



May 2014

# NUCLEAR SECURITY

## NNSA Should Establish a Clear Vision and Path Forward for Its Security Program

# GAO Highlights

Highlights of [GAO-14-208](#), a report to congressional requesters

## Why GAO Did This Study

NNSA, a semiautonomous agency in DOE, is responsible for protecting sensitive assets, including classified information and plutonium used at its contractor-operated sites to carry out nuclear weapons-related missions. Contractors provide security at NNSA's sites under the direction and oversight of DNS, NNSA field offices, and DOE. In response to rising security costs and other concerns, from 2009 to 2012, DOE and NNSA initiated various reforms to identify and eliminate potentially unnecessary security costs; realign security requirements that may be impeding sites' productivity; and streamline federal oversight. After a serious security breach at its Y-12 site in July 2012, however, NNSA reexamined some of its reforms and considered additional actions.

GAO was asked to examine NNSA's security reforms. GAO examined (1) DOE, NNSA, and contractors' implementation of the 2009 to 2012 security reforms, including any benefits or drawbacks they identified for NNSA and its sites, and (2) NNSA's actions or plans to improve security performance and oversight after the Y-12 security breach. GAO reviewed DOE and NNSA documents and interviewed DOE and NNSA headquarters officials and NNSA field office officials and contractors at the seven NNSA sites.

## What GAO Recommends

GAO recommends NNSA develop a clear vision and path forward for its security program and an implementation strategy including regular monitoring. NNSA agreed with the recommendation.

View [GAO-14-208](#). For more information, contact David C. Trimble at (202) 512-3841 or [trimbled@gao.gov](mailto:trimbled@gao.gov).

May 2014

## NUCLEAR SECURITY

### NNSA Should Establish a Clear Vision and Path Forward for Its Security Program

## What GAO Found

Implementation of security reforms from 2009 to 2012 generally varied among National Nuclear Security Administration (NNSA) sites. According to Department of Energy (DOE) and NNSA officials and contractors, some of these efforts helped manage security costs and enhance productivity, among other benefits, but may also have increased security risks and reduced security performance at the Y-12 National Security Complex (Y-12) in Tennessee and other NNSA sites, depending on how the sites implemented the reforms. For example, NNSA's headquarters Office of Defense Nuclear Security (DNS) conducted in-depth reviews at sites and recommended elimination of certain expenditures, for a potential savings of \$53 million. However, not all of these cuts were implemented by the sites, and NNSA has limited quantifiable data on the benefits of these or other actions. NNSA officials and contractors at several sites also noted that some recommendations made during the reviews may have encouraged inappropriate risks by, for example, calling for cuts in what some of the officials or contractors described as critical protective force posts and patrols. Other actions to implement the reforms may also have increased risks, particularly at Y-12. Specifically, NNSA issued its own security policies in place of DOE's security directives, giving NNSA's contractors greater authority to make security decisions and accept risks. At the same time, DOE and NNSA scaled back on their security inspections and increased their reliance on contractors to self-monitor and self-evaluate their security performance at NNSA sites. Particularly at Y-12, some of these actions to implement the 2009 to 2012 reforms may have increased risks and reduced security performance. Some of the actions at Y-12 to implement the reforms were also later identified by DOE and NNSA as being among the causes of that site's July 2012 security breach.

After the Y-12 security breach, NNSA took a number of actions designed to improve its security performance and oversight but did so without first developing a clear vision and path forward for its security program and an implementation strategy, including milestones and responsibilities for carrying them out. For example, NNSA initiated actions to reinstate the DOE security directives, which it had previously replaced with its own security policies; started, then discontinued, a security inspection program; and reorganized its headquarters security office twice. According to some DOE and NNSA officials, NNSA undertook these and other actions without first developing the NNSA security "road map" that its Security Task Force had called for in 2012, as a priority recommendation after the Y-12 breach. More specifically, the task force had recommended that NNSA develop a clear vision and path forward for its security program and an implementation strategy, including regular monitoring, to help ensure that its actions will lead to sustainable solutions—a recommendation that mirrors effective practices GAO has previously identified for successfully implementing and sustaining management improvement initiatives. Without a road map for its security program, NNSA may prolong what some of its own officials have described as a "chaotic" or "dysfunctional" period in NNSA's security program since the 2012 security breach. In addition, NNSA risks putting in place short-lived or ineffective responses to its security problems, on which GAO and others have reported for more than a decade.

---

# Contents

---

|              |  |    |
|--------------|--|----|
| Letter       |  | 1  |
|              | Background   | 6  |
|              | Reforms May Have Helped Manage NNSA's Security Costs and Enhance Its Productivity but May Have Increased Risks at Some Sites | 11 |
|              | NNSA Initiated Actions to Improve Security Performance and Oversight but Has Not Developed a Clear Path Forward              | 24 |
|              | Conclusions  | 29 |
|              | Recommendation for Executive Action  | 30 |
|              | Agency Comments and Our Evaluation   | 30 |
| Appendix I   | Key Changes from DOE Security Directives in NNSA's 2010 Policy Letters   | 33 |
| Appendix II  | Comments from the National Nuclear Security Administration   | 35 |
| Appendix III | GAO Contact and Staff Acknowledgments  | 36 |
| Table        |  |    |
|              | Table 1: Key Changes from DOE Security Directives to the Security-Related Policy Letters NNSA Issued in 2010                 | 34 |
| Figures      |  |    |
|              | Figure 1: Selected Mission Activities of Seven National Nuclear Security Administration Sites                                | 7  |
|              | Figure 2: National Nuclear Security Administration's (NNSA) Physical Security Budget, Fiscal Years 2001 through 2014         | 9  |

---

---

## Abbreviations

|      |  |
|------|--|
| DNS  | Office of Defense Nuclear Security       |
| DOD  | Department of Defense                    |
| DOE  | Department of Energy                     |
| HSS  | Office of Health, Safety and Security    |
| M&O  | management and operating                 |
| NNSA | National Nuclear Security Administration |
| SNM  | special nuclear material                 |
| Y-12 | Y-12 National Security Complex           |

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.



May 30, 2014

### Congressional Requesters

The National Nuclear Security Administration (NNSA) is responsible for protecting classified information and special nuclear material primarily used to ensure the safety and reliability of the nation's nuclear weapons stockpile without underground nuclear testing. A successful attempt by terrorists or others to steal, sabotage, or otherwise gain unauthorized access to classified information or special nuclear material—including plutonium and highly enriched uranium—could harm national security.<sup>1</sup> Congress created NNSA in 1999 as a semiautonomous agency within the Department of Energy (DOE) to, among other things, take responsibility for strategic management and safeguards and security at government-owned sites where nuclear stockpile management and nonproliferation missions are carried out.<sup>2</sup> NNSA manages these missions at seven sites, which include three research and development laboratories and four nuclear production and testing sites.<sup>3</sup> However, day-to-day mission-related tasks, such as analyzing weapons in the nuclear stockpile or refurbishing weapons to extend their operational lives, are largely performed by contractors at the sites. Contractors also provide on-site security, including hiring, training, and equipping the sites' protective forces and providing personnel to evaluate security risks and to operate and maintain the cameras, alarms, fences, and other security features. Contractors' activities to secure NNSA's sites are governed by federal legal requirements and by DOE policies, under the direction and oversight of NNSA headquarters and field offices. Also, DOE's Office of Health, Safety and Security (HSS) has traditionally established DOE's nuclear

---

<sup>1</sup>Special nuclear material is material that can be used for nuclear weapons. Such material includes plutonium or uranium enriched in the isotope 233 or in the isotope 235.

