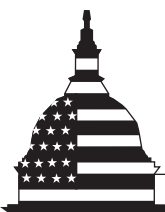


December 2010

# INFORMATION SECURITY

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



G A O

Accountability \* Integrity \* Reliability

## 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 [wilshusen@gao.gov](mailto:wilshusen@gao.gov), Gene Aloise at (202) 512-3841 or [aloisee@gao.gov](mailto:aloisee@gao.gov), or Naba Barkakati at (202) 512-6415 or [barkakatin@gao.gov](mailto:barkakatin@gao.gov).

## INFORMATION SECURITY

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

## 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.

---

# Contents

---

<b>Letter</b>		1
	Background	3
	NNSA Has Not Fully Implemented Contingency and Disaster Recovery Planning and Testing for Its Classified Supercomputing Assets	11
	The Laboratories Have the Ability to Share Supercomputing Capacity, but Barriers Exist	18
	NNSA Does Not Track the Costs for Ensuring Contingency and Disaster Recovery Planning for Its Supercomputing Assets	20
	Conclusions	21
	Recommendations for Executive Action	22
	Agency Comments and Our Evaluation	23
<b>Appendix I</b>	<b>Objectives, Scope, and Methodology</b>	26
<b>Appendix II</b>	<b>NNSA Annual Obligations for Its Advanced Simulation and Computing Program, Fiscal Years 2007 through 2009</b>	28
<b>Appendix III</b>	<b>Comments from the National Nuclear Security Administration</b>	31
<b>Appendix IV</b>	<b>GAO Contacts and Staff Acknowledgments</b>	34
<b>Table</b>		
	Table 1: Inventory of NNSA-Deployed Classified Supercomputing Systems (as of October 2010)	6
<b>Figures</b>		
	Figure 1: Common Hardware Components of a Supercomputing System	4

---

---

Figure 2: NNSA’s Classified Supercomputing Network Infrastructure	7
Figure 3: Total Usable Supercomputing Capacity at Each Weapons Laboratory, 2010 and 2011	19
Figure 4: Annual Obligations for NNSA’s Advanced Simulation and Computing Program, Fiscal Years 2007 through 2009	29

---

### Abbreviations

ASC	Advanced Simulation and Computing
BIA	business impact analysis
CNSS	Committee on National Security Systems
DISCOM	Distance Computing
DOD	Department of Defense
DOE	Department of Energy
FISMA	Federal Information Security Management Act of 2002
FLOPS	floating-point operations per second
Livermore	Lawrence Livermore National Laboratory
Los Alamos	Los Alamos National Laboratory
NIST	National Institute of Standards and Technology
NNSA	National Nuclear Security Administration
Sandia	Sandia National Laboratories

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.



**G A O**

Accountability \* Integrity \* Reliability

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

---

December 9, 2010

The Honorable Henry Waxman  
Chairman  
Committee on Energy and Commerce  
House of Representatives

The Honorable Edward J. Markey  
Chairman  
Subcommittee on Energy and the Environment  
Committee on Energy and Commerce  
House of Representatives

The Honorable Bart Stupak  
Chairman  
Subcommittee on Oversight and Investigations  
Committee on Energy and Commerce  
House of Representatives

The National Nuclear Security Administration<sup>1</sup> (NNSA) provides classified supercomputing capabilities for assessing the performance of nuclear weapons. In the absence of nuclear weapons testing—which ceased in 1992—the simulation capabilities of NNSA’s supercomputers are a necessary means to determine the effects of changes to current weapons systems and to determine a level of confidence in the performance of future untested systems.<sup>2</sup> These simulation capabilities also contribute to the enhancement of NNSA’s ability to predict the performance of weapons systems to ensure the systems meet all military requirements established by the Department of Defense (DOD).

NNSA’s three nuclear weapons laboratories—Los Alamos National Laboratory (Los Alamos) in New Mexico, Lawrence Livermore National Laboratory (Livermore) in California, and the Sandia National

---

<sup>1</sup>NNSA was established in 2000 as a separately organized agency within the Department of Energy (DOE) and is responsible for the nation’s nuclear weapons, nonproliferation, and naval reactors programs.

<sup>2</sup>For nearly half a century, the United States’ nuclear program was spearheaded by underground nuclear testing and never had to rely on weapon systems that had exceeded their design life times. The United States last produced a nuclear weapon in 1991 and performed its last underground nuclear test in 1992.

---

Laboratories (Sandia) with locations in New Mexico and California—use these supercomputing simulation capabilities to obtain a comprehensive understanding of the entire nuclear weapons life cycle, from design to safe processes for dismantlement. These classified supercomputing capabilities are a considerable investment and serve as a cornerstone for NNSA's Stockpile Stewardship Program.<sup>3</sup> In addition, classified supercomputing capabilities are essential for informing critical decisions related to the nuclear stockpile, including all stockpile modernization and warhead studies. NNSA classified supercomputing capabilities are also used to address other areas of national security, including intelligence analyses, nuclear forensics, and emergency response. Because of the importance of these classified supercomputing capabilities to issues central to national security, contingency and disaster recovery planning<sup>4</sup> are key to ensuring that, when unexpected events occur, NNSA can recover and reconstitute its classified supercomputing systems, data, and operations.

Our objectives were to assess the extent to which (1) NNSA has implemented contingency and disaster recovery planning and testing for its classified supercomputing assets, (2) the three laboratories are able to share classified supercomputing capacity for recovery operations, should service disruptions occur, and (3) NNSA tracks the costs for ensuring contingency and disaster recovery planning for its classified supercomputing assets. To accomplish these objectives, we examined contingency and disaster recovery planning controls for the systems

---

<sup>3</sup>The *National Defense Authorization Act for Fiscal Year 1994*, Pub. L. No. 103-160, § 3138 (1993), directed DOE to establish the Stockpile Stewardship Program. In the absence of underground nuclear testing, the program encompasses a broad range of activities to increase understanding of the basic phenomena associated with nuclear weapons, provide better predictive understanding of the safety and reliability of weapons, and ensure a strong scientific and technical basis for future nuclear weapons policy objectives. The Stockpile Stewardship Program is carried out through the nuclear weapons complex, which includes three nuclear weapons laboratories.

<sup>4</sup>Continuity of operations focuses on restoring an organization's mission-essential functions at an alternate site and performing those functions for a short period of time before returning to normal operations. Contingency and disaster recovery planning include a broad scope of activities designed to sustain and recover critical information and information system services for a range of potential service disruptions. Contingency and disaster recovery planning components may include the relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or the performance of information system functions using alternative methods. For the purposes of this report, the term contingency and disaster recovery planning refer to the interim measures NNSA should use to recover information system services after an unexpected service disruption.

---

within the classified supercomputing environment that are a necessary means for NNSA's achievement of its nuclear weapons mission. In addition, we performed technical assessments of classified supercomputing capabilities at each weapons laboratory, including each laboratory's ability to share supercomputing capacity. Further, we obtained information from NNSA and laboratory officials to determine how expenditures were tracked for contingency and disaster recovery planning of the classified supercomputing systems at each of the laboratories, as well as projected future cost estimates for ensuring the recovery of these assets.

We conducted this performance audit from December 2009 through December 2010 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. A more detailed description of our objectives, scope, and methodology is contained in appendix I.

