December 2010

INFORMATION SECURITY

National Nuclear Security Administration Needs to Improve Contingency Planning for Its Classified Supercomputing Operations

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-11-67, a report to congressional requesters

Why GAO Did This Study

In the absence of underground nuclear weapons testing, the National Nuclear Security Administration (NNSA) relies on its supercomputing operations at its three weapons laboratories to simulate the effects of changes to current weapons systems, calculate the confidence of future untested systems, and ensure military requirements are met.

GAO was requested to assess the extent to which (1) NNSA has implemented contingency and disaster recovery planning and testing for its classified supercomputing systems, (2) the laboratories are able to share supercomputing capacity for recovery operations, and (3) NNSA tracks the costs for contingency and disaster recovery planning for supercomputing assets. To do this work, GAO examined contingency and disaster recovery planning policies and activities, and analyzed classified supercomputing capabilities at the weapons laboratories, and NNSA budgetary data.

What GAO Recommends

GAO recommends, among other things, that NNSA clearly define roles and responsibilities for its component organizations in providing oversight for contingency and disaster recovery planning for the classified supercomputing environment. NNSA agreed with most of GAO's recommendations, but did not concur with recommendations relating to capacity planning and cost tracking.

View GAO-11-67 or key components. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, Gene Aloise at (202) 512-3841 or aloisee@gao.gov, or Naba Barkakati at (202) 512-6415 or barkakatin@gao.gov.

What GAO Found

All three NNSA weapons laboratories—Los Alamos, Sandia, and Lawrence Livermore—have implemented some components of a contingency planning and disaster recovery program. NNSA, however, has not provided effective oversight to ensure that the laboratories have comprehensive and effective contingency and disaster recovery planning and testing. Further, due to lack of planning and analysis by NNSA and the laboratories, the impact of a system outage is unclear. Only one of the three laboratories—Los Alamos—had conducted a business impact analysis to assess the criticality of resources and acceptable outage time frames; yet, NNSA and all three laboratories consider the consequence associated with the loss of system availability to be low impact and do not consider the classified supercomputers to be mission critical. Nonetheless, NNSA classified supercomputing capabilities serve as a computational surrogate to nuclear weapons testing and are used to address other areas of national security. Despite the absence of business impact analyses, all laboratories had key components of a contingency planning program in place. However, shortcomings existed. For example, all laboratories had backup processes in place and had developed contingency plans, but the plans were not comprehensive. Specifically, one plan did not address the supercomputing operations, and none of the plans had been tested at the time of GAO's review. In addition, the laboratories addressed disaster recovery to a limited extent, but not specifically for the supercomputers. These shortcomings existed, at least in part, because NNSA's component organizations, including the Office of the Chief Information Officer, were unclear about their roles and responsibilities for providing oversight in the laboratories' implementation of contingency and disaster recovery planning. Until the agency fully implements a contingency and disaster recovery planning program for its weapons laboratories, it has limited assurance that vital information can be recovered and made available to meet national security priorities and requirements.

Although the laboratories have the technological capability to share supercomputing capacity across all three weapons laboratories, barriers exist that could impede recovery operations. For example, the laboratories do not know the minimum supercomputing capacity needed to meet program requirements, such as simulating the effects of changes to weapons systems, should a disruption occur. In addition, the laboratories have not tested the technological capability to share the capacity on an on-demand basis for recovery operations. Without having an understanding of capacity needs and subsequent testing, the laboratories have little assurance that they could effectively share capacity if needed.

Although NNSA obligated approximately $1.7 billion to help implement its classified supercomputing program from fiscal years 2007 through 2009, the agency has not tracked costs for contingency and disaster recovery planning and is uncertain of actual funds that were spent toward these efforts.