<sup>2</sup>See National Nuclear Security Administration Act, Pub. L. No. 106-65, Tit. XXXII, 113 Stat. 512, 953 (1999).

<sup>3</sup>In addition to these seven sites, NNSA also conducts some mission work at facilities at DOE's Savannah River Site in South Carolina. We did not include the Savannah River Site in our review, because that site is primarily overseen by DOE's Office of Environmental Management and has had a more limited role in NNSA's security reforms than the NNSA sites.

---

safety and security policies and conducted independent oversight of safety and security at DOE and NNSA sites.<sup>4</sup>

Since its establishment, NNSA has taken various steps to improve its security program and manage security risks at its sites, including organizing an Office of Defense Nuclear Security at NNSA headquarters to coordinate security across NNSA and consolidating sites' dangerous nuclear materials into fewer locations needing high-level security protection. After the terrorist attacks of September 11, 2001, DOE put in place more demanding requirements for contractors to provide security for DOE and NNSA sites with special nuclear material, necessitating major investments by DOE and NNSA to upgrade the sites' security infrastructure and to increase the size and capability of the sites' protective forces.

However, NNSA's creation has not yet had the desired effect of fully resolving long-standing security management and oversight problems. We have frequently reported on security incidents at NNSA sites,<sup>5</sup> including incidents that contributed to the temporary stand-down of operations at Los Alamos and Lawrence Livermore National Laboratories in 2004 and 2005, as well as initiatives by contractors at these sites to help address the problems.<sup>6</sup> At the same time, some officials and contractors at DOE and NNSA as well as in the Department of Defense—which manages the nuclear stockpile along with DOE and NNSA—the National Research Council, and other organizations, raised concerns that requirements placed on DOE's and NNSA's contractors were, in their view, overly prescriptive and burdensome, and that oversight of contractors' activities at DOE and NNSA sites had become excessive. In particular, the officials were concerned that what they saw as overly burdensome nuclear safety and security requirements and excessive

---

<sup>4</sup>As part of an ongoing reorganization in DOE, the Secretary and Deputy Secretaries of Energy announced in February 2014 that these policy-setting and independent oversight functions would be removed from HSS and placed within new organizations in the department.

<sup>5</sup>See, for example, GAO, *Modernizing the Nuclear Security Enterprise: Observations on DOE's and NNSA's Efforts to Enhance Oversight of Security, Safety, and Project and Contract Management*, [GAO-13-482T](#) (Washington, D.C.: Mar. 13, 2013).

<sup>6</sup>See GAO, *Stand-Down of Los Alamos National Laboratory: Total Costs Uncertain; Almost All Mission-Critical Programs Were Affected but Have Recovered*, [GAO-06-83](#) (Washington, D.C.: Nov. 18, 2005).

---

oversight were lowering the productivity and quality of work performed at NNSA's sites. The officials were also concerned that burdensome requirements and excessive oversight could be contributing to increases in NNSA's security budget, which—in the area of physical security—had roughly doubled from around \$360 million in fiscal year 2001 to a peak of \$728 million in fiscal year 2008, before declining somewhat in fiscal years 2009 to 2014.<sup>7</sup>

In response to these concerns, DOE and NNSA separately undertook various and sometimes parallel reforms from 2009 to 2012. At the request of the Deputy Secretary of Energy, in 2009, HSS began revising DOE's safety and security policies and oversight approach and, in 2010, and 2011, DOE issued new policy directives on safety, security, and oversight at DOE and NNSA sites.<sup>8</sup> Also, in 2009, at the request of the NNSA Administrator, NNSA began a "governance transformation" project to reengineer and unify business practices and oversight across NNSA to improve collaboration with its contractors and achieve greater cost-effectiveness in carrying out and supporting NNSA's missions. Consistent with this effort, NNSA also initiated a Zero-Based Security Review in 2009—a comprehensive reexamination of NNSA's physical security program, involving various changes in NNSA policies and processes for conducting security at its sites. The NNSA review was largely directed by the Office of Defense Nuclear Security and carried out by that office and by the contractors responsible for securing NNSA's sites.<sup>9</sup>

---

<sup>7</sup>According to HSS and NNSA officials, measures to address security vulnerabilities identified after the terrorist attacks of September 11, 2001, accounted for much of this increase.

Physical security costs have included budgeted costs for NNSA's protective forces; sensors, alarms, barriers, and related physical security systems; control and accountability of nuclear materials and classified information; processes to screen personnel's eligibility to access classified information or nuclear material; and security program management. Physical security budgets have sometimes also included costs for security upgrades to comply with DOE threat policies, or other such costs. Generally not included in NNSA's physical security budget are other notable security costs, such as those for cyber security, security-related construction projects, and secure transportation of nuclear materials between sites. NNSA has included such costs elsewhere in its budget.

<sup>8</sup>We previously reported on the nuclear safety reforms under this effort. See GAO, *Nuclear Safety: DOE Needs to Determine the Costs and Benefits of Its Safety Reform Effort*, [GAO-12-347](#) (Washington, D.C.: Apr. 20, 2012).

<sup>9</sup>NNSA, Office of Defense Nuclear Security, *Defense Nuclear Security Project Execution Plan, Zero-Based Security Review* (Aug. 9, 2010).

---

Collectively, these various DOE and NNSA reforms had the following goals, concerning NNSA security:

- to identify and eliminate potentially unnecessary security costs;
- to improve efficiency by realigning security requirements that may be impeding NNSA sites' productivity; and
- to streamline federal oversight to be less intrusive, while ensuring appropriate monitoring and evaluation of contractors' security performance by DOE and NNSA.

While these reforms were being implemented, a serious security breach occurred in July 2012 at the Y-12 National Security Complex (Y-12) in Tennessee, in which three trespassers gained access to the protected area directly adjacent to one of the nation's most critically important nuclear weapon-related facilities before being interrupted by the security measures in place. This breach led to a 2-week stand-down of that site's operations. According to DOE's Inspector General, the security breach was unprecedented and represented multiple system failures, including failures to maintain critical security equipment, respond properly to alarms, and understand security protocols.<sup>10</sup>

After the July 2012 security breach at Y-12, DOE's Inspector General, HSS, NNSA, and others investigated the causes, and immediate actions were taken to improve Y-12's security and assess whether conditions leading to the security breach were present at other NNSA sites. In addition, study groups, such as a 2012 NNSA Security Task Force convened by the NNSA Administrator in the wake of the Y-12 security breach, identified longer-term goals and recommendations to improve NNSA's security performance and oversight. Partly as a result of these reviews—and as discussed later in this report—NNSA halted, reversed, or modified some of the security reforms initiated in 2009 to 2012.