---

## Background

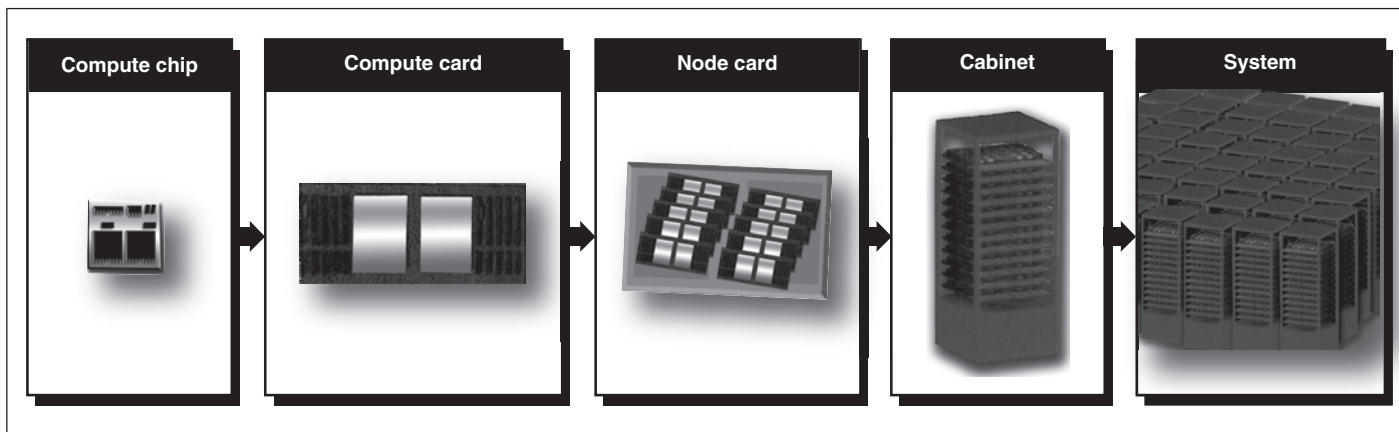
NNSA relies on its Stockpile Stewardship Program to ensure the safety, security, and effectiveness of the nuclear weapons stockpile. The Stockpile Stewardship Program is comprised of various elements, including, but not limited to: (1) the Advanced Simulation and Computing (ASC) Campaign, which provides the computational science and simulation tools to understand the behaviors and effects of nuclear weapons; (2) Directed Stockpile Work, which provides evidence of the health of the nuclear weapons stockpile and involves day-to-day maintenance of these weapons, including life extension efforts; (3) the Science Campaign, which provides tools and capabilities geared toward advancing the general understanding of all nuclear weapons systems; and (4) the Engineering Campaign, which provides a sustained basis for stockpile certification and assessments throughout the life cycle of each weapon. The coordination among the Stockpile Stewardship elements is instrumental to increasing NNSA's confidence in the performance of nuclear weapons.

To help accomplish its Stockpile Stewardship mission, NNSA relies on the three weapons laboratories—Los Alamos, Livermore, and Sandia. Los Alamos and Livermore are the two design laboratories that are responsible for designing the nuclear weapons' explosive package and conducting

research to better understand nuclear weapons phenomena. Sandia is an engineering laboratory and has principal responsibility for the research, design, and development of nonnuclear warhead components; integration of these components with Los Alamos and Livermore; and overall warhead systems integration with DOD. In accordance with NNSA, management and operations contractors, who are responsible for day-to-day operations of the laboratories, are required to adhere to agency policies.<sup>5</sup>

At the time of our review, NNSA's classified supercomputing resources consisted of 12 classified supercomputing systems. Figure 1 shows the hardware configuration of a supercomputing system.

**Figure 1: Common Hardware Components of a Supercomputing System**



Source: GAO, data provided by Los Alamos, Livermore, and Sandia.

NNSA classified supercomputing systems employ a large number of interdependent processors, which are the core unit of a computer that gathers instructions and data. These processors are mounted onto a compute chip, which is the portion of the system that carries out the instructions of a computer program. These compute chips are inserted

<sup>5</sup>Los Alamos is managed and operated by Los Alamos National Security, LLC, which is a consortium of contractors that includes Bechtel National, the University of California, the Babcock and Wilcox Company, and the Washington Division of URS. Livermore is managed and operated by Lawrence Livermore National Security, LLC, which is comprised of a corporate management team that includes Bechtel National, the University of California, the Babcock and Wilcox Company, and the Washington Division of URS. Sandia is managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation.



---

onto a compute card, which also holds memory for the compute chips to use. A number of compute cards are attached to a node card, which have one or more processors with a common memory and are connected by high-speed interconnection networks. Each node card is inserted into a single cabinet, and that configuration is repeated many times to build a single supercomputing system. Each supercomputing system has a peak performance, which is the maximum rate of floating-point operations per second (FLOPS) that the system can sustain.<sup>6</sup> Currently, almost all NNSA classified supercomputer systems operate at the teraFLOP level, which represents a trillion FLOPS.

According to NNSA, the laboratories have three types of classified supercomputing systems:

**Capacity:** Small systems that execute parallel problems with more modest computational requirements. These systems serve as the workhorse for the ASC program and are responsible for processing the day-to-day supercomputing workload.

**Capability:** This type of supercomputer is used to solve the largest and most demanding problems that other computing systems cannot manage.

**Advanced architecture:** Research and development systems that assist the ASC program in preparing to rapidly deploy and exploit the next generation of supercomputing technology. These systems have a targeted workload and serve as the foundation for the next generation of NNSA supercomputers.

Table 1 shows the classified supercomputing systems currently in use at the three weapons laboratories.

---

<sup>6</sup>FLOPS are a measure of a supercomputing system's performance. Floating-point performance is the rate at which a computer executes floating-point operations.

**Table 1: Inventory of NNSA-Deployed Classified Supercomputing Systems (as of October 2010)**

Site	System name	System type	Delivery date	Total processors	Peak performance (TeraFLOPS)
Los Alamos	Roadrunner Base	Capacity	10/2006	18,432	76.0
	Roadrunner Phase-3	Advanced architecture	9/2008	24,480	1,280.0
	Hurricane	Capacity	9/2008	5,760	51.2
Livermore	BlueGene/L	Advanced architecture	11/2004	131,072	367.0
	Purple <sup>a</sup>	Capability	6/2005	12,288	93.4
	Rhea	Capacity	9/2006	4,608	22.1
	Minos	Capacity	6/2007	6,912	33.2
	Juno	Capacity	5/2008	18,432	162.2
	Dawn	Advanced architecture	1/2009	147,456	501.4
Sandia-NM	Red Storm	Advanced architecture	3/2005	31,680	284.0
	Unity	Capacity	3/2009	4,352	38.0
Sandia-CA	Whitney	Capacity	3/2009	4,352	38.0

Source: GAO summary of data from Los Alamos National Laboratory, Lawrence Livermore National Laboratory, and Sandia National Laboratories.

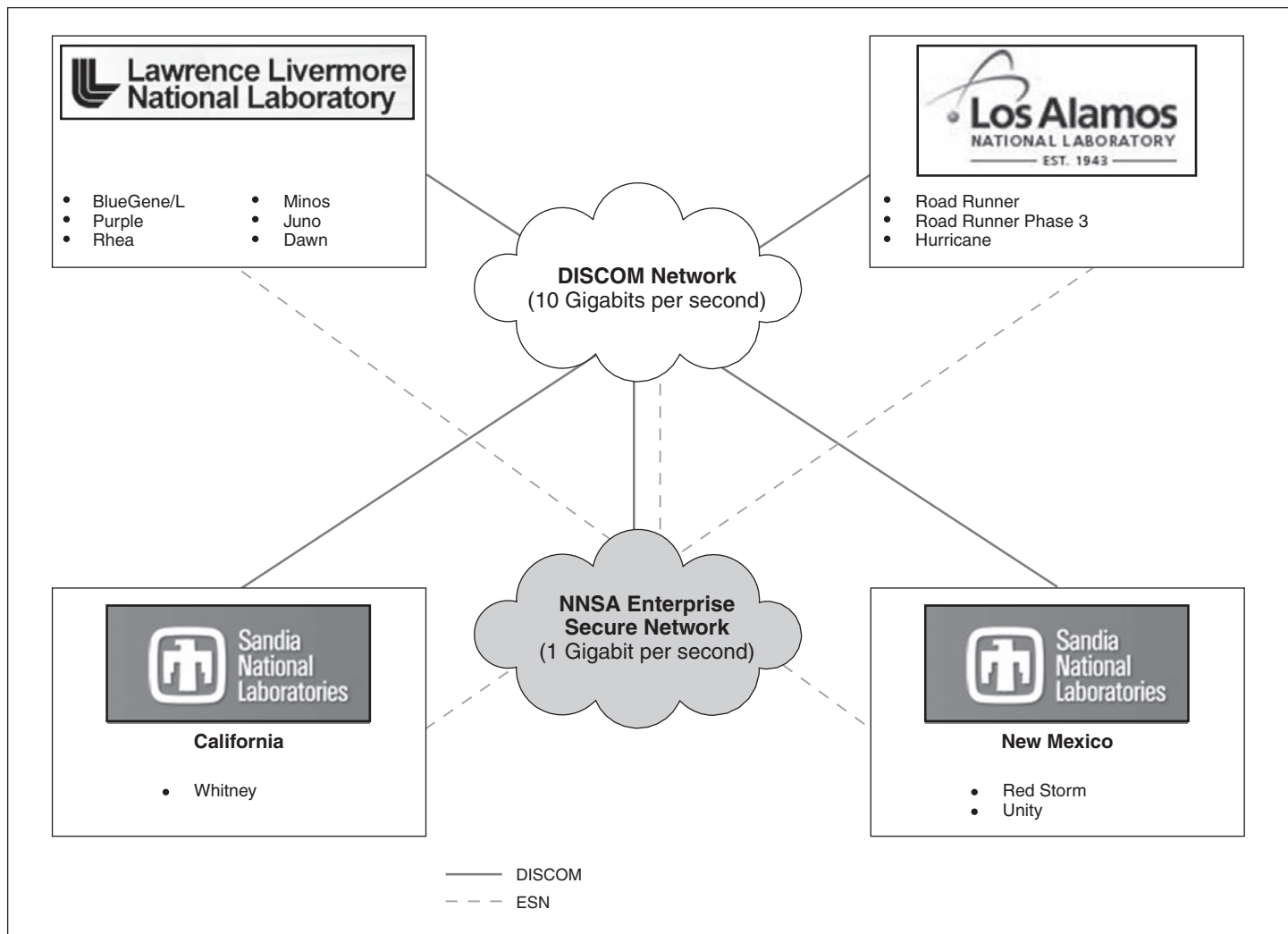
<sup>a</sup>Although Purple was the capability system in use at the time of our site visits, Livermore retired the system in November 2010.

