a site's protection program be subject to performance testing to provide comprehensive assurance that the required levels of protection are met. Essential elements include the equipment (such as weapon systems), procedures (such as security incident response plans), and personnel (such as security police officers) components of LLNL's safeguards and security program. The failure of any of these components would reduce protection of departmental property to an unacceptable level. Each site, including LLNL, is required to develop a Performance Assurance Program Plan that describes the program and its implementation by identifying elements essential to the protection of Category I and II special nuclear material and Top Secret classified matter. The results of required performance assurance tests should contribute to the security topic self-assessments.

We reviewed LLNL's quarterly reports to LSO on the laboratory's performance assurance testing activities for fiscal year 2007 and the first half of fiscal year 2008. With the exception of the first quarter of fiscal year 2007, these reports show the performance testing requirements were met or exceeded. However, the Office of Independent Oversight's inspection revealed multiple deficiencies in the design and implementation of LLNL's performance assurance testing program. Specifically, the office found that (1) the individual test plans LLNL developed for essential protection elements did not always measure the effective performance of these elements; (2) not all essential elements were included in LLNL's performance assurance testing program; and (3) LLNL did not perform annual force-on-force exercises or quarterly integrated performance tests as required. The September 2007 LSO security survey also found that LLNL did not perform some performance assurance tests with the required frequency. Table 2 provides information on LLNL's required protective force performance assurance tests and deficiencies identified by the Office of Independent Oversight and LSO.

Table 2: LLNL's Required Protective Force Performance Assurance Testing

Type of test	Description	Minimum performance test frequency	Office of Independent Oversight and LSO findings
Limited Scope Performance Tests	Scheduled or unscheduled limited scope performance tests of individuals or teams test any operation, procedure, skill, or task performance that falls within the scope of protective force responsibility. Examples of these tests include individual and team tactical movement, arrest and control techniques, building clearing, command and control activities, and implementation of protection strategies.	Weekly at Category I/II special nuclear material facilities; all other facilities as required depending on security protection levels.	The Office of Independent Oversight found that LLNL's protective force lacked a specific protection capability that should have been demonstrated in limited scope performance tests. Further, technical problems with the mobile weapon platform should have been identified to a greater extent during limited scope performance tests. Finally, some limited scope performance tests did not effectively measure the performance of the security elements being tested.
Alarm Response and Assessment Performance Tests	Unscheduled tests based on simulated adversary actions consistent with the DBT to evaluate protective force response to a specific location under alarm protection and readiness to alarm conditions.	Twice per quarter at Category I/II special nuclear material facilities and other alarmed special nuclear material facilities; once per quarter at all other locations.	The LSO survey reported that LLNL failed to assure that the required number of alarm response and assessment performance tests were conducted.
Validation Force-on-Force Exercises	Major tests of all elements involved in response to a DBT and site-specific threats that is used to validate site-specific protection strategies.	Once per year per facility for all sites with armed protective force.	The Office of Independent Oversight noted LSO's finding in its report.
Command Post Exercises	Scheduled or unscheduled exercises conducted to observe and evaluate crisis teams' overall handling of simulated safeguards and/or security or a natural disaster incident. Lines of authority, timeliness of reporting and decision-making, and facility and equipment availability must be included.	Twice per year at Category I/II special nuclear material facilities, and once per year at all other facilities.	Not discussed.

Type of test	Description	Minimum performance test frequency	Office of Independent Oversight and LSO findings
Command Field Exercises	Extensions of Command Post Exercises, these exercises test the interaction among various support organizations, site management, and the protective force to a simulated event. Exercises focus on procedures, tactical intelligence, communications, logistics, and the interfaces between federal and contractor support systems.	Twice per year at Category I/II special nuclear material facilities, and once per year at all other facilities.	Not discussed.
Joint Training Exercises	Exercises conducted with outside agencies that support the successful mitigation of a security incident.	At least once per year and consistent with requirements of the Site Safeguards and Security Plan.	Not discussed.
Integrated Performance Tests	Scheduled tests encompassing all essential protection elements associated with a comprehensive site or facility threat scenario conducted to evaluate the overall facility safeguards and security effectiveness.	Category I facilities requiring denial protection strategies under the DBT (such as LLNL's Superblock) must conduct Integrated Performance Tests on a quarterly basis.	The Office of Independent Oversight reported that there was no evidence that LLNL's protective force had conducted quarterly integrated performance tests as required.
Training Exercises	Exercises involving each protective force shift are site-specific to the protective force in preventing the success of potential adversarial acts defined in the DBT.	Monthly.	Not discussed.

Sources: GAO analysis of DOE Manual 470.4-3, *Protective Force*; DOE Manual 470-4.1, *Safeguards and Security Program Planning and Management*; Lawrence Livermore National Laboratory, Safeguards and Security Organization Performance Testing and Assurance Program Plan, September 21, 2006; Department of Energy, Office of Health, Safety, and Security, Volume I: *Independent Oversight Safeguards and Security Inspection of the Livermore Site Office and the Lawrence Livermore National Laboratory*, June 26, 2008; and National Nuclear Security Administration, Livermore Site Office, *Periodic Safeguards and Security Survey of Lawrence Livermore National Laboratory (LLNL) October 2, 2006, through September 28, 2007*.