You asked us in 2010 to review the department's safety and security reforms. We reported on DOE's and NNSA's safety reforms in an April 2012 report.<sup>11</sup> This review focuses on the second part of your request on

---

<sup>10</sup>DOE, Office of Inspector General, *Inquiry into the Security Breach at the National Nuclear Security Administration's Y-12 National Security Complex*, DOE/IG-0868 (August 2012).

<sup>11</sup>[GAO-12-347](#).



---

NNSA's security. We examined (1) DOE, NNSA, and contractors' implementation of the 2009 to 2012 security reforms, including benefits or drawbacks, if any, that they identified for NNSA and its sites and (2) the extent to which DOE and NNSA have taken actions or developed plans to improve NNSA's security performance and oversight after the Y-12 security breach.

To conduct this work, we reviewed DOE and NNSA security policies and documentation of DOE and NNSA security reforms implemented since 2009 and interviewed DOE and NNSA officials and contractors responsible for managing or overseeing security at NNSA sites. Specifically, to help us understand DOE, NNSA, and contractors' implementation of the 2009 to 2012 security reforms, including key benefits or drawbacks they identified for NNSA and its sites, we reviewed reform implementation plans, security policies, and other documents from NNSA's Zero-Based Security Review and related reforms. We also interviewed NNSA headquarters officials from the Office of Defense Nuclear Security and HSS officials from the Offices of Security and of Enforcement and Oversight. We visited a nonprobability sample of three of the seven NNSA sites, selected to reflect a mix of NNSA's research and development laboratories and production and testing sites. The three sites we visited were Lawrence Livermore National Laboratory in California, the Nevada National Security Site, and the Pantex Plant in Texas. We contacted by telephone the four other NNSA sites: the Kansas City Plant in Missouri; the Los Alamos and Sandia National Laboratories in New Mexico; and Y-12. For all seven sites, we interviewed NNSA officials and contractors responsible for overseeing or carrying out security at the sites. We also reviewed cost analyses, reports, or other documents obtained from the NNSA officials and contractors on sites' implementation of the security reforms and associated benefits or drawbacks. To review the extent to which DOE and NNSA have taken actions or developed plans to improve NNSA's security performance and oversight after the Y-12 security breach, we examined reports from reviews by the DOE Inspector General, HSS, the NNSA Security Task Force, and others, conducted after the Y-12 security breach. We also interviewed headquarters officials from HSS and NNSA, as well as NNSA field office officials and contractors.

We conducted this performance audit from September 2012 to May 2014 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that

---

the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

---

## Background

During the late 1990s, DOE experienced problems at the nation's nuclear weapons laboratories, including significant cost overruns on major projects and security incidents. According to a June 1999 report by the President's Foreign Intelligence Advisory Board, DOE's management of its nuclear weapons laboratories, while representing "science at its best," also embodied "security at its worst," because of "organizational disarray, managerial neglect, and a culture of arrogance." The advisory board urged Congress to create a new organization that, whether established as an independent agency or a semiautonomous agency within DOE, would have a clear mission, streamlined bureaucracy, and drastically simplified lines of authority and accountability. Subsequently, Congress created NNSA under Title 32 of the National Defense Authorization Act for Fiscal Year 2000—the NNSA Act.<sup>12</sup> The NNSA Act established the position of DOE Under Secretary for Nuclear Security, who was also designated as the Administrator for NNSA. Under the act, the Secretary and Deputy Secretary of Energy may establish policy for, and give direction to, the Administrator. DOE directives remain the primary means to establish, communicate, and institutionalize policies, requirements, and procedures for multiple departmental elements, including NNSA. However, the act also gives the NNSA Administrator the authority to establish NNSA-specific policies, unless disapproved by the Secretary of Energy. NNSA does so through the issuance of Policy Letters.<sup>13</sup> The act further established the Office of Defense Nuclear Security, headed by the Chief of Defense Nuclear Security, who reports to the NNSA Administrator but has direct access to the Secretary of Energy on security matters.

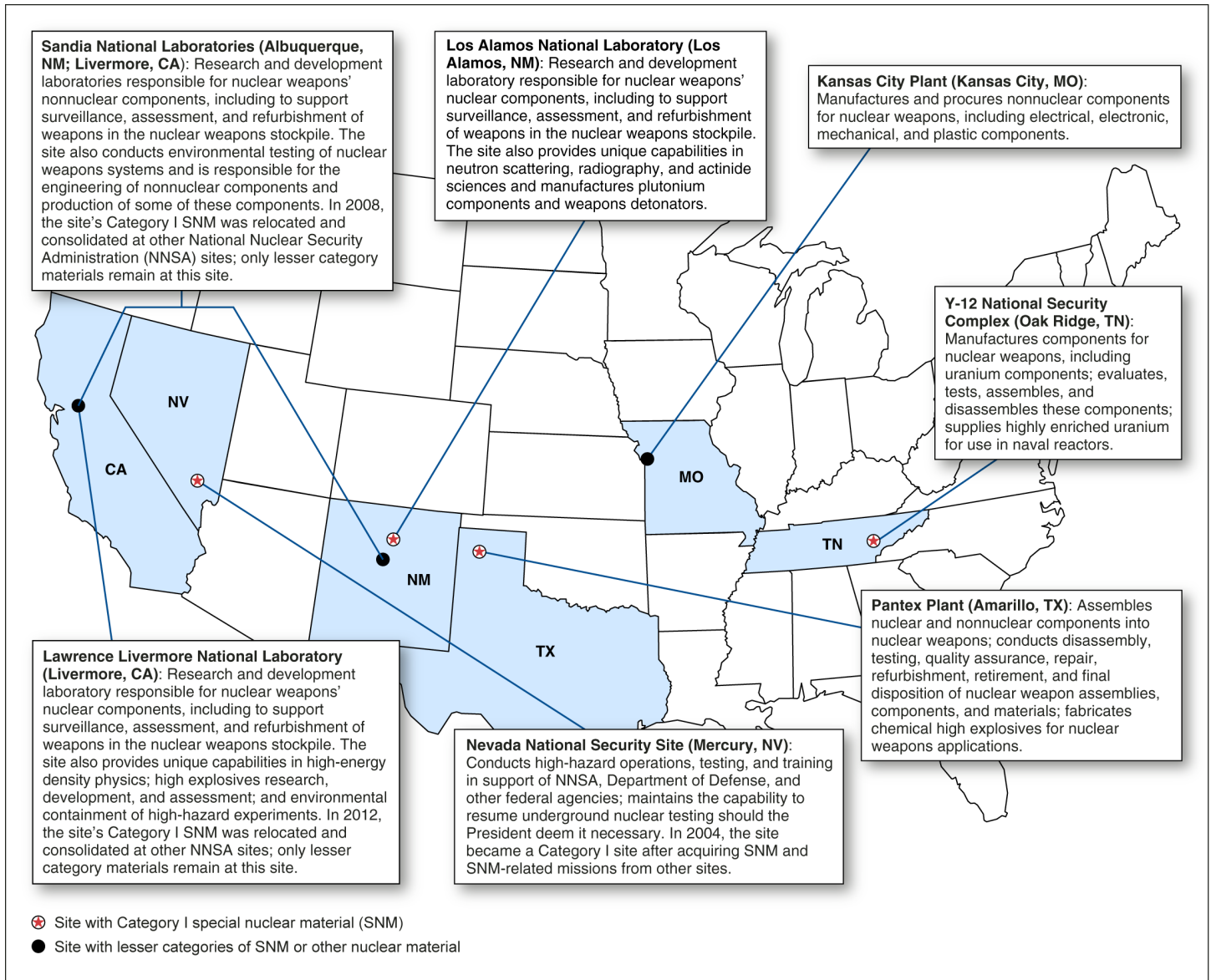
To carry out NNSA's missions, contractors at the seven NNSA sites work in the many research, manufacturing, testing, or other facilities located at those sites. At four of the sites, there are facilities used to process and store Category I special nuclear material, which receives the highest levels of security protection (see fig. 1 for an overview of the activities conducted at the seven NNSA sites).