NNSA’s classified supercomputing capabilities consist of supporting resources, including (1) parallel files systems, which store transitory data; (2) network file systems, which store user and project data for a calculation; (3) archival storage systems, which serve as storage for data; and (4) visualization systems, which enable users to better comprehend the results of their computations.

NNSA’s classified supercomputing systems are connected via its Enterprise Secure Network and the Distance Computing (DISCOM) network, which function as supporting resources for the classified supercomputing environment. The Enterprise Secure Network provides classified communications across the nuclear weapons complex, including security services and other activities that ensure the flow of NNSA’s data sharing and business missions. DISCOM provides secure, high-speed remote access for intra- and inter-site file transfers and enables users, across the three weapons laboratories, to operate on remote computing

resources as if they were local. DISCOM and the Enterprise Secure Network serve as the backup networks to each other. Figure 2 shows the composition of NNSA's classified supercomputing network infrastructure.

**Figure 2: NNSA's Classified Supercomputing Network Infrastructure**



Source: GAO, data provided by Los Alamos, Livermore, and Sandia.

---

NNSA reported obligating approximately \$1.7 billion from fiscal years 2007 through 2009 to support ASC program activities at the three weapons laboratories.<sup>7</sup> The \$1.7 billion was predominantly associated with three efforts:

**Weapons codes and models.** This effort is intended to develop and improve weapons simulation models and codes for predicting the behavior of weapons systems and devices in the nuclear stockpile.

**Computational systems and software environment.** This effort is intended to provide ASC users a stable, seamless computing environment for ASC-deployed platforms. It is responsible for procuring, delivering, and deploying ASC computational systems and user environments via technology development and integration across the three weapons laboratories.

**Facility operations and user support.** This effort is intended to provide both the necessary physical facility and operational support for reliable supercomputing and storage environments, as well as a suite of user services for effective use of the three weapons laboratories' computing resources. Facility operations cover physical space, power and other utility infrastructure, and local- and wide-area networking, as well as system administration, cyber security, and operations services for ongoing support. The user support function includes planning, development, integration and deployment, continuing product support, and quality and reliability activity collaborations.

To strengthen the security of information and information systems across the federal government, including those at NNSA's weapons laboratories, the *Federal Information Security Management Act of 2002* (FISMA) requires each agency to develop, document, and implement an agencywide information security program that supports the operations and assets of the agency, including those provided or managed by another agency or contractor on its behalf.<sup>8</sup> This security program is to include plans and procedures to ensure the continuity of operations for information systems

---

<sup>7</sup>For additional information regarding budgetary information for the classified supercomputing program from fiscal years 2007 through 2009, see appendix II.

<sup>8</sup>44 U.S.C. § 3544(b); FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

---

that support the agency's operations.<sup>9</sup> Pursuant to its FISMA responsibilities, the National Institute of Standards and Technology (NIST) has issued federal standards and guidelines on information security, such as a contingency planning guide for federal information systems, and recommended security controls, which address contingency and disaster recovery planning and testing.<sup>10</sup> To further ensure the security of national security systems, the Committee on National Security Systems (CNSS)<sup>11</sup> requires federal agencies with national security systems to implement a comprehensive set of security controls and enhancements for these systems.<sup>12</sup> CNSS requires that each agency implement a contingency and disaster recovery planning capability that ensures the integrity and availability of its national security information and information systems.<sup>13</sup>

---

<sup>9</sup>For the purposes of this report, we will refer to "continuity of operations procedures for information systems" as contingency and disaster recovery planning.

<sup>10</sup>NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems* (Washington, D.C.: June 2002) and NIST Special Publication 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* (Gaithersburg, Md.: August 2009).

<sup>11</sup>Formerly known as the National Security Telecommunications and Information Systems Security Committee, CNSS provides a forum for the discussion of policy issues, sets national policy, and provides direction, operational procedures, and guidance for the security of national security systems. DOD chairs the committee under the authorities established by National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, issued in July 1990. This directive designates the Secretary of Defense and the Director of the National Security Agency as the Executive Agent and National Manager, respectively. The committee has 21 voting representatives from various departments and agencies, including the Department of Energy.

<sup>12</sup>National security systems include any information system used or operated by an agency, or by a contractor of an agency, that processes, stores, or transmits national security information. They do not include those systems used for routine administrative and business applications.

<sup>13</sup>CNSS Instruction 1253 provides federal government departments, agencies, bureaus, and offices with a process for security categorization of national security systems that collect, generate, process, store, display, transmit, or receive national security information. In addition, this instruction serves as a companion document to NIST Special Publication 800-53, Revision 3.

---

FISMA, NIST guidelines,<sup>14</sup> and CNSS policies all call for contingency and disaster recovery planning—also referred to as continuity of operations for information systems—for critical components of information protection. DOE and NNSA policies also regard contingency and disaster recovery plans as being necessary for information protection. If normal operations are interrupted, contingency and disaster recovery plans allow senior agency officials to detect, mitigate, and recover operations. Examples of the key components that make up contingency and disaster recovery planning programs include (1) assessing the criticality and sensitivity of computerized operations and identification of supporting resources such as developing business impact analyses (BIA), (2) taking steps to prevent and minimize potential damage and interruption such as establishing data backup processes, (3) developing comprehensive contingency and disaster recovery plans,<sup>15</sup> and (4) conducting periodic testing of contingency and disaster plans.

The extent to which controls—such as contingency and disaster recovery planning—are implemented depends on a level of risk assigned to the system or information maintained on the system. NIST standards and guidelines, CNSS instructions, and NNSA policy allow consideration of risk in determining the level of protection of systems and data. These standards and policies require that organizations consider the impact or consequences of loss as it relates to the confidentiality, integrity, and availability of the information, and assign a value of low, moderate, or high impact levels. For contingency and disaster recovery planning, consideration of “availability” is the key element. NNSA policy defines the values for the consequences of loss associated with availability as follows:

**High**—Loss of life might result from loss of availability; information must always be available on request, with no tolerance for delay; loss of availability will have an adverse effect on national-level interests; federal requirement (i.e., requirement for material control and accountability)

---

<sup>14</sup>Although NIST guidelines note they shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems, CNSS instructions, as well as DOE and NNSA policies for national security systems, refer to the NIST guidelines as being applicable.

<sup>15</sup>A contingency plan is designed to maintain or restore business operations, including computer operations, possibly at an alternate location in the event of emergencies, system failures, or disaster. A disaster recovery plan is a written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

---

inventory); or loss of availability will have an adverse effect on confidentiality.

**Moderate**—Information must be readily available with minimum tolerance for delay; bodily injury might result from loss of availability; or loss of availability will have an adverse effect on organizational-level interests.