Had LLNL's self-assessment program been implemented comprehensively, with the required breadth and depth, and used performance assurance testing in addition to compliance-based reviews, security deficiencies identified by the Office of Independent Oversight might have been self-identified and corrected internally. This is particularly true with respect to deficiencies in the operation of the mobile weapon platform and protective force performance in command and control, communications, and team tactics. Significantly, the one area of LLNL security performance where the Office of Independent Oversight identified no security findings was nuclear material control and accountability. According to DOE and LLNL officials, the self-assessment program for nuclear material control and accountability provides assurance that all elements are evaluated. In addition, appropriate performance testing is conducted in this area. Since the April 2008 force-on-force exercise, LLNL has conducted four full-scale exercises—two each in August and November 2008—during which

protective force performance was successful. In addition, limited scope performance tests continue to be conducted to ensure readiness and knowledge of LLNL's Security Incident Response Plan. Furthermore, since April 2008 LLNL has conducted quarterly force-on-force exercises, which the laboratory believes fulfills the requirement to conduct quarterly integrated performance tests. According to a LLNL security official, LSO and LLNL disagree as to whether conducting quarterly force-on-force exercises meets the requirement to conduct quarterly integrated performance tests. The official said LLNL and LSO are working to resolve the disagreement.

LSO's Annual Security Survey Did Not Identify Deficiencies DOE Reported in 2008

LSO completed an annual survey of LLNL's security performance in September 2007, 6 months before the Office of Independent Oversight inspected LLNL in April 2008. The survey consisted of a year-long process during which LSO staff conducted assessments, walk-throughs, and observations to gather data on different security programs. As a result of this survey, LLNL received 100-percent satisfactory ratings in its security performance—differing markedly from the security performance DOE observed during its inspection a short time later. In particular, LSO's survey report noted as strengths that LLNL's self-assessment program was supported by laboratory management and that LLNL had succeeded in sustaining a protection strategy consistent with the 2003 DBT, assertions the Office of Independent Oversight inspection called into question. The LSO survey did result in six findings of security deficiencies: one for protective force, two for physical security systems, two for cyber security, and one for nuclear material control and accountability. For example, with respect to protective forces, LSO found that LLNL could not assure that it had conducted the necessary number of alarm response and assessment performance tests during the survey period. With respect to physical security, LSO found that LLNL did not adequately implement DOE requirements prohibiting employees from bringing personal laptop computers into secure locations and did not adequately implement a key management system.

The Office of Independent Oversight also includes a review of site offices' survey programs when it conducts its inspection of the protection program management security topic. In its April 2008 review, the office found LSO's survey program was deficient in several areas. Specifically, the office found that the LSO security survey:

- Was not comprehensive, as required by DOE Manual 470.4-1. LSO staff did not consistently follow the assessment schedule, did not prepare adequate

assessment plans, and did not retain evidence files of individual survey activities. It also did not provide enough data to assure that survey reports comply with DOE requirements to characterize the impact associated with observed deficiencies.

- Did not consistently assure that security deficiencies were identified or that identified deficiencies resulted in findings that would require corrective action. For example, the office noted that survey narratives pertaining to the physical security systems area identified several deficiencies; however, the survey program did not assign findings to these deficiencies, and the survey report did not describe LLNL's compensatory measures, as required.
- Resulted in a satisfactory rating for LLNL's self-assessment program without conducting the activities necessary to determine that the program was comprehensive.
- Used reviews of the contractor's records and the contractor's implementation of the performance assurance program to determine the status of compliance and performance of protective force duties, rather than conducting independent performance assessments of LLNL's protective force.

LSO security officials told us they are redesigning their security survey program in response to these findings. Rather than aggregating LSO security staffs' observations made over the course of a year, security at LLNL will be comprehensively surveyed during two set periods each year. These survey periods will be supplemented by continuous observation throughout the year. Surveys will continue to review compliance with DOE orders and requirements, but will also increase focus on assessing the extent to which security performance is effective. In addition, LSO is creating a security training program to ensure that all LSO officials who participate in the security survey program cover the different security topics comprehensively and are expert enough to recognize and report on deficiencies. According to LSO officials, site office employees have been responsible for identifying their own training needs and have had independence in determining how they met training requirements. Little formal training was provided on how to conduct security surveys. Rather, training was received on the job and through what one official described as an "oral tradition" of how to perform oversight activities. The new training program is designed around DOE security standards, and LSO officials said the majority of the training will be provided by DOE's National Training Center. The program is intended to ensure that LSO

security staff members are adequately trained to fulfill their duties and responsibilities. LSO's goal is to have all security staff qualified through this program by 2010. Underpinning this new training program is what LSO security officials described as a "cultural shift"—an effort to rely less on contractor assurance of security performance and more on independent, federal expertise to test and recognize that performance. However, according to LSO officials, LSO does not have a specific budget to implement this new security training program.¹⁰

LLNL Has Developed Corrective Action Plans to Address 54 Identified Security Deficiencies, and Both NNSA and DOE Will Oversee Their Implementation

Corrective Action Plans Are Intended to Address 54 Identified Security Deficiencies

LLNL has developed corrective actions to address the security deficiencies identified by the Office of Independent Oversight. LSO and DOE will oversee the implementation of these corrective actions, and NNSA will judge whether implementation was successful when it determines LLNS' contract award fee at the end of fiscal year 2009. While LLNL's corrective actions put the laboratory on a path toward improved security performance, LLNL has not sustained corrective actions intended to address security deficiencies identified in 1999 and 2002 that are similar to those identified by the Office of Independent Oversight in 2008.