---

<sup>12</sup>Pub. L. No. 106-65, Tit. XXXII, 113 Stat. 512, 953 (1999).

<sup>13</sup>NNSA, *Policy Letters: NNSA Policies, Supplemental Directives, and Business Operating Procedures*, NA SD 251.1 (Washington, D.C.: July 5, 2011).

**Figure 1: Selected Mission Activities of Seven National Nuclear Security Administration Sites**



Sources: NNSA; Map Resources (map). | GAO-14-208

Note: Special nuclear material (SNM) is material that can be used for nuclear weapons. SNM includes plutonium or uranium enriched in the isotope 233 or in the isotope 235. As defined in DOE policy, Category I denotes significant, specified quantities and forms of SNM. The risks associated with Category I SNM vary but may include nuclear detonation of a weapon, test device, or improvised nuclear device, capable of producing a nuclear yield, among other risks. Lesser quantities of SNM—Category II, III, and IV quantities—are not, by themselves, capable of producing a nuclear yield but must be secured to prevent theft for use in radioactive dispersal or to accumulate Category I quantities.

---

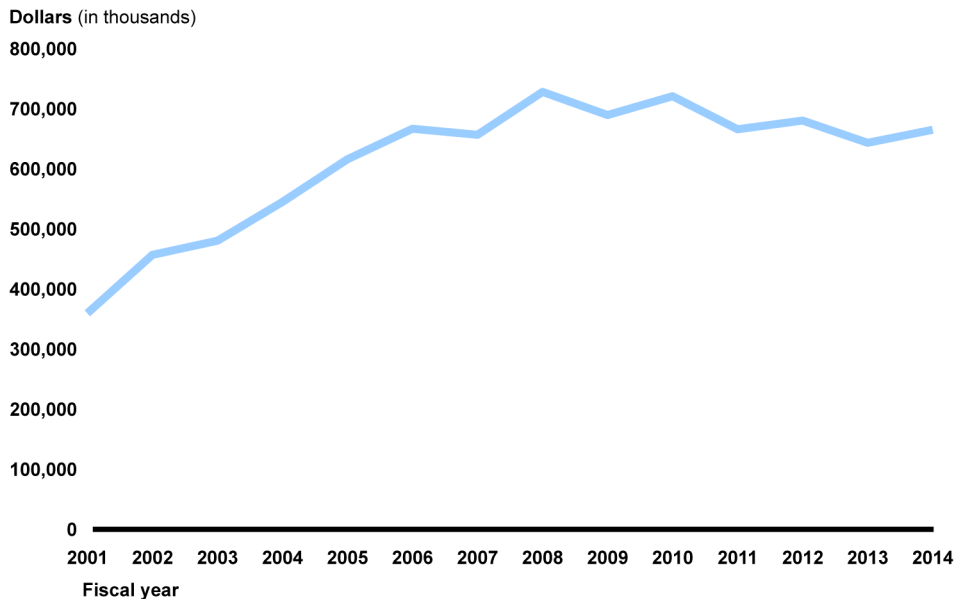
To protect Category I special nuclear material and other security assets—including classified information, which is present at the seven NNSA sites—DOE and NNSA sites use a “defense in depth” strategy, providing multiple layers of physical security measures designed to work in concert to deter, detect, assess, communicate about, delay, and respond to intruders or unauthorized activities. Working in combination with the sites’ armed protective forces, these security measures typically include physical security features and systems, such as integrated cameras, alarms, and motion sensors; fences and antivehicle barriers; numerous access control points, such as turnstiles, badge readers, and vehicle inspection stations; and hardened facilities, including locked storage containers and vaults and specialized procedures for preventing loss or unauthorized access to special nuclear material or classified information.<sup>14</sup>

Costs for protective forces have generally comprised around 60 percent of NNSA’s physical security budget in fiscal years 2001 to 2014. After NNSA’s physical security budget doubled from around \$360 million in fiscal year 2001 to \$728 million in fiscal year 2008, these budgeted costs fluctuated from year to year but, overall, declined somewhat from fiscal year 2009 to fiscal year 2014 (see fig. 2).

---

<sup>14</sup>At five of the seven sites—the Kansas City and Pantex Plants; Lawrence Livermore and Sandia National Laboratories; and Y-12—NNSA’s management and operating (M&O) contractors, which carry out NNSA’s weapons and nonproliferation missions, also provide site security, including protective forces. However, at Los Alamos National Laboratory, protective forces are provided by a subcontractor hired by that site’s M&O contractor and, at the Nevada Nuclear Security Site, these services are provided by a separate contractor hired by NNSA. Before the July 2012 security breach, protective forces at Y-12 were provided by a separate contractor to NNSA. Shortly after the breach, the M&O contractor at Y-12 took over providing the site’s protective forces.

**Figure 2: National Nuclear Security Administration's (NNSA) Physical Security Budget, Fiscal Years 2001 through 2014**



Source: National Nuclear Security Administration. | GAO-14-208

Note: The figure reflects budgeted costs in nominal dollars (i.e., unadjusted for inflation) for what has frequently been designated as “physical security” in NNSA’s congressional budget requests since fiscal year 2001. Most notably, these costs have included budgeted costs for NNSA’s protective forces; sensors, alarms, barriers, and related physical security systems; control and accountability of nuclear materials and classified information; processes to screen personnel’s eligibility to access classified information or nuclear material; and security program management. Physical security budgets have sometimes also included costs for security upgrades to comply with DOE threat policies, or other such costs. Generally not included in NNSA’s physical security budget are other notable security costs, such as those for cyber security, security-related construction projects, and secure transportation of nuclear materials between sites. NNSA has included such costs elsewhere in its budget.

