September 25, 2008

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

NUCLEAR SECURITY

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

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.