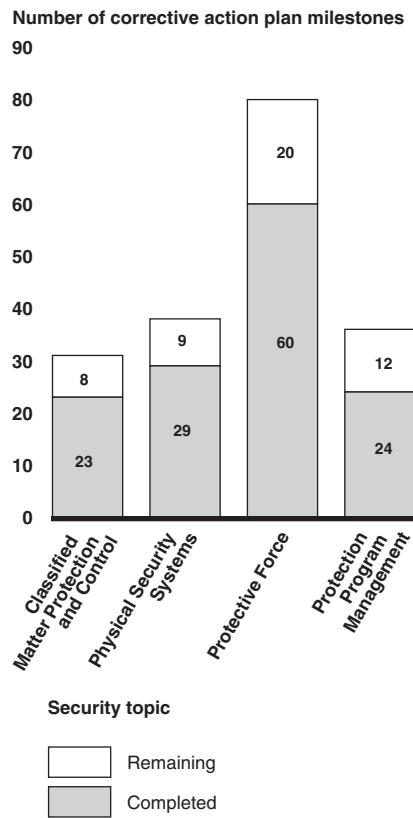
LLNL has developed corrective action plans to address 54 security deficiencies identified by the Office of Independent Oversight.¹¹ These plans include a total of 257 individual milestones, 185 of which are associated with the 4 security areas DOE rated as either having significant weaknesses or needing improvement. Corrective action plans associated with physical security deficiencies were made final between September and November, 2008. LLNL has reported that it will complete implementation of physical security milestones by October 30, 2009. As of

¹⁰We have reported in the past on the lack of comprehensiveness of site office security surveys and on a lack of training for site office staff. See GAO, *Nuclear Security: NNSA Needs to Better Manage Its Safeguards and Security Program*, GAO-03-471 (Washington, D.C.: May 30, 2003); and *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).

¹¹LLNL's 54 corrective action plans address both physical and cyber security findings. Of these plans, 34 corrective action plans address physical security topical areas that received less than effective performance ratings.

December 2008, LLNL reported having completed 136 of the 185 milestones, or about 74 percent (see fig. 1).

Figure 1: LLNL Corrective Action Milestones by Security Topic, as of December 2008



Source: GAO analysis of LLNL corrective action plans and milestone completion reports.

In compliance with DOE Manual 470.4-1, *Safeguards and Security Program Planning and Management*, each corrective action plan includes a root cause analysis, risk assessment, and cost-benefit analysis, where appropriate. To complete root cause analyses, LLNL used a DOE-agreed upon methodology and assigned root causes as directed by agency guidance. Of the 54 findings, LLNL determined that 29 had a single root cause, 18 had 2 root causes, 2 had 3 root causes, and 5 had 4 or more root causes. LLNL identified five recurring causes and issues as a result of its root cause analysis, including:

-
- *Resource allocation.* LLNL identified resource allocation as the single largest root cause of the security deficiencies. According to the Office of Independent Oversight, LLNL had sufficient financial and human resources to meet applicable protection requirements. However, LLNL and LSO officials believe that LLNL could not fully fund all security program activities within available security budgets. Instead, LLNL allocated security resources on the basis of a broad set of priorities, management decisions, and budget constraints, which resulted in unfunded security activities and accepted risks. By identifying resource allocation as a root cause of the security deficiencies, LLNL determined that security deficiencies might have been avoided if resources had been allocated differently.
 - *Work/organization planning.* In several cases, an activity or project was poorly planned or deviated from its plan because of time or budget constraints. In addition, some projects did not follow good project management practices or did not include contingency plans. For example, the Office of Independent Oversight found that a protective force armorer assigned to maintain weapons had not completed DOE's recertification requirements. LLNL determined that armorer recertification planning could be improved by adding this requirement to a training database.
 - *Policies and procedures.* In several instances, policies or procedures were not followed, and DOE orders and requirements were unclear or were interpreted differently from the Office of Independent Oversight's interpretation. For example, the Office of Independent Oversight found that LLNL did not follow DOE's requirement to conduct weekly inventories for all hard drives containing classified nuclear weapons design information. LLNL had interpreted DOE's requirement differently and did not conduct weekly inventories for hard drives that had been demagnetized, which makes the information stored on them unreadable.
 - *Training.* In several cases, training content did not adequately cover all requirements. In addition, LLNL reported that a lack of practical, hands-on experience—performance testing—was a contributing factor in many areas of protective force deficiencies. NNSA headquarters security officials told us that the lack of training was the main cause for the protective force's performance during the April 2008 force-on-force exercise.