To ensure protection systems operate effectively and efficiently, DOE establishes minimum performance standards and requires implementation of an oversight program to identify and test essential system components and ensure performance. Minimum performance standards for protecting special nuclear material, classified information, and other assets are established in DOE’s system of directives—including orders, manuals, and other policy documents, which DOE and NNSA incorporate into their contracts as requirements for the contractors at their sites. In particular, DOE’s threat policy—a classified policy directive specifying the potential size and capabilities of adversary forces that sites with special nuclear material must defend against—establishes minimum protection standards for special nuclear material at these sites and plays a key role in the design of the sites’ protective strategies and the

---

evaluation of their security performance. As a result, the policy also plays a key role in determining the sites' security costs, particularly for Category I sites. After the terrorist attacks of September 11, 2001, HSS, which has traditionally developed DOE's safety and security policies,<sup>15</sup> revised DOE's threat policy, the Design Basis Threat, on multiple occasions, putting in place increasingly demanding protection requirements.<sup>16</sup> However in 2008, HSS, to reflect updated Intelligence Community assessments of potential adversaries' threat capabilities, reduced some security requirements in the DOE policy, which it renamed the Graded Security Protection Policy.<sup>17</sup> The 2008 DOE policy also did more to recognize sites' varying security needs and risks than previous versions of the policy, providing added flexibility for mission organizations, like NNSA, and their sites to design sites' protective strategies and evaluate their security performance.

Other DOE policies establish more specific standards and requirements for protecting classified information and special nuclear material and for carrying out other security-related activities, such as security planning; fielding sites' protective forces; providing, maintaining, and testing alarms and other security features at sites; and overseeing contractors' security performance and compliance with requirements. DOE policies also govern DOE, NNSA, and contractor employees' authority to make security-related decisions, including the authority to implement security measures at a site or accept security risks. A variety of complementary measures are used to oversee security, including regular inspections and assessments by the contractors responsible for providing sites' security and by the federal field offices that direct and oversee the contractors day

---

<sup>15</sup>As part of the ongoing reorganization in DOE, the Secretary and Deputy Secretaries of Energy announced in February 2014, that HSS's safety and security policy-setting organizations would be relocated from HSS to a new DOE Office of the Under Secretary for Management and Performance.

<sup>16</sup>For additional information, see GAO, *Nuclear Security: DOE Needs to Address Protective Forces' Personnel System Issues*, [GAO-10-275](#) (Washington, D.C.: Jan. 29, 2010) and *Nuclear Security: DOE's Office of the Under Secretary for Energy, Science and Environment Needs to Take Prompt, Coordinated Action to Meet the New Design Basis Threat*, [GAO-05-611](#) (Washington, D.C.: July 15, 2005).

<sup>17</sup>DOE Order 470.3B, *Graded Security Protection (GSP) Policy* (approved Aug. 12, 2008).

---

to day.<sup>18</sup> Furthermore, DOE’s Office of Enforcement and Oversight, an office within HSS, has conducted periodic independent inspections or other assessments to validate the protection systems’ performance.<sup>19</sup> These inspections were often comprehensive—covering all the relevant security topics at a site—and entailed a variety of assessment activities over a period of days or weeks, and usually include rigorous “force-on-force” exercises to test the site’s security response to a simulated attack.

---

## Reforms May Have Helped Manage NNSA’s Security Costs and Enhance Its Productivity but May Have Increased Risks at Some Sites

Implementation of security reforms from 2009 to 2012 generally varied among NNSA’s sites. DOE and NNSA officials and contractors told us that some of their actions to implement the reforms helped manage security costs and enhance productivity, among other benefits, but NNSA has limited quantifiable data on these benefits. They also said that, as a main drawback, actions to implement some of the reforms may have increased security risks and reduced security performance at Y-12 and other sites, depending on how the sites implemented the reforms.

---

## Officials and Contractors Said Implementation of Reforms Helped Manage Security Costs and May Have Enhanced Some Sites’ Productivity

DOE, NNSA, and contractors took various actions to implement the reforms that DOE and NNSA initiated in 2009 to 2012 to identify and eliminate potentially unnecessary security costs, improve efficiency by realigning security requirements that may be impeding NNSA sites’ productivity, and streamline federal oversight. Although some of the actions to implement the 2009 to 2012 reforms aimed to standardize

---

<sup>18</sup>NNSA field offices (formerly known as site offices) collocated at most NNSA sites administer NNSA’s contracts and direct and oversee the contractors at those sites. In 2012, NNSA opened an NNSA Production Office to carry out these responsibilities for two sites—namely, the Pantex Plant and Y-12—in place of the separate field offices for these sites. It did so in anticipation of combining management and operation of the two sites under a single M&O contract. Specialized NNSA personnel at the field offices and the NNSA Production Office direct and oversee contractors’ security performance day to day, in accordance with headquarters policy and direction.

<sup>19</sup>As part of the ongoing reorganization in DOE, the Secretary and Deputy Secretaries of Energy announced in February 2014 that independent oversight inspections would be carried out by a new Office of Independent Enterprise Assessments, rather than by HSS’s Office of Enforcement and Oversight, which has traditionally conducted these inspections.

---

Actions Intended to Identify and Eliminate Potentially Unnecessary Security Costs

---

sites' security approaches, DOE, NNSA, and contractors' actions generally varied among NNSA's sites.

To identify and eliminate potentially unnecessary security costs, NNSA and its contractors took the following actions to institute a more "corporate" or standardized approach to security budgeting or other aspects of sites' security:

- *Standardizing site security budgets.* To obtain more detailed information about NNSA sites' security expenditures and costs and improve comparability of cost data, NNSA's Office of Defense Nuclear Security (DNS) increased from 30 to 41 the number of security-related cost categories that contractors must use for security budgeting and reporting. DNS also issued security costing guidelines to clarify which costs may be paid for using NNSA's physical security budget and developed various spreadsheets and other tools to help standardize sites' security budgeting in order to better track their expenditures. One of the new tools, a spreadsheet for sites to use for budgeting and tracking of their protective force costs, required sites to provide detailed information for each protective force guard post and patrol, of which there may be dozens at a site. The required information included the numbers of personnel, labor hours, and average pay rates for various protective force positions; equipment usage; and other information.
- *In-depth reviews.* To help monitor sites' spending and identify potentially unnecessary costs, DNS enlisted security experts from across NNSA to review sites' annual budget submissions and conduct quarterly reviews of sites' security spending. DNS also coordinated and led in-depth reviews of contractor requirements, known as "deep dives," at six of the NNSA sites to assess whether the sites' physical security spending was consistent with the new costing guidelines and verify that sites' security measures—particularly, measures not directly related to the protection of Category I special nuclear material—did not exceed DOE and NNSA security requirements.<sup>20</sup>

---

<sup>20</sup>Officials at the Kansas City Plant told us that the site did not undergo a "deep dive" review, because the site's security budget is much smaller than NNSA's Category I sites. Instead, a DNS-led team evaluated the site's protective force operations in depth in 2010, which like the "deep dive" reviews, included recommendations for reducing costs and improving compliance with NNSA's costing guidelines and DOE and NNSA policies. "Deep dives," in contrast, examined other aspects of sites' physical security, such as alarms and related security systems, in addition to examining protective forces.