**Low**—Information must be available with flexible tolerance for delay.

---

## NNSA Has Not Fully Implemented Contingency and Disaster Recovery Planning and Testing for Its Classified Supercomputing Assets

Contingency and disaster recovery planning and testing for NNSA's classified supercomputing systems have not been fully implemented at each of the three weapons laboratories—Los Alamos, Sandia, and Livermore. Specifically, NNSA did not ensure that the laboratories (1) developed BIAs to determine the impact of potential service disruptions, (2) fully tested data backup processes, and (3) developed and tested contingency and disaster recovery plans. These shortcomings existed, at least in part, because NNSA's component organizations were unclear of 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 classified supercomputing assets at the weapons laboratories, it has limited assurance that vital information can be recovered and made available to meet national security priorities and requirements.

---

## Not All of the Laboratories Assessed the Criticality and Sensitivity of Supercomputer Operations and Resources, or Potential Outage Impact

To assess the criticality and sensitivity of computerized operations and identification of supporting resources, NIST guidelines state that agencies should determine their recovery strategies by performing business impact analyses of their systems. A BIA is an analysis of information technology system requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. NIST guidelines state that agencies conduct a BIA to identify critical information systems to fully characterize the system's requirements, processes, and interdependencies to determine contingency requirements and priorities. In addition, according to NIST guidelines, the BIA process should follow three main steps: (1) identify critical data and information technology resources, (2) identify outage

---

impacts and allowable outage times,<sup>16</sup> and (3) develop recovery priorities and strategies. NNSA policy also requires a BIA to identify systems that provide critical services to site operations and prioritize these systems and their components.

One of the laboratories—Los Alamos—had conducted a BIA that addressed its classified supercomputing systems, generally following the three steps of a BIA. However, the BIA was not always specific. For example, the laboratory identified critical information technology resources for each of its classified supercomputing systems, but did not specifically identify the critical data. Instead, Los Alamos noted that the systems are not considered mission critical nor mission essential to the business needs of the laboratory,<sup>17</sup> and that the consequence of loss for system availability is low. Additionally, it defined a specific number of days for the allowable time frames for fully and partially disabled systems, but did not provide specifics on allowable outage impacts. Further, the analyses indicated high-level recovery priorities, but did not provide specifics regarding the recovery process or strategies that would be used for recovery efforts.

The other two laboratories did not conduct BIAs specifically for classified supercomputing systems, but plan to do so. Livermore has a BIA in place for its logical assets—the applications and services that provide basic operational support to the Livermore computing environment, but the BIA did not address any of the classified supercomputing systems. However, at the time of our site visit, Livermore officials stated they were beginning the process of developing a BIA that would address their information technology needs for their classified supercomputing systems, but the process was still in the planning stage. Similarly, according to Sandia officials, the laboratory has BIAs that address its unclassified information technology systems, but does not currently have one specifically for its

---

<sup>16</sup>Outage impacts and allowable outage times enable the organization to develop and prioritize recovery strategies that personnel will implement during contingency plan activation. The effects of the outage may be tracked over time, which will enable the organization to identify the maximum allowable time that a resource may be unavailable before it inhibits the performance of an essential function. The effects of the outage can also be tracked across related resources, identifying any cascading effects that may occur as an effect of a service disruption.

<sup>17</sup>The Department of Energy defines “*mission critical*” as an information system that supports an organization’s core missions and goals, and “*mission-essential (or business essential)*” as an information system whose failure would not preclude organizations from accomplishing core business functions in the long term.



---

classified supercomputing systems. However, Sandia officials indicated that they plan to conduct a BIA for classified supercomputing systems in 2011.

Although the two laboratories have not conducted any BIAs—in line with the BIA conducted by Los Alamos—they have considered the risk of consequence of loss from availability as low impact. NNSA also considers the consequence of loss as low impact. In addition, NNSA and the three laboratories do not consider the classified supercomputers to be “mission critical.” One laboratory categorized the systems as “mission essential,” while another referred to them as “mission support elements, not mission essential elements.” However, NNSA’s mission includes maintaining the safety, security, and effectiveness of the nuclear deterrent without nuclear testing. The supercomputers provide a necessary means to determine the effects of changes to current weapons systems and to determine a level of confidence in the performance of future untested systems. The classified supercomputing capabilities serve as the computational surrogate to nuclear weapons testing and are central to national security.

Regarding recovery priorities and strategies, each of the laboratories indicated that it would likely rely on a process that is currently being used for the capability system shared among the laboratories. The laboratories generally rely on the Capability Computing Campaign to prioritize the workload and develop priorities for jobs that need to be run on the capability system.<sup>18</sup> In the event of a service disruption or emergency, laboratory officials told us that they would likely rely on the same process for all of their systems. However, this process has not been documented as a means for establishing overall recovery priorities across the laboratories.

Until all of the laboratories have a BIA in place for their classified supercomputing systems that (1) identifies and categorizes critical data, (2) identifies acceptable allowable outage impacts and time frames, and (3) establishes emergency processing priorities and strategies, the potential impact of a system outage will remain unclear.

---

<sup>18</sup>The Capability Computing Campaign includes a committee made up of staff from the NNSA ASC program office, as well as ASC executives located at the laboratories at Los Alamos, Livermore, and Sandia.

---

---

## The Laboratories Have Backup Processes in Place, but One Storage Site May Be Susceptible to Damage

Data backup processes offer a means of taking steps to prevent and minimize potential damage and interruption to computerized services. NIST guidelines, as well as CNSS instructions and NNSA policies, call for agencies to conduct backups of user-level information, system-level information, and information system documentation. In addition, NIST, CNSS, and NNSA all provide that agencies establish an alternate storage site that is separated from the primary storage site so that both are not susceptible to the same hazards. To ensure the availability of data stored in the alternate storage site, NIST and CNSS require that agencies test the backup information to verify the integrity of the data.

All of the laboratories had backup processes in place. Each of the laboratories follows similar data backup processing—both manual and automated procedures—to back up user-level information, system-level information, and information system documentation. For example, this information can include global directories, user home directories, project directories, desktop systems, and critical systems documentation. Backups occur in increments: daily incremental backups to disk, weekly full backups to tape, and monthly full-system backups to tape (with a 6-month on-site storage retention policy). The laboratories also have vendor-provided software that takes periodic snapshots of user directories for storage retention purposes. The snapshot process can be performed manually or can be set up for automatic processing. Users are encouraged to maintain their data in a shared environment on the network and are allowed to make their own determinations regarding what data should be backed up from the classified supercomputing systems.

Not all of the laboratories have an alternate storage site sufficiently separated from the primary site to not be susceptible to the same hazards. Two of the three laboratories have alternate storage sites a considerable distance from their primary storage site. Livermore sends its system backups electronically to Los Alamos every 6 months. Sandia sends its backup data to its alternate site locations (e.g, the California site sends its data to the New Mexico site and the New Mexico site sends its data to the California site). However, Los Alamos maintains its alternate storage facility on-site in a building located less than 1 mile away from the primary local backup storage facility. Consequently, both sites could be susceptible to the same hazards, such as a wildfire.

The laboratories had processes in place to verify the integrity of the backed up data. However, tests of their backup procedures rely predominantly on ad hoc recovery, rather than periodically planned tests. Los Alamos officials indicated that thousands of file recoveries have been

---

performed over the years by end users as part of their testing. Livermore officials stated that the laboratory tests its local backup procedures through actual system usage on almost a daily basis, and tests their remote backup procedures at least once annually. Further, Sandia officials told us they had successfully tested a sample of data at their offsite facility.

---

### Not All Laboratories Had Developed and Tested Contingency and Disaster Recovery Plans

NIST guidelines and CNSS policies call for the development and testing of contingency plans and the development of disaster recovery plans for each information system to ensure that, in the event of a service disruption, the work and supporting functions of the agency can continue to be performed. According to NIST guidelines, at a minimum, the contingency plan should address the identification and notification of key personnel, plan activation, system recovery, and system reconstitution to meet the needs of the agency's critical supporting operations. The guidelines also state that the plan should be tested periodically; CNSS specifies that the frequency of testing should be annually. NIST also notes that the disaster recovery plan should be designed to restore operability of the targeted system, application, or computer facility at an alternate site after a major service disruption. DOE and NNSA policies also require the development of contingency and disaster recovery plans and the testing of these plans in line with NIST and CNSS.