LLNL, LSO, and DOE officials agreed on other factors that contributed to the laboratory's overall security performance. First, the change in management and operating contractor from the University of California to LLNS in October 2007 contributed to a loss of focus on security performance. According to LLNL security officials, during the period of

contract transition, employees' focus was on ensuring safety as well as on potential impacts on employee pensions. In addition, the contract transition contributed to a delay in conducting LLNL's required annual force-on-force exercise. Second, DOE's and NNSA's determination to declare LLNL a non-enduring site for Category I and II special nuclear material affected the morale of laboratory employees. LLNL security officials said highly experienced employees left the laboratory as a result of this declaration. Finally, successive changes to DOE's DBT policy between 2003 and 2005 affected the analytical process that underpins security planning. In particular, LLNL security officials said the laboratory faced challenges in completing necessary vulnerability assessments.

To complete corrective action plans' risk assessments, LLNL security officials evaluated the worst-case scenario presented by individual findings of security deficiencies relative to a set of seven risk areas: mission success, cost, schedule, health and safety, environment, safeguards and security, and political and public trust. Ultimately, each finding was assigned a single, overall risk level: negligible risk, low risk, moderate risk, or high risk. According to LLNL's analysis, 43 percent of the findings were determined to be of negligible risk, and 57 percent were determined to be of low risk. LLNL officials said the low risk ratings associated with each of these findings is associated with the relatively low likelihood of a worst case scenario ever occurring, as well as the level of redundancy that exists for security systems. In contrast to LLNL's risk assessment methodology, the Office of Independent Oversight based its security ratings on evaluations of management system performance.

The vast majority of the physical security corrective actions LLNL has planned can be completed using existing funding, according to the laboratory's plans. The complexity of these corrective actions and the costs associated with their implementation range from relatively simple and inexpensive to complex and expensive. For example, to correct one classified matter protection and control deficiency concerning policies for handling accountable classified removable electronic media after regular laboratory hours, LLNL plans to develop a new policy and conduct a series of briefings on how to implement the policy. Milestones associated with completing these corrective actions are straightforward and can be completed with existing funds.

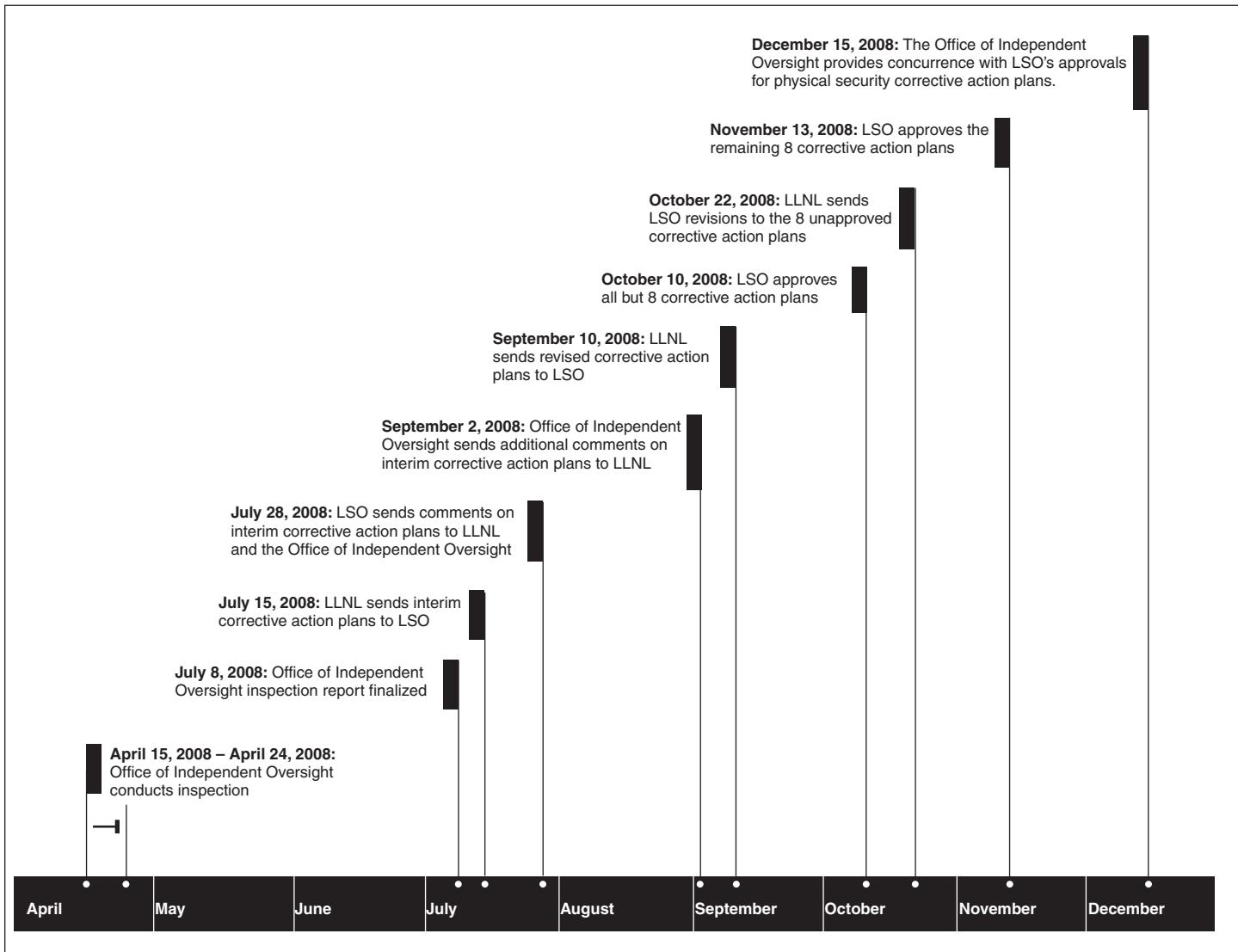
In contrast, to address the finding that LLNL's protective force had not conducted quarterly integrated performance assurance tests of sufficient scope, LLNL plans to redesign its performance assurance testing program and has already begun to conduct larger, more frequent protective force