---

The reviews, which were carried out in 2011 and 2012 by multidisciplinary teams of NNSA officials and contractors, resulted in site-specific recommendations, including potential cost savings for some of the recommendations. A number of the recommendations entailed consolidating or eliminating specific guard posts, patrols, or other security measures that a review team had found to be potentially unnecessary or had identified as potentially deviating from NNSA's costing guidelines or DOE and NNSA security requirements. In other cases, the review teams recommended changes to improve the efficiency or effectiveness of sites' security program management, such as processes for security budgeting or vulnerability assessment. In a few cases, the teams recommended that sites invest in additional security equipment or technologies to help enable future cost savings or that sites begin paying for certain security-related costs using NNSA's physical security budget rather than using other funds, in order to improve conformity with NNSA's new costing guidelines. DNS officials told us that approximately \$53 million in total potential savings had been identified from the "deep dive" reviews.

- *Protective forces' training and equipment.* To better coordinate training requirements for protective forces across NNSA and manage associated costs, DNS and contractor and NNSA security specialists at sites collaborated to develop NNSA-wide protective force training requirements, including a common set of performance and testing standards for various protective force roles. In response to previous recommendations, including from our prior report,<sup>21</sup> the officials and contractors also formed a security commodity team to standardize security equipment across NNSA sites and better leverage NNSA's buying power for purchasing security equipment. In 2010 and 2011, this team entered into two 5-year agreements with vendors allowing NNSA sites to receive discounts on purchases of protective masks, uniforms, and other equipment.

In an additional effort that was at least partly intended to identify and eliminate potentially unnecessary security costs, in 2011, DOE and the Department of Defense (DOD) jointly updated DOD's intelligence

---

<sup>21</sup>In 2010 we recommended that DOE develop and, as practicable, carry out implementation plans for the 29 recommendations made by its 2009 study group for enhancing protective forces' career longevity and retirement options. The group's recommendations included standardizing protective forces' equipment, such as uniforms and weapons, where possible. See [GAO-10-275](#).

---

assessment of terrorist and other threats to U.S. nuclear sites.<sup>22</sup> This updated assessment characterized the potential terrorist threat as less capable than envisioned in DOE's 2008 threat policy, which as noted earlier, specifies the potential size and capabilities of adversary forces that DOE and NNSA sites must defend against and plays a key role in determining sites' security costs. According to HSS officials and DNS, revisions to the 2008 threat policy, which were being drafted during the 2009 to 2012 reforms, considered a broader range of nonterrorist threats and offered the potential for reducing security costs by allowing DOE's and NNSA's Category I sites to prepare for a less-demanding terrorist threat. In anticipation of DOE eventually issuing the draft revisions as an updated version of the threat policy, DNS worked with HSS and NNSA officials or contractors at sites to begin evaluating some sites' security performance against threats described in the draft revisions and identifying opportunities for potentially reducing some security measures and associated costs. Additionally, HSS and DNS collaborated with DOD and other agencies that protect nuclear assets to begin establishing more consistent protection standards and, as appropriate, modifying such standards that, according to HSS and NNSA officials, may have previously led to unnecessary security costs in DOE and NNSA.

NNSA and contractors cited a number of benefits from the actions to identify and eliminate what they viewed as potentially unnecessary security costs. DNS officials said that, as a result of standardizing site security budgets and in-depth reviews, the transparency of NNSA security costs and the consistency of cost reporting greatly improved, providing the officials with a more detailed understanding of costs and greater assurance of the costs' completeness and accuracy when evaluating sites' budget requests and when monitoring and forecasting sites' security spending. Similarly, NNSA officials and contractors at some sites said standardizing site security budgets allowed them to more easily

---

<sup>22</sup>DOE and DOD collaborated on a 2011 update of the Nuclear Security Threat Capabilities Assessment, a document that describes, primarily, terrorist threats to U.S. nuclear sites based on historical precedents and plausible scenarios. At various times since the attacks of September 11, 2001, this document or its predecessor have been used in the development of DOE's and DOD's security policies. For more information, see GAO, *Homeland Defense: Greater Focus on Analysis of Alternatives and Threats Needed to Improve DOD's Strategic Nuclear Weapons Security*, [GAO-09-828](#) (Washington, D.C.: Sept. 18, 2009) and *Nuclear Security: DOE and NRC Have Different Security Requirements for Protecting Weapons-Grade Material from Terrorist Attacks*, [GAO-07-1197R](#) (Washington, D.C.: Sept. 11, 2007).

---

benchmark their security costs against those of other sites and provided them additional opportunities to interact with DNS and other sites. NNSA officials told us that they had begun achieving some cost savings from the approximately \$53 million in potential savings identified during the “deep dive” reviews. Regarding the reforms to better coordinate protective force training and equipment, the security commodity team reported in early 2012 that it had achieved about \$245,000 in savings on purchases of 2,900 protective masks through one of its new agreements. The team was anticipating additional savings through this agreement, as well as \$279,000 in savings on protective force uniforms from the team’s other agreement, which sites had only recently begun using.

Even with some reported cost savings, however, the overall impact from the actions to identify and eliminate potentially unnecessary costs is difficult to assess, in part because relevant cost information was not always included in savings estimates. For instance, contractors at Los Alamos National Laboratory told us, in October 2013, that their site had saved nearly \$700,000 in fiscal year 2013 from implementing “deep dive” recommendations made earlier that year. However, these savings were partially offset when another NNSA program opted to take over funding for a guard post which laboratory officials had agreed to eliminate in response to a “deep dive” recommendation, but which the program determined was needed for robust security. While total physical security costs have declined somewhat from their peak in 2008, other factors may have played a role in reducing these costs, making it difficult to isolate the contribution of the reforms to assess their impact on security costs. For example, around the time of the 2009 to 2012 reforms, some NNSA sites were also engaging in their own efforts to reduce their security costs that were separate from their actions to implement the reforms.

**Actions Intended to Improve Efficiency by Realigning Security Requirements That May Be Impeding NNSA Sites’ Productivity**

To improve efficiency by realigning DOE security requirements that NNSA believed may be impeding its sites’ productivity, DNS worked with NNSA and contractor security specialists in multiple working groups to identify such requirements and draft new NNSA security policies. Collectively, the working groups drafted six NNSA Policy Letters on various security-related topics; these Policy Letters were intended to replace the corresponding DOE security policies on those topics. During the reforms of 2009 to 2012, two of the six Policy Letters were approved by the NNSA Administrator and issued as policy in 2010, and the other four remained in draft and were never issued. The two issued Policy Letters—which focused on the control of classified information, such as classified documents and electronic media, and on the physical protection of facilities, property, personnel, and national security interests, such as

---

special nuclear material—were included in NNSA’s contracts as security requirements for its contractors in place of the corresponding DOE directives.<sup>23</sup> In contrast, other DOE directives, such as directives governing security program management and protective forces, were allowed to remain in NNSA’s contracts.

According to the two issued Policy Letters, the new NNSA security policies were largely based on DOE’s policies but, in some cases, were tailored to meet NNSA’s programmatic needs and address NNSA and contractor concerns by changing or eliminating requirements seen as overly burdensome—mainly requirements for protecting classified information (see app. I). The changes were also intended to better align NNSA’s policies with national standards, including the National Industrial Security Program, which was established in 1993 through an Executive Order to safeguard federal classified information released to the federal government’s contractors, licensees, and grantees. According to NNSA officials, other provisions in the issued Policy Letters aimed to allow security decisions to occur at the “right” level by expanding contractors’ authority to make security decisions and accept some security risks at their sites, particularly for what NNSA considered lower risk, lower consequence activities.