Each of the laboratories had developed contingency plans for their classified supercomputing systems; however, the plans were not always comprehensive, and at the time of our site visits, these plans had not been tested. The laboratories addressed disaster recovery planning to a limited extent; none specifically addressed the supercomputing environment. For example,

- Two laboratories—Los Alamos and Sandia—had contingency plans that addressed the classified supercomputing systems. Although Livermore had an information technology contingency plan and a master security plan, neither specifically addressed the supercomputers. In addition, the plans for both Los Alamos and Sandia included key components such as the identification and notification of key personnel, plan activation, system recovery, and system reconstitution procedures; however, the sufficiency of the level of detail varied. For instance, one plan provided specific details regarding system recovery processes and the notification and identification of key personnel, but provided limited details regarding plan activation and system reconstitution procedures.

- 
- At the time of our site visits, none of the laboratories had tested their contingency plans, which were less than a year old. One of the laboratories—Los Alamos—had created testing guides but had not yet conducted formal testing. Subsequent to our site visit, Los Alamos officials indicated that the first test of their plan took place in September 2010 and noted that the results would be finalized in December. Additionally, although Sandia had a contingency plan in place, the plan states that testing is not required because, in the event of a service disruption, the laboratory would either wait until the equipment was fully operational or simply acquire new equipment. This is contrary to NIST guidelines, CNSS instructions, and DOE and NNSA policies.
  - Each of the laboratories had addressed disaster recovery planning to a limited extent. For example,
    - Los Alamos included disaster recovery planning as a section within their classified supercomputing system’s contingency plans. Although it provided high-level instructions such as directing individuals to call 911 for all emergencies, it did not include information regarding the specifics for restoring operability of the classified supercomputing system at an alternate site after a major service disruption.
    - None of the plans submitted by Livermore specifically addressed the supercomputing environment, although in the disaster recovery section of the master security plan, the laboratory noted that it had no mission-essential systems in the computing environment, and systems may be offline for an extended period for system upgrades.
    - Sandia also had disaster recovery plans in place, designed for emergency preparedness and disease response planning needs for the laboratory. These plans focused on emergencies involving the facilities, operations, and activities for the laboratory, and provided individuals with emergency information should pandemics plague the laboratory. However, these plans did not include any information regarding the classified supercomputing systems.

Unless each of the laboratories develops and sufficiently tests comprehensive contingency and disaster recovery plans in accordance with applicable policies and guidance for their classified supercomputing systems, they face a risk of not being able to successfully recover their supercomputing assets and operations after a service disruption.

---

## NNSA Component Organizations Were Unclear of Their Roles and Responsibilities for Providing Oversight

The aforementioned shortcomings existed, at least in part, because NNSA's component organizations were unclear of their roles and responsibilities for providing oversight in the laboratories' implementation of contingency and disaster recovery planning. FISMA requires that the chief information officer, in coordination with other senior agency officials, manage the development and implementation of an agencywide information security program that includes plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. NIST guidelines and DOE policies call for individuals with information system or security management and oversight responsibilities to take responsibility for the development, implementation, assessment, monitoring, reviewing, and updating of security planning policies and procedures, which includes contingency and disaster recovery plans. Further, the *NNSA Safety Management Function and Responsibilities and Authorities Manual* states that the chief information officer is responsible for information technology programs and initiatives and for ensuring the security of the agency's information and systems.

Although roles and responsibilities are defined at a high level in FISMA, NIST guidelines, as well as DOE and NNSA policies, NNSA component organizations were confused about their roles in providing oversight of the laboratories' implementation of contingency and disaster recovery planning for the supercomputing systems. For example, at the beginning of our review, ASC officials told us that, although they were responsible for administering and managing the program that uses the classified supercomputing systems, they were not responsible for contingency and disaster recovery planning. Instead, they directed us to the Office of the Chief Information Officer (OCIO), where officials told us that they were not responsible for contingency and disaster recovery planning for these systems, and noted that they would only provide guidance if requested by ASC. Further, OCIO officials told us that ASC has not requested any assistance. ASC officials subsequently acknowledged that they had responsibility for contingency and disaster recovery planning; however, this organizational responsibility is contrary to NIST guidelines and DOE policies, as well as NNSA's own manual, which gives this responsibility to the OCIO. In the absence of effective oversight, the laboratories did not consistently comply with, or fully implement, federal requirements and guidance related to contingency planning and disaster recovery. Until NNSA clearly establishes and carries out defined roles and responsibilities for OCIO and ASC pertaining to contingency and disaster recovery planning for the classified supercomputing environment, it will not be able

---

to effectively manage and oversee the recovery of its supercomputing operations should service disruptions occur.

---

## The Laboratories Have the Ability to Share Supercomputing Capacity, but Barriers Exist

Technologically, the weapons laboratories have demonstrated the ability to share classified supercomputing capacity using their capacity and capability systems under normal operating conditions. Although these supercomputers process unique workloads and operate independently, they are designed with a similar operating system, resource manager, and job scheduler, which is built on a LINUX foundation. These supercomputers also include application codes that are portable across supercomputing systems and a data network, which allows authorized users local and remote access to the systems.

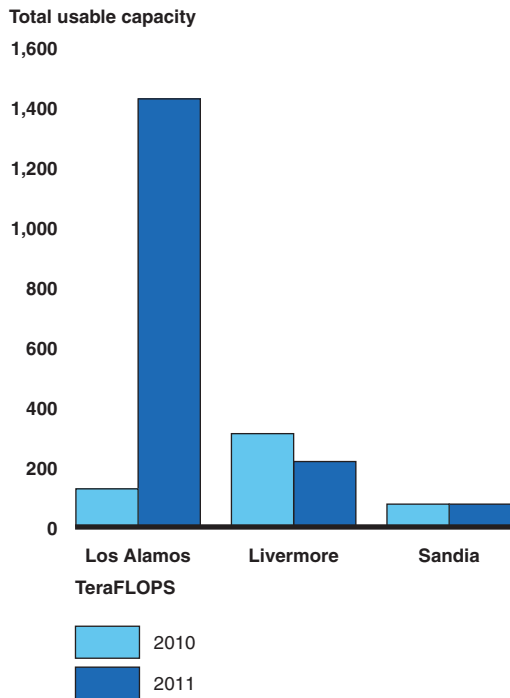
Although the weapons laboratories have the ability to share supercomputing capacity, barriers exist. One barrier to sharing supercomputing capacity is that the weapons laboratories do not know the minimum supercomputing capacity needed to achieve processing priorities in the event of a service disruption. NIST guidelines recommend, and NNSA policy requires, that capacity planning be conducted so that there is adequate capacity for information processing and supporting resources during contingency operations. Although the weapons laboratories have identified the supercomputing processing needed for normal business operations, they have not identified the minimum supercomputing capacity needed to achieve processing priorities in the event of a service disruption.

Another barrier to sharing supercomputing processing is the disparity in usable supercomputing processing across the laboratories. Figure 3 depicts this disparity by identifying the amount of total usable supercomputing capacity, in teraFLOPS, for each of the three weapons laboratories for 2010 and 2011.<sup>19</sup>

---

<sup>19</sup>Total usable supercomputing capacity includes the supercomputers that have the ability to run all weapons program codes and could be used in the event of a service disruption, and includes capacity and capability systems.

**Figure 3: Total Usable Supercomputing Capacity at Each Weapons Laboratory, 2010 and 2011**



Source: GAO analysis of supercomputing capacity data provided by Los Alamos, Livermore, and Sandia.

For example, in 2010, total usable capacity at Livermore has been 311 teraFLOPS, whereas Los Alamos and Sandia have had 127 teraFLOPS and 76 teraFLOPS, respectively. Should Livermore experience service disruptions for a sustained amount of time, neither Los Alamos nor Sandia possesses the necessary usable supercomputing capacity to accommodate the additional workload and NNSA will have to reprioritize the computational workloads across the other two laboratories. As previously noted, officials at the laboratories told us that, should disruptions occur, they would use the Capability Computing Campaign model for re-prioritizing the workload. However, this process has not been documented for recovery activities.