exercises. According to LLNL and NNSA security officials, conducting additional performance assurance training has resulted in a 30-percent overtime increase for the protective force and a \$5.5 million budget shortfall in fiscal year 2009 to address findings and sustain this level of activity. According to NNSA, after an examination of security priorities and tradeoffs, the Office of Defense Nuclear Security provided LLNL with additional funding to cover this shortfall.

**NNSA and DOE Plan to
Oversee Implementation of
Corrective Actions**

LSO and the Office of Independent Oversight have overseen the development of LLNL's corrective action plans, and the completion of these plans has been an iterative process (see fig. 2). While the process was ongoing, LLNL took steps to complete milestones that would be included in final corrective action plans.

Figure 2: Timeline for the Development and Final Approval of LLNL's Corrective Action Plans



Source: GAO analysis of LLNL, LSO, and Office of Independent Oversight corrective action plan documentation.

LSO officials said they plan to meet with LLNL officials every month to review the status of the corrective actions. LSO is required to describe the overall implementation status of corrective action plans and the extent to which these actions are effective in its annual security survey reports. In addition, the Office of Independent Oversight has scheduled a follow-up security inspection of LLNL for April 2009 that will include a force-on-

force exercise. Office of Independent Oversight officials told us the inspection will also include a review of progress on corrective actions associated with the four security areas that received less than satisfactory ratings in 2008.

In keeping with the requirements of the National Defense Authorization Act for Fiscal Year 2000 which created NNSA,¹² NNSA's Office of Defense Nuclear Security has provided significant assistance to LLNL and LSO to help address identified security deficiencies. Office of Defense Nuclear Security officials have worked directly with LLNL to develop a recovery plan to improve the effectiveness of LLNL's protection strategy. In addition, Office of Defense Nuclear Security officials have assisted LLNL in identifying corrective actions, and have provided assistance in implementing these corrective actions effectively. For example, officials from the Office of Defense Nuclear Security observed force-on-force exercises conducted at LLNL in August and November 2008 and provided feedback. In addition, to help LSO better integrate its security activities and improve security oversight, the Office of Defense Nuclear Security temporarily augmented LSO's security staff with assistance teams of security experts from other NNSA site offices and from NNSA headquarters. These assistance teams provided independent technical reviews of revisions to LLNL's vulnerability assessment documentation, protection strategy, training and testing procedures, and Site Safeguards and Security Plan, as well as support in resolving issues associated with classified matter protection.

NNSA will ultimately judge the success of LLNL's corrective action implementation when it determines a contract award fee at the end of fiscal year 2009.¹³ In fiscal year 2008—LLNL's first year of contract performance evaluated under the new performance-based contract with LLNS—LLNS earned approximately \$17.2 million, or 54 percent of the

¹²Pub. L. No. 106-65, 113 Stat. 512, 953 (1999).

¹³According to LLNL's corrective action plans, one milestone to correct a protective force deficiency will not be completed before the end of fiscal year 2009. It is scheduled for completion on October 30, 2009.

total “at-risk” incentive fee available under the contract.¹⁴ This amount included \$1.3 million, or just 9 percent, of the total incentive fee available for safe and secure operations. NNSA identified the results of the Office of Independent Oversight’s inspection and the significant issues in LLNL’s physical and information security programs as concerns that contributed to the low award fee determination in this area. In particular, NNSA noted in its performance evaluation report for LLNL that considerable management attention from LLNS, NNSA, and DOE leadership was required to assure that the laboratory could meet protection requirements for special nuclear material. Furthermore, NNSA reported that LLNL failed to submit a security self-assessment report for fiscal year 2008, despite the Office of Independent Oversight’s findings on the laboratory’s self-assessment program.

LLNL Has Not Sustained Corrective Actions That Addressed Past Security Deficiencies

In its June 1999 and April 2002 inspections of security performance at LLNL, the Office of Independent Oversight identified weaknesses in LLNL’s protection program management and protective force performance, as well as numerous deficiencies in its classified matter protection and control program. LLNL implemented corrective actions, and the Office of Independent Oversight later rated LLNL’s performance as effective in these areas. However, LLNL did not sustain the corrective actions. Specifically:

- In 1999, the Office of Independent Oversight reported that LLNL’s capability to conduct the vulnerability assessments that underpin protection program planning was deficient. By 2000, LLNL had corrected this problem, and in a follow-up inspection the office called LLNL’s vulnerability assessment program a model for the rest of the nuclear weapons complex. In its 2008 inspection, however, the Office of Independent Oversight again reported several deficiencies in the area of vulnerability assessment.
- In 2002, the office found weaknesses in protective force training and command and control. These weaknesses appear to have been addressed by the time of the 2006 force-on-force exercise, when Office of

¹⁴In fiscal year 2008, \$1.5 million was deducted from the \$17.2 million in incentive fee that LLNS earned as a penalty for the loss of key personnel during the first year of the contract. However, LLNS also was awarded an additional \$21.9 million, which represents the fixed fees for laboratory management and operation (\$13.7 million) and work for other federal agencies and organizations (\$8.2 million). In total, LLNS earned \$37.5 million, or 70 percent of the maximum available total fee.