NNSA and contractors cited benefits from the actions to improve efficiency by realigning security requirements that they believed may be impeding sites’ productivity, including productivity gains or other benefits,

---

<sup>23</sup>NNSA’s policies included Policy Letter 70.2, *Physical Protection*, and 70.4, *Information Security*, which were approved in July 2010 and replaced, respectively, DOE M 470.4-2A, *Physical Protection Manual* (July 2009), and DOE M 470.4-4A, *Information Security Manual* (January 2009). As part of its own reform effort, DOE subsequently canceled and replaced the manuals and other DOE directives with DOE Order 473.3, *Protection Program Operations* (June 2011) and Order 471.6, *Information Security* (June 2011). However, one section of DOE M 470.4-4A on technical surveillance countermeasures was retained as policy.

In addition, the Kansas City Plant has been operating under its own site-specific safeguards and security requirements, as requested by the NNSA Administrator in 2006 to reduce safety and security requirements that may have been impeding productivity at the site, among other goals. Because the site largely engages in nonnuclear activities, it was able to gain exemptions from many DOE requirements and develop its own site-specific requirements, which according to NNSA documents and the official responsible for directing NNSA’s security oversight of the site, were generally based on departmental directives and national industrial standards. NNSA officials and contractors at the Kansas City Plant also told us they used their experience to help NNSA develop its security Policy Letters and participated in other aspects of the 2009 to 2012 reforms.

---

although they were not always able to quantify them. For example, field office officials and contractors at several NNSA sites told us they were able to improve their productivity by eliminating steps to control and account for certain types of classified electronic media or by modifying or eliminating other security measures, as allowed under NNSA's new security policies. Field office officials or contractors at several of the sites told us that motion sensors no longer required for protecting classified information were deactivated or removed in some areas, thus reducing the amount of testing and maintenance needed for motion sensors at their site and potentially reducing the rate of false and nuisance alarms that security officials must respond to. NNSA and contractors also noted other productivity gains from some reductions in security measures, including time savings for employees from no longer having to lock up certain classified documents (or other forms of classified information) and retrieve them from locked storage containers—sometimes residing in inconvenient locations within the locked security areas—throughout the workday. Furthermore, some NNSA officials and contractors said the process of developing the Policy Letters provided its own benefits, including better collaboration between headquarters and the field and a greater sense of “ownership” of the security policies they oversee or carry out day to day. However, attempts to quantify the benefits have been somewhat limited. A 2009 study at Lawrence Livermore National Laboratory, for example, concluded that allowing that site's employees to leave classified information in locked security areas but outside of locked storage containers during the workday could prevent as much as \$48.5 million each year in lost productivity without any “discernible” increase in security risks. After implementing this policy under the 2009 to 2012 reforms, however, the contractor officials there told us that, during the reforms, they did not attempt to routinely measure the effect of the policy change on productivity, which they and officials at other NNSA sites said would be difficult to quantify accurately on a continuing basis.<sup>24</sup>

**Actions Intended to Streamline Federal Oversight**

During the reforms in 2009 to 2012, DOE, NNSA, and contractors also took actions to streamline federal oversight. The actions, which became

---

<sup>24</sup>In 2013, Livermore's contractor estimated that the policy change, which was still in effect at the site, was preventing between \$16.2 million and \$65.2 million (and an average of \$36.9 million) annually in lost productivity, depending on employees' usage of the policy.

---

known by the National Research Council and others as “hands-off, eyes-on” oversight,<sup>25</sup> included the following:

- From 2010 to 2012, HSS scaled back on its traditional independent oversight inspections at NNSA sites and, instead, began conducting inspections or other types of assessments that were more limited in scope.<sup>26</sup> Rather than conducting traditional independent oversight inspections, during this period, HSS conducted a series of limited performance assessments and other reviews of limited aspects of NNSA sites’ security, such as a 2010 review of Y-12’s protective forces. At NNSA’s request, HSS also provided technical assistance on various security matters at Y-12 and other NNSA sites.<sup>27</sup> According to HSS officials, traditional independent oversight was scaled back to enable HSS to assist with NNSA’s security reforms and to revise DOE’s independent oversight process, as part of the safety and security reforms requested by the Deputy Secretary of Energy. According to the officials, HSS also issued significantly fewer deficiency findings during this period, opting, instead, to raise issues and recommend opportunities for improvements, which—unlike findings from traditional oversight inspections—do not require NNSA or contractors to prepare and implement formal corrective action plans. In April 2012, before the Y-12 security breach in July of that year, HSS said it resumed its comprehensive independent oversight inspections under a revised version of its independent oversight policy that focused on a smaller number of security-related topics.<sup>28</sup> After resuming its more narrowly focused comprehensive inspections, HSS did not conduct such an inspection at Y-12 until its August through

---

<sup>25</sup>See, for example, National Research Council, *Managing for High-Quality Science and Engineering at the NNSA National Security Laboratories*, (Washington, D.C.: Feb. 15, 2012).

<sup>26</sup>In the past, DOE has temporarily modified its independent oversight. For example, force-on-force testing activities, which have often been conducted as part of independent oversight inspections, were temporarily scaled back to allow for an increase in security protections at DOE and NNSA sites after the terrorist attacks of September 11, 2001.

<sup>27</sup>See, for example, HSS, *Independent Oversight Protective Force Site Assistance Visit at the Y-12 National Security Complex* (Aug. 12, 2010).

<sup>28</sup>DOE canceled its 2002 policy directive on independent oversight with the issuance of a new directive in August 2011—DOE Order 227.1, *Independent Oversight Program*—as part of the safety and security reforms directed by the Deputy Secretary of Energy in 2009.

---

September 2012 inspection in response to that site's July 2012 security breach.

- As part of its governance transformation project, NNSA issued a policy in 2011 that laid out basic requirements for a new oversight model for NNSA.<sup>29</sup> NNSA's new model was consistent with the oversight changes directed by the NNSA Administrator, as well as the oversight changes and policy updates directed by the Deputy Secretary of Energy, as part of DOE's parallel reform effort. To implement the new oversight model, some NNSA field office officials said that they began conducting fewer security inspections of their own and relying more heavily on contractors' self-inspections, which the officials sometimes observed (or "shadowed"). The officials also said that they essentially discontinued doing security "surveys"—a long-standing oversight approach, required in DOE policies, that involves annual inspections to assess contractors' security performance and compliance with security requirements for a broad range of security topics.<sup>30</sup> Instead, the officials and contractors began coordinating their inspection schedules to avoid what NNSA's policy described as unnecessary duplication of oversight. They also used risk assessment methods to focus federal oversight, including inspections, on higher-risk activities and known performance problems.
- Under the new NNSA oversight model, NNSA also placed greater reliance on data from "contractor assurance systems"—management systems and processes designed and used by NNSA's contractors to monitor their own performance and self-identify and correct potential problems. NNSA, which validates the systems, used the systems' data to monitor contractors' performance in safety, security, and other areas and to tailor the level of oversight. In the area of security, contractors made performance information available to NNSA officials on a variety of measures. For example, the contractor at Lawrence Livermore National Laboratory provided NNSA weekly reports on 17 performance measures, ranging from the percentage of protective

---

<sup>29</sup>NNSA Policy Letter 21, *Transformational Governance and Oversight* (approved Feb. 28, 2011).