Further limiting the ability of the weapons laboratories to recover from a service disruption, in 2011, there will be a significant disparity in projected usable supercomputing capacity. For example, in 2011, Los Alamos' usable capacity is projected to be 1,427 teraFLOPS, whereas usable capacity at Livermore and Sandia is to be 218 teraFLOPS and 76 teraFLOPS,

---

respectively. Should Los Alamos' supercomputing systems become unavailable for an extended period of time, neither Livermore nor Sandia possesses sufficient usable supercomputing capacity to achieve its workload and accommodate the additional potential computational workload from Los Alamos. According to laboratory officials, an additional supercomputer will be deployed at Los Alamos in 2011. This supercomputer is a replacement for the single capability supercomputer currently at Livermore that was retired in 2010. Therefore, a significant amount of usable supercomputing capacity will be centralized at Los Alamos. Because the weapons laboratories have not determined the minimum supercomputing capacity requirements for their emergency processing priorities, they may not be able to meet the minimum computational workload required to meet Stockpile Stewardship milestones.

Another barrier to sharing supercomputing capacity across the weapons laboratories is that the capability to share usable capacity on an "on-demand"<sup>20</sup> basis has not been fully tested in a recovery scenario. According to officials at the laboratories, during normal operating conditions, simulation programs have run on other supercomputing systems. However, consideration has not been given to include and test these abilities in a disaster recovery scenario should a service disruption occur. As a result, NNSA has limited assurance that its disaster recovery approach would work effectively should a service disruption occur.

---

## NNSA Does Not Track the Costs for Ensuring Contingency and Disaster Recovery Planning for Its Supercomputing Assets

Although NNSA reported obligating approximately \$1.7 billion from fiscal 2007 through 2009 to implement its ASC program activities at the three weapons laboratories, the costs for ensuring the recovery of its classified supercomputing operations are unknown. Under GAO's *Standards for Internal Control in the Federal Government*, financial information should be recorded and communicated to program managers who need this information to make operational decisions and to effectively allocate resources for program activities.

NNSA officials reported obligating approximately \$390 million for facility operations and user support activities, which include the funds associated

---

<sup>20</sup>The term "on demand" is defined as the ability to move an application (simulation program/code) from one supercomputer to a different supercomputer at a different physical facility and use the existing computational resources without the need for major modifications.



---

with contingency and disaster recovery planning activities, but they were unable to provide detailed financial information for contingency and disaster recovery planning activities. According to NNSA officials, costs for contingency and disaster recovery planning for classified supercomputing systems are unknown because ASC program expenditures are part of the NNSA ASC operational budget, whose costs are tracked at an aggregate level. As a result, neither NNSA nor the three weapons laboratories can track what has been spent since fiscal year 2007 for ensuring the recovery of classified supercomputing operations and, consequently, they do not know whether funding levels for these activities have been adequate. Although certain components of contingency and disaster recovery planning are in place at the three weapons laboratories, NNSA is uncertain as to what funds were spent on these information protection activities.

Furthermore, NNSA has not developed contingency planning and disaster recovery cost estimates for its classified supercomputing assets. For fiscal years 2011 through 2014, NNSA projects that it needs about \$2.2 billion to implement its ASC activities, which support its Stockpile Stewardship program—\$984 million for weapons codes and models, \$604 million for computational systems and software environment, and \$588 million for facility operations and user support. Although NNSA has developed its out-year funding needs over the next 4 years, it has not developed estimates regarding the future costs for ensuring the recovery of its classified supercomputing assets in the event of service disruptions. Until NNSA develops a means for tracking current contingency and disaster recovery costs and for developing estimates of future costs, the agency will not have the information needed to determine whether it is meeting its goals for effective stewardship of public resources.

---

## Conclusions

All three NNSA weapons laboratories 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. For example, B IAs that identify critical resources and outage impacts have not been developed for all classified supercomputing systems and existing contingency plans at the laboratories have not been thoroughly tested. Although one laboratory's analysis is not comprehensive and the other two laboratories have not completed a BIA, NNSA and the laboratories consider the consequence of loss of availability of the classified supercomputers as a low-risk impact, and do not consider them to be mission critical. However, it is unclear

---

how NNSA made this determination given that (1) the analyses have not been completed; (2) NNSA’s mission includes maintaining the safety, security, and effectiveness of the nuclear deterrent without nuclear testing; (3) the classified supercomputing capabilities serve as the computational surrogate to underground nuclear weapons testing and are central to our national security; and (4) NNSA has obligated about \$1.7 billion over 3 fiscal years to support the Advanced Simulation and Computing program, which includes classified supercomputing activities.

Beyond the activities undertaken by the laboratories, NNSA has not developed a means for identifying, tracking, or re-prioritizing the classified supercomputing workload across the operating environment. In addition, the laboratories have not tested offsite recovery capabilities and the agency has not tested the laboratories’ ability to share “on-demand” capacity if needed or determined the minimum capacity needed to meet Stockpile Stewardship Program requirements, particularly in the event that it may need to establish emergency processing priorities. Further, although over a billion dollars have been obligated to support the classified supercomputing capabilities within the last 3 years, NNSA has not tracked the costs for ensuring the recovery of the classified supercomputing systems, data, and supporting resources should a service disruption occur. The classified supercomputing program represents a significant investment, and accountability for these systems is essential. Until NNSA clearly defines its component organizations’ roles and responsibilities and fully implements an effective contingency and disaster planning program, it has limited assurance that, in the event of a service disruption, vital information could be recovered and made available to meet national security priorities.

---

## Recommendations for Executive Action

To improve the effectiveness of contingency and disaster recovery planning for NNSA’s classified supercomputing capabilities, we recommend that the Administrator of NNSA direct the weapons laboratories to take the following four actions, where not already implemented:

- Develop business impact analyses that, among other things, (1) identify and prioritize critical systems, data, and supporting resources; (2) identify allowable outage times and impacts for classified supercomputing capabilities; and (3) identify recovery priorities and strategies.
- Develop and implement comprehensive contingency and disaster recovery plans for all classified supercomputing systems that identify how each

---

weapons laboratory's classified supercomputing capabilities will be recovered following service disruptions.

- Conduct contingency and disaster recovery plan testing.
- Test the three weapons laboratories' ability to share "on-demand" classified supercomputing capacity to ensure this capability will work in the event of unexpected service disruptions.

In addition, we recommend that the Administrator of NNSA take the following five actions:

- Document an agencywide means for reprioritizing the workload across NNSA's classified supercomputing systems should a disruption occur.
- Clearly define the oversight responsibilities of the NNSA ASC program office and the NNSA Office of the Chief Information Officer, as they relate to contingency and disaster recovery planning for NNSA's classified supercomputing operations.
- Identify, assess, and communicate the minimum classified supercomputing capacity needed to meet Stockpile Stewardship requirements in the event of a service disruption.
- Develop, document, and implement a process that identifies and tracks expenditures for contingency and disaster recovery planning for NNSA's classified supercomputing assets.
- Develop and document the total anticipated costs for contingency and disaster recovery planning of NNSA's classified supercomputing assets, which includes the replacement costs for these assets.

---

## Agency Comments and Our Evaluation

In providing written comments (reprinted in app. III) on a draft of this report, NNSA's Associate Administrator for Management and Administration agreed that improvements can be made in contingency and disaster recovery planning for supercomputing operations. He indicated that NNSA agreed with six of our nine recommendations and outlined the agency's intent to conduct business impact analyses, develop and test appropriate contingency and disaster recovery plans, document workload prioritization, and clearly define roles and responsibilities.

However, NNSA did not agree with our recommendation related to identifying the minimum capacity needed to meet Stockpile Stewardship

---

requirements in the event of a service disruption. The Associate Administrator stated that this recommendation did not take into account that the different types of supercomputers—capacity and capability—serve different functions and are procured and managed differently. In our report, we recognize that different types of supercomputers exist and that they are used for different purposes, they process unique workloads and operate independently. However, as we point out in the report, although the weapons laboratories have identified supercomputing processing needed for normal business operations, they have not identified the minimum capacity needed to achieve processing priorities in the event of a service disruption. We believe that the recommendation appropriately focuses on meeting NNSA’s Stockpile Stewardship mission and that capacity planning is essential to ensure that information processing and supporting resources exist during contingency operations, regardless of the type of system used. Although NNSA did not agree with the recommendation, the Associate Administrator stated that the agency will conduct a BIA and build appropriate contingency strategies for both types of supercomputers, as well as enhance capacity sizing actions to account for contingency and disaster recovery operations.