Independent Oversight officials said LLNL's protective force performed well. In its 2008 inspection, however, the office again found significant weaknesses in protective force training and command and control.

- In its 1999 inspection the office gave LLNL's classified matter protection and control program the lowest possible rating, but the office rated LLNL's program as satisfactory in a follow-up inspection 6 months later. Though some findings were reported in the interim, overall satisfactory ratings were maintained for classified matter protection and control until the Office of Independent Oversight's 2008 inspection.

According to officials in NNSA's Office of Defense Nuclear Security, it will be challenging to sustain the security improvements that result from LLNL's successful implementation of corrective actions because of the laboratory's non-enduring status and the drawdown in security resources that will come as special nuclear material de-inventory activities are completed. Officials said that NNSA must provide incentives to ensure that LLNL's protective force can sustain the appropriate levels of protection until de-inventory is complete. According to a senior LSO official, sustaining attention on security performance could be difficult as NNSA priorities shift and future Site Office management weighs NNSA priorities. LLNL has taken steps to ensure a sufficient number of protective force members will remain employed by the laboratory to protect Category I and II special nuclear material throughout the de-inventory process as currently scheduled. A new collective bargaining agreement with LLNL's protective force union, concluded in December 2008, expires at the end of fiscal year 2012. The agreement includes annual, additional lump sum payments of up to \$50,000 over 3 years to protective force members who remain at LLNL during the de-inventory process.

LLNL Faces Challenges in Implementing Plans to Complete De-inventory of Its Category I and II Special Nuclear Material by the End of Fiscal Year 2012

When DOE concurred with NNSA's decision to remove Category I and II special nuclear material from LLNL, the de-inventory process was expected to be completed no later than the end of fiscal year 2014. According to officials from NNSA's Office of Nuclear Material Management Integration, NNSA decided to accelerate this schedule and complete de-inventory by the end of fiscal year 2012 as part of its efforts to transform the nuclear weapons complex. LLNL has completed a detailed schedule and associated resource-loaded project management documentation in support of the 2012 de-inventory date. NNSA officials said this accelerated schedule does not include any contingency funds set aside for risks within the project scope; however, LLNL officials said the schedule is aggressive but realistic. As of August 2008, LLNL had already decreased its inventory of Category I and II special nuclear material by approximately 33 percent from the laboratory's fiscal year 2006 inventory.

In order to de-inventory most of its special nuclear material, LLNL must stabilize the material and package it according to DOE standards for shipment to a receiving site.¹⁵ The stabilization process uses special equipment, such as furnaces and gloveboxes, to remove impurities. The material packages are containers approved for use in transporting Category I and II special nuclear material to storage and other disposition sites. Given these requirements, it takes time to prepare packages for shipment. For example, according to LLNL it takes approximately 2 months to prepare each package of plutonium oxide for shipment. LLNL plans to ship over 250 packages of special nuclear material to sites around the nuclear weapons complex to complete the de-inventory, including Los Alamos National Laboratory; the Nevada Test Site; the Savannah River Site in Aiken, South Carolina; the Y-12 National Security Complex in Oak Ridge, Tennessee; the Idaho National Laboratory near Idaho Falls, Idaho; and the Waste Isolation Pilot Plant, in Carlsbad, New Mexico. Each of these sites has particular safety requirements in place that govern the types and amounts of material they can receive. For example, according to NNSA officials, the Savannah River Site can only receive material excess to programmatic needs. Similarly, the Waste Isolation Pilot Plant can only receive certain waste material. Work to stabilize and package LLNL's special nuclear material inventory is being conducted at Superblock while programmatic operations are ongoing.

¹⁵DOE-STD-3013-2004 *Stabilization, Packaging, and Storage of Plutonium-Bearing Materials* (April 2004); and DOE-STD-3028-2000 *Criteria for Packaging and Storing Uranium-233-Bearing Materials* (July 2000).