<sup>30</sup>For more on DOE's security surveys, see GAO, *Nuclear Security: NNSA Needs to Better Manage Its Safeguards and Security Program*, [GAO-03-471](#) (Washington, D.C.: May 30, 2003).

---

force members achieving weapons qualification to the number of self-inspections completed.

- NNSA field offices and contractors also began reporting quarterly to DNS on the overall status and performance of their sites' security program. The quarterly reports varied somewhat by site but generally included narrative on security performance and issues, as well as quantitative or other data on various performance measures, such as the number of security inspections completed and the extent to which security spending has stayed within budget and contractor assurance systems have been effective in helping NNSA officials and contractors monitor security performance.

Some NNSA officials and contractors said the actions to streamline federal oversight helped them apply a more efficient or effective oversight approach. In particular, coordinating their inspection schedules and using a risk-based approach helped them reduce duplication and prioritize oversight on higher-risk activities and known problem areas, rather than covering a broad range of topics every year, as required for security surveys. Also, NNSA officials or contractors at two sites said that the more streamlined approach allowed greater opportunity to assess the effectiveness of the sites' security approaches and understand the "root causes" of security problems, rather than focusing on sites' compliance with security requirements. Furthermore, HSS and NNSA officials said the limited performance assessments and other reviews provided valuable assistance for NNSA sites, whereas traditional independent oversight inspections had sometimes led to unnecessary requirements and associated costs, according to some NNSA officials and contractors.

---

### **Actions to Implement Some Reforms Reportedly May Have Increased Risks and Reduced Security Performance at Some Sites**

In addition to identifying benefits of the reforms, DOE and NNSA officials and contractors we interviewed said that actions to implement some of the reforms in 2009 to 2012 may have had the drawback of increasing security risks and reducing security performance at some sites, particularly at Y-12. However, the potential amount of risk associated with the reforms largely depended on their implementation, which, as we noted earlier, varied among the sites. Regarding the actions to identify and eliminate potentially unnecessary security costs, NNSA officials and contractors at several sites said that some of the recommendations made during the "deep dive" reviews of contractor requirements—while focused on measures not directly related to the protection of Category I special nuclear material—may have encouraged inappropriate risks, for example, by recommending cuts in protective force posts and patrols. Some NNSA field office officials or contractors said these posts and patrols provided



---

critical protections or enhanced security awareness of the site. Likewise, some actions to prepare for the draft revisions to DOE's 2008 threat policy may have encouraged sites to take additional risks. For example, NNSA may have encouraged increased risks at Y-12 when the Chief of Defense Nuclear Security directed the site to suspend any further actions to achieve full compliance with the 2008 threat policy. As of 2011, the site had not yet achieved full compliance with the 2008 policy. According to the DNS Chief's December 2011 memorandum directing Y-12 to suspend its efforts to achieve full compliance, such efforts would result in costs that would likely be unnecessary with the anticipated revisions to the 2008 policy. Also, according to the memorandum, the efforts would complicate future plans to substantially reduce Y-12's protective forces in line with the anticipated revisions. According to NNSA officials and Y-12 contractor personnel, some reductions in the site's protective forces had occurred before the July 2012 security breach, and additional reductions were being planned. DNS officials told us that at least some of these reductions were in response to security improvements put in place at Y-12 after 2008. After the security breach in July 2012, however, NNSA canceled the planned reductions, and protective force patrols were temporarily increased at the site.

Regarding the actions to improve efficiency by realigning security requirements that may be impeding NNSA sites' productivity, HSS raised concerns on multiple occasions about potential risks from NNSA's security Policy Letters developed under the reforms. Before the Y-12 security breach, for example, HSS expressed concern in a March 2012 draft "special study" of DOE and NNSA security policies that the Policy Letters delegated overly broad security authority to NNSA contractors and did not clearly distinguish federal and contractor authorities to make security decisions and accept risks, among other concerns. In an April 2012 memorandum to the HSS Deputy Chief for Operations, the DNS Chief responded that language in both the issued Policy Letters and the draft letters, which NNSA was preparing to issue, clearly distinguished between federal and contractor authorities. However, HSS's report on its independent oversight inspection of Y-12 conducted in response to the security breach,<sup>31</sup> described the Y-12 contractors' authority to make

---

<sup>31</sup>HSS, *Independent Oversight Safeguards and Security Inspection of the National Nuclear Security Administration's Y-12 National Security Complex* (Sept. 28, 2012).

---

security decisions as appearing to be “unconstrained” and cited NNSA’s policies as a contributing factor in the security breach.

Regarding the actions to streamline federal oversight, NNSA officials and contractors at some sites told us that implementation of “hands-off, eyes-on” oversight model had not been carefully managed, potentially increasing sites’ security risks. At Sandia National Laboratories, for instance, the lead NNSA official responsible for overseeing contractors’ security performance said her office did not receive adequate guidance or training on how to implement the oversight changes. At Y-12, the officials with this responsibility said that their site’s implementation of “hands-off, eyes-on” oversight required them to greatly increase their reliance on contractor self-inspections, which were sometimes inadequate for ensuring protection at the site.<sup>32</sup> Furthermore, according to an August 2012 review by Y-12’s contractor and Y-12 contractor representatives we interviewed, the site’s contractor assurance system—used by NNSA’s contractors to self-monitor performance and self-identify potential problems—did not track certain key security performance measures, including ones related to false and nuisance alarm rates and security equipment maintenance, until after the July 2012 security breach. Although the contractor assurance system had previously been certified by NNSA, high rates of false and nuisance alarms and extensive repair times for inoperable security equipment were later found to have contributed to the security breach. According to the reports from the Y-12 contractor and the DOE Inspector General’s investigation of the security breach, these and other security problems were not captured by the contractor assurance system or received positive performance ratings in the system. Furthermore, according to the Inspector General’s report, the Y-12 contractor did not include known security problems in the quarterly reports it submitted to DNS, and the NNSA officials there took no action to resolve such problems until after the security breach, even with their

---

<sup>32</sup>In one instance, NNSA’s security oversight officials at Y-12 observing a contractor’s self-inspection in March 2012 concluded that methods used to test motion sensors outside the facility being inspected were inadequate to ensure protection of the facility’s classified matter and violated DOE and NNSA security policies, which required more rigorous testing methods. According to a report from NNSA officials who observed the self-inspection, the contractor had determined that more rigorous testing was unnecessary and used the decision-making flexibility in NNSA’s security Policy Letters to authorize less rigorous testing and, effectively, exempt itself from DOE and NNSA requirements. While the NNSA officials observing the inspection found that the contractor had overstepped its authority and placed classified matter at risk, according to their report, other NNSA officials at Y-12 ultimately determined the issue did not constitute a security vulnerability.

---

awareness of the prolonged equipment outages and other problems. Likewise, a DNS-led review team convened shortly after the