October 2009

INFORMATION SECURITY

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

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-28, a report to congressional committees

Why GAO Did This Study

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

What GAO Recommends

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

NNSA generally agreed with a draft of this report.

View GAO-10-28 key components.
For more information, contact Gene Aloise at (202) 512-3841 or aloisee@gao.gov; Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov; or Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

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

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

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