The plan to de-inventory LLNL's Category I and II special nuclear material by the end of fiscal year 2012 is challenging because executing it depends on a number of factors, some of which LLNL does not control. Specifically:

- *The willingness and ability of other NNSA and DOE sites to receive the material.* NNSA officials said work stoppages at receiving sites could delay shipments, as could disputes over the terms of receiving special nuclear material. NNSA's Office of Nuclear Material Management Integration, an office NNSA created in July 2008 to coordinate the consolidation of special nuclear material among DOE sites, is helping to anticipate material acceptance issues by conducting monthly videoconferences with LLNL and receiving sites.
- *The Superblock facility will be operational nearly 100 percent of the time through fiscal year 2012.* According to NNSA officials, there is always a chance of a work stoppage in Superblock. At least one lengthy, safety-related work stoppage at Superblock occurred in the recent past and lasted approximately 16 months, from January 2005 to May 2006, until operations fully resumed.
- *Timely and adequate funding.* LLNL estimates the entire de-inventory process will cost \$41.3 million over 5 years (fiscal years 2008 through 2012). This estimate does not include inflation or contingency funding.
- *The availability of specialized shipping packages and transport trucks consistent with the de-inventory schedule.* All sites within the nuclear weapons complex use the same shipping packages and rely on NNSA's Office of Secure Transportation to safely and securely move special nuclear material. The current de-inventory schedule plans to have completed packaging and shipment of 90 percent of the inventory by March 2011. The final 10 percent of the material, the most difficult to process, will take the remaining 18 months. Any change in the availability of packages or transport trucks could affect the de-inventory schedule.
- *The availability of skilled staff and fissile materials handlers.* According to a LLNL official, a limited number of people are qualified to use the equipment at LLNL necessary to stabilize and package special nuclear material, and the number of skilled staff may diminish as the laboratory's special nuclear material inventory diminishes.
- *The on-time procurement, installation, and startup of additional equipment.* In order to meet the accelerated 2012 schedule, LLNL is procuring and installing additional equipment to add capabilities specific to the stabilization processes for certain metals and oxides. The last of

these capabilities is expected to come on line in June 2009. A delay could potentially affect the de-inventory schedule.

According to LLNL and NNSA officials, there are not any feasible options that would allow substantial acceleration of the de-inventory schedule. We agree with this assessment. LLNL explored three options for further schedule acceleration. First, LLNL assessed the extent to which increasing its processing rate for special nuclear material by adding manpower or installing additional processing equipment would accelerate de-inventory. LLNL determined that only moderate schedule gains would be made by adding manpower because processing equipment is already operating 24 hours a day, 7 days a week. Installing additional processing equipment is not feasible because, according to LLNL, startup of new equipment of this type generally takes several years and would not be operational in time to affect the de-inventory process as currently scheduled. Second, LLNL explored options for shipping materials to other sites for processing at a later date. LLNL determined that this option is not feasible because sites do not have enough storage space for material that is not yet packaged. Furthermore, a LLNL official said other sites do not have processing capability, and material would have to be shipped back to LLNL for processing at a later date. Moreover, sites have restrictions on the types of material they can receive. Finally, DOE looked at whether the Department of Transportation's regulatory requirements for packaging and shipping could be relaxed. DOE and LLNL determined that any such relaxation would unacceptably increase safety, environmental, and security risks.

Conclusions

It is essential that sites adequately protect the Category I and II special nuclear material they possess, given the threats and risks this material poses. Until LLNL has fully completed the process of de-inventorying its Category I and II special nuclear material from Superblock, it must maintain a high level of security. As LLNL's inventory of Category I and II special nuclear material diminishes, it may prove difficult to sustain the level of security vigilance expected of Category I sites. Even after Category I and II special nuclear material is no longer present at LLNL, LSO's security oversight responsibilities will continue because laboratory employees must comply with requirements for protecting and controlling classified matter and lesser categories of special nuclear material. Strong federal oversight can help ensure that security remains a priority at LLNL and that corrective actions implemented as a result of the Office of Independent Oversight's April 2008 inspection are sustained. To do this, a federal site office with adequately trained subject matter experts to

perform comprehensive security oversight, as required by DOE policies, is needed. In addition, NNSA's annual performance evaluation plans, associated with its management and operating contract for the laboratory, include financial incentives for security performance. NNSA can use performance evaluation plans to provide LLNS with financial incentives to sustain laboratory security improvements.

Recommendations for Executive Action

To improve and sustain federal oversight of security performance at LLNL, we recommend that the Administrator of NNSA and the LSO Manager take the following two actions:

- Develop a detailed plan and budget for implementing LSO's proposed security training program.
- Incorporate financial incentives into future performance evaluation plans, as allowed by the new LLNS management and operating contract, for sustaining security improvements at LLNL through the completion of the laboratory's Category I and II special nuclear material de-inventory.

Agency Comments and Our Evaluation

We provided a draft of this report to NNSA for its review and comment. NNSA generally agreed with the report and its recommendations. NNSA noted that in its view the Office of Defense Nuclear Security and LSO are providing strong oversight over security at LLNL to ensure that security improvements are fully implemented and sustained. In particular, NNSA emphasized the Office of Defense Nuclear Security's role in supporting the overall improvement of security at LLNL. NNSA's comments on our draft report are presented in appendix II. NNSA also provided technical comments, which we incorporated into the report as appropriate.

As arranged with your offices, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after the date of this report. At that time, we will send copies of this report to the Secretary of Energy; Administrator of NNSA; Director of LLNL; and appropriate congressional committees. In addition, the report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or your staffs have any questions about this report or need additional information, please contact me at (202) 512-3841 or aloise@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Appendix III lists key contributors to this report.

A handwritten signature in black ink that reads "Gene Aloise". The signature is fluid and cursive, with "Gene" on the first line and "Aloise" on the second line.