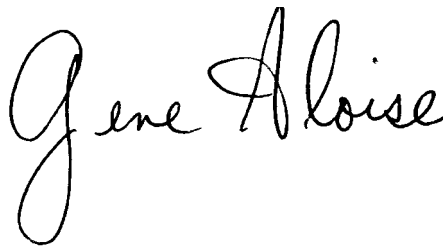
Further, NNSA did not agree with two recommendations related to identifying and tracking expenditures for contingency and disaster recovery planning and documenting anticipated recovery planning costs, including replacement costs of the assets. The Associate Administrator asserted that this information would not add significant value to managing contingency and disaster recovery planning. However, we believe such actions reflect good government practices and would add value by providing NNSA program managers with useful expenditure and cost information to aid decision making with regards to contingency and disaster recovery planning. As our report points out, GAO’s *Standards for Internal Control in the Federal Government* states that financial information should be recorded and communicated to program managers to help them make operational decisions and effectively allocate resources for program activities. Strong financial and internal controls are a major part of managing any organization because they help government program managers achieve desired results through effective stewardship of public resources. Accordingly, we believe our recommendations have merit.

---

We are sending copies of this report to the Secretary of Energy; the Administrator of NNSA; and the Directors of Los Alamos, Livermore, and Sandia laboratories. Copies of the report will also be available to others at no charge on the GAO Web site at <http://www.gao.gov>.

---

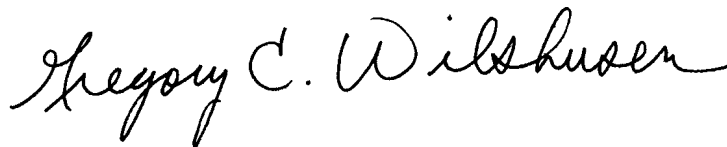
If you or your staffs have any questions about this report, please contact Gene Aloise at (202) 512-3841, or [aloise@gao.gov](mailto:aloise@gao.gov); Nabajyoti Barkakati at (202) 512-6415 or [barkakatin@gao.gov](mailto:barkakatin@gao.gov); or Gregory C. Wilshusen at (202) 512-6244 or [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are included in appendix IV.



Gene Aloise  
Director, Natural Resources and Environment



Nabajyoti Barkakoti  
Director, Center for Technology and Engineering



Gregory C. Wilshusen  
Director, Information Security Issues

---

# Appendix I: Objectives, Scope, and Methodology

---

The objectives of our review were to assess the extent to which (1) the National Nuclear Security Administration (NNSA) has implemented contingency and disaster recovery planning and testing for its classified supercomputing assets, (2) the three laboratories are able to share classified supercomputing capacity for recovery operations, should service disruptions occur, and (3) NNSA tracks the costs for ensuring contingency and disaster recovery planning for its classified supercomputing assets. To address these objectives, we focused on contingency and disaster recovery planning activities at NNSA headquarters, as well as the operating environment for the 12 classified supercomputing systems at the three weapons laboratories—Los Alamos National Laboratory, Livermore National Laboratory, and Sandia National Laboratories.

To assess the extent to which NNSA has implemented contingency and disaster recovery planning and testing for its classified supercomputing assets, we examined contingency and disaster recovery planning controls for the systems within the classified supercomputing environment that are critical to NNSA’s achievement of its nuclear weapons mission. We collected and reviewed policies, procedures, and guidelines from the National Institute of Standards and Technology, the Committee on National Security Systems, the Department of Energy, and NNSA. We also reviewed contingency plans and business impact analyses provided by the weapons laboratories and compared them to federal guidelines. We interviewed NNSA and laboratory officials to determine whether they had documented critical system, data, and supporting resources and whether contingency plans had been tested. Further, we interviewed NNSA officials to determine to what extent they have provided specific guidance and oversight for the laboratories to ensure that contingency and disaster recovery planning requirements are being met.

To determine the extent to which the three weapons laboratories have the ability to share supercomputing capacity for backup and recovery operations, we visited each weapons laboratory and gained an understanding of the overall classified supercomputing infrastructure and identified interconnectivity and control points. We performed technical assessments of supercomputing capabilities at each weapons laboratory, including each laboratory’s ability to share supercomputing capacity under normal operating conditions. We reviewed the weapons laboratories’ efforts to determine the minimal supercomputing capacity needed to meet NNSA Stockpile Stewardship Program requirements along with the ability of the weapons laboratories to share supercomputing capacity on an “on-demand” basis, including the use of advanced architecture systems. In

addition, we obtained documents describing the supercomputing system environment as well as capacity information, along with the views of officials from NNSA and the three weapons laboratories.

To assess the extent to which NNSA tracks costs for ensuring contingency and disaster recovery planning for classified supercomputing assets, we interviewed NNSA and weapons laboratory officials to determine how expenditures were tracked for contingency and disaster recovery planning of the classified supercomputing systems at each of the laboratories. We also requested the amount of funds NNSA obligated to the three weapons laboratories, and the amount of funds the laboratories spent, in implementing NNSA's classified supercomputing capabilities from fiscal years 2007 through 2009. Further, we interviewed NNSA and laboratory officials to determine how they projected future cost estimates for ensuring the recovery of these assets for fiscal years 2011 through 2014. To assess the reliability of data provided, we reviewed (1) the fiscal year 2009 financial statement audit for the system and (2) responses NNSA provided to questions about processes and procedures for ensuring the accuracy and completeness of data. Based on this information, we determined the data are sufficiently reliable for the purposes of this report.

We conducted this performance audit from December 2009 through December 2010 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.

---

# Appendix II: NNSA Annual Obligations for Its Advanced Simulation and Computing Program, Fiscal Years 2007 through 2009

---

NNSA reported obligating approximately \$1.7 billion from fiscal years 2007 through 2009 to support Advanced Simulation and Computing (ASC) program activities at the three weapons laboratories. The \$1.7 billion was used mainly for three efforts:

**Weapons codes and models.** This effort is intended to develop and improve weapons simulation codes and models for predicting the behavior of weapons systems and devices in the nuclear stockpile.

**Computational systems and software environment.** This effort is intended to provide ASC users a stable, seamless computing environment for ASC-deployed platforms. It is responsible for procuring, delivering, and deploying ASC computational systems and user environments via technology development and integration across the three weapons laboratories.

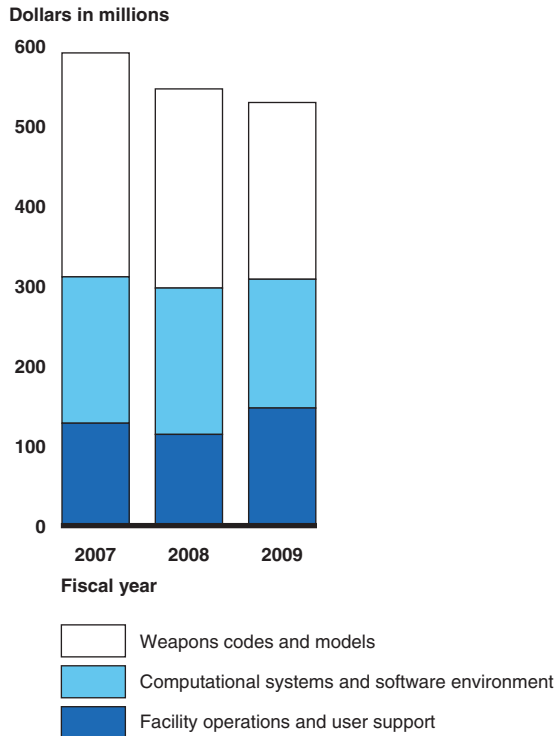
**Facility operations and user support.** This effort is intended to provide both the necessary physical facility and operational support for reliable supercomputing and storage environments, as well as a suite of user services for effective use of the three weapons laboratories' computing resources. Facility operations cover physical space, power and other utility infrastructure, and local- and wide-area networking, as well as system administration, cyber security, and operations services for ongoing support. The user support function includes planning, development, integration and deployment, continuing product support, and quality and reliability activity collaborations.