Gene Aloise
Director, Natural Resources
and Environment

Appendix I: Safeguards and Security Topics Covered in Office of Independent Oversight Inspections

Safeguards and security topics	Program definition
Protection Program Management <ul style="list-style-type: none">• Planning process• Organization and staffing• Budget process• Program direction• Control systems• Survey program	Programs are designed to ensure that security interests are provided an appropriate degree of protection from hostile acts. It is an iterative process, whereby activities related to planning, staffing, budget, direction, and feedback are integrated with overall strategic and near-term operational planning.
Physical Security Systems <ul style="list-style-type: none">• Intrusion detection assessment• Entry and search controls• Badges, passes, and credentials• Barriers• Communications• Testing and maintenance	Programs are designed to use intrusion detection and assessment, entry and search control, barriers, communications, testing and maintenance, and supporting systems and interfaces to deter, detect, annunciate, assess, delay, and communicate an unauthorized activity.
Protective Force <ul style="list-style-type: none">• Management• Training• Equipment and facilities• Duties	Programs are designed to protect both DOE security interests from theft, sabotage, and other hostile acts that may adversely impact national security or the health and safety of the public, as well as life and property at DOE facilities.
Classified Matter Protection and Control <ul style="list-style-type: none">• Program management• Control of secret and confidential documents• Control of top secret documents• Control of classified materials• Special programs• Operations security• Technical surveillance countermeasures• Classification management	Programs are designed to provide protection against unauthorized disclosure of classified matter and for sensitive information from its inception to destruction or decontrol.
Material Control and Accountability <ul style="list-style-type: none">• Administration• Accounting• Measurements• Inventories• Containment	Programs are designed to provide an information and control system for nuclear material. These programs encompass those systems and measures necessary to establish and track nuclear material inventories, control access, detect loss or diversion of nuclear material, and ensure the integrity of those systems and measures.

**Appendix I: Safeguards and Security Topics
Covered in Office of Independent Oversight
Inspections**

Safeguards and security topics	Program definition
Personnel Security <ul style="list-style-type: none">• Management• Personnel clearance program• Security education program• Visitor control program• Human reliability program	Programs are designed to ensure that access to sensitive information, classified matter, and special nuclear material will be granted only after it has been determined that such access will not endanger security and is consistent with the national interest.
Cyber Security—classified and unclassified	Programs are designed to prevent deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, modification, or loss of information contained within computer networks and systems, as well as measures designed to prevent denial of authorized use of the system.

Source: Office of Independent Oversight's inspector guides.

Note: The Office of Independent Oversight inspects classified and unclassified cyber security as separate security topics.

Appendix II: Comments from the National Nuclear Security Administration



Department of Energy
National Nuclear Security Administration
Washington DC 20585

March 5, 2009

OFFICE OF THE ADMINISTRATOR

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

Dear Mr. Aloise:

The National Nuclear Security Administration (NNSA) appreciates the opportunity to review the Government Accountability Office's (GAO) draft report, GAO-09-321, "NUCLEAR SECURITY: Better Oversight Needed to Ensure that Security Improvements at Lawrence Livermore National Laboratory Are Fully Implemented and Sustained." We understand that GAO conducted this audit at the request of the House's Committee on Homeland Security to assess aspects of Livermore's security posture.

The NNSA generally agrees with the report and recommendations. Following the Office of Independent Oversight's inspection of the Livermore Site Office (LSO) and Lawrence Livermore National Laboratory (LLNL) that identified significant weaknesses in the security program at the Laboratory, LLNL initiated an aggressive plan to improve the effectiveness of its protection strategy in coordination with the Office of Defense Nuclear Security (DNS) and LSO. DNS has devoted considerable resources supplementing LSO's efforts to oversee improvements to LLNL security and will continue to provide significant support and validate the site's capability of moving forward in a positive manner. Through the DNS/LSO collaboration, teams of security experts have monitored and evaluated the security strategy upgrades and a revision to the Security Incident Response Plan to ensure they were effective. The teams actively worked to provide independent technical reviews for vulnerability assessment actions, as well as protective force strategy and training/testing procedures, and provided advice and procedures for further improvements. Additionally, LLNL has made good progress in their de-inventory efforts in that they have recently relocated 20% of their special nuclear material inventory for a total of a 55% reduction since the site's de-inventory effort began. The active role of LSO and DNS provides strong oversight of the Laboratory's security program to ensure the implementation and sustainment of the LLNL security posture.

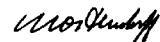


Printed with soy ink on recycled paper

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

Enclosed are general and technical comments to the report for your consideration. Should you have any questions about this response, please contact Cathy Tullis, Acting Director, Policy and Internal Controls Management.

Sincerely,



William C. Ostendorff
Principal Deputy Administrator

Enclosure

cc: Associate Administrator for Defense Nuclear Security
Director, Service Center
Senior Procurement Executive

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the individual named above, Jonathan Gill and John Cooney, Assistant Directors; Allison Bawden; Tom Twambly; Ray Rodriguez; Omari Norman; Jamie Roberts; Tim Persons; Nabajyoti Barkakati; and Carol Hernstadt Shulman made important 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