Figure 4 depicts NNSA's annual obligations for each of the three efforts from fiscal years 2007 through 2009.



**Appendix II: NNSA Annual Obligations for Its  
Advanced Simulation and Computing  
Program, Fiscal Years 2007 through 2009**

**Figure 4: Annual Obligations for NNSA's Advanced Simulation and Computing Program, Fiscal Years 2007 through 2009**



Source: GAO analysis of data provided by NNSA.

As shown in figure 4, NNSA annual obligations for its classified supercomputing operations decreased from about \$591 million to \$529 million between fiscal years 2007 and 2009. The largest obligation for the classified supercomputing program was for weapons codes and models, which accounted for approximately \$750 million (or 45 percent) of total obligations.

Obligations for computational systems and software environment accounted for approximately \$527 million (or 32 percent) of total obligations. For the period, obligations for this effort decreased from \$183 million to \$161 million.

The facility operations and user support activities, which includes, among other things, expenditures for contingency and disaster recovery planning, accounted for \$390 million (or 23 percent) of total obligations over the

---

**Appendix II: NNSA Annual Obligations for Its  
Advanced Simulation and Computing  
Program, Fiscal Years 2007 through 2009**

---

period. These obligations ranged from \$114 million to \$147 million for the 3 fiscal years.

# Appendix III: Comments from the National Nuclear Security Administration



Department of Energy  
National Nuclear Security Administration  
Washington, DC 20585



November 23, 2010

Mr. Gregory C. Wilshusen  
Director  
Information Security Issues  
U.S. Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

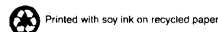
Dear Mr. Wilshusen:

The National Nuclear Security Administration (NNSA) appreciates the opportunity to review the Government Accountability Office's (GAO) draft report, GAO-11-67, *INFORMATION SECURITY: National Nuclear Security Administration Needs to Improve Contingency Planning for Its Classified Supercomputing Operations*. I understand the House Committee on Energy and Commerce requested GAO to assess various aspects of NNSA's Continuity of Operations Program to ensure that, in case of service disruptions, the three weapons laboratories can maintain the computer simulation capabilities needed to meet nuclear weapons assessment and certification requirements. Specifically, GAO identified, (1) whether NNSA has Continuity of Operations planning and testing procedures in place across the classified supercomputing environment of the three weapons laboratories; (2) whether the weapons laboratories are able to share capacity for backup and recovery operations; and (3) the past, present and future resources needed to maintain supercomputing capabilities.

We are pleased that GAO recognizes the importance of the simulation capabilities of NNSA's supercomputers to address stockpile stewardship and other national security matters. While the draft report implies, without explicitly stating, that the timeframe for reconstitution of supercomputing assets should be similar to that required for Continuity of Operations for national command and control, major financial systems, and health and emergency services, that time urgency is not consistent with existing policies for the recovery of research and development capabilities, nor should it be. Nevertheless, we agree that improvements can be made in contingency and disaster recovery planning for supercomputing operations.

After careful review, additional time is required to establish further plans and schedule solutions for addressing the GAO's recommendations. NNSA will provide a more detailed response to the recommendations when the final report is issued. However, we are providing a summary of responses to the recommendations presented in the draft report.

**Recommendation 1:** *Develop business impact analyses that, among other things, (1) identify and prioritize critical systems, data, and supporting resources, (2) identify allowable outage times and impacts for classified supercomputing capabilities, and (3) identify recovery priorities and strategies.*



**Concur:** NNSA will leverage current Business Impact Analysis (BIA) activities underway at Lawrence Livermore National Laboratory, Los Alamos National Laboratory, and Sandia National Laboratories and perform a national level BIA to provide a consistent assessment across the laboratories for classified supercomputing.

**Recommendation 2:** *Develop and implement comprehensive contingency and disaster recovery plans for all classified supercomputing systems that identify how each weapons laboratory's classified supercomputing capabilities will be recovered following service disruptions.*

**Concur:** NNSA will develop appropriate plans based on the assessment results of the BIA performed per the GAO's first recommendation.

**Recommendation 3:** *Conduct contingency plan testing.*

**Concur:** NNSA will conduct contingency plan testing according to contingency and disaster recovery plans to be implemented based on the assessment results of the BIA performed per the GAO's first recommendation.

**Recommendation 4:** *Classified supercomputing capacity to ensure this capability will work in the event of unexpected service disruptions.*

**Concur:** NNSA will test the three weapons laboratories' ability to share classified capacity supercomputers according to contingency and disaster recovery plans to be implemented based on the assessment results of the BIA.

**Recommendation 5:** *Document an agency-wide means for reprioritizing the workload across NNSA's classified supercomputing systems should a disruption occur.*

**Concur:** The NNSA will adapt, apply and exercise procedures that are routinely being used for prioritizing workload in capability computing campaigns for use in contingencies and disasters.

**Recommendation 6:** *Clearly define the oversight responsibilities of the NNSA ASC program office and the NNSA Office of the Chief Information Officer, as they relate to contingency and disaster recovery planning for NNSA's classified supercomputing operations.*

**Concur:** In general, the NNSA Office of the Chief Information Officer provides policy and guidance and the Office of Advanced Simulation and Computing (ASC) has responsibilities for execution. Oversight responsibilities will be clearly defined through the BIA and development and implementation of the contingency and disaster recovery plans.

**Recommendation 7:** *Identify, assess, and communicate the minimum classified supercomputing capacity needed to meet Stockpile Stewardship requirements in the event of a service disruption.*

**Nonconcur:** This recommendation does not take into account that capacity and capability systems serve different functions under different cost of ownership models, and consequently are procured and managed differently. The ASC program has deployed its supercomputing assets to mitigate single site failures. For the future, the program will enhance capacity sizing actions to account for contingency and disaster recovery operations when planning host sites for capacity computing capabilities. We will conduct a BIA assessment recognizing the differences and build appropriate contingency strategies for both classes of computing.

**Recommendation 8:** *Develop, document, and implement a process that identifies and tracks expenditures for contingency and disaster recovery planning for NNSA's classified supercomputing assets.*

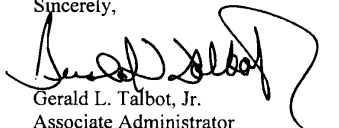
**Nonconcur:** Almost all classified supercomputing contingency and disaster recovery planning leverages computing resources and activities funded as part of a production simulation environment for weapons designers and engineers. These expenses are integral to ASC's Facility Operations and User Support Program element and tracking them separately would not add significant value to managing contingency and disaster recovery.

**Recommendation 9:** *Develop and document the total anticipated costs for contingency and disaster recovery planning of NNSA's classified supercomputing assets, which includes the replacement costs for these assets.*

**Nonconcur:** As stated in the response to Recommendation 8, these expenses are integral to ASC's Facility Operations and User Support program element and tracking them separately would not add significant value to managing contingency and disaster recovery.

If you have any questions related to this response, please contact JoAnne Parker, Director, Office of Internal Controls, at 202-586-1913.

Sincerely,



Gerald L. Talbot, Jr.  
Associate Administrator  
for Management and Administration

cc: Acting Chief Information Officer  
Deputy Administrator for Defense Programs

---

# Appendix IV: GAO Contacts and Staff Acknowledgments

---

## GAO Contacts

Gene Aloise (202) 512-3841 or [aloisee@gao.gov](mailto:aloisee@gao.gov)  
Nabajyoti Barkakati (202) 512-6415 or [barkakatin@gao.gov](mailto:barkakatin@gao.gov)  
Gregory C. Wilshusen (202) 512-6244 or [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov)

---

## Staff Acknowledgments

In addition to the individuals named above, Glen Levis, Edward M. Glagola, Jr., and Jeffrey Knott (Assistant Directors); and Preston S. Heard, Jennifer R. Franks, Kevin Metcalfe, and Zsaroq Powe were key contributors to this report. Neil Doherty, Nancy Glover, Franklin Jackson, and Jonathan Kucskar also made key 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](http://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](http://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](http://www.gao.gov/fraudnet/fraudnet.htm)

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Ralph Dawn, Managing Director, [dawnr@gao.gov](mailto: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](mailto:youngc1@gao.gov), (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, DC 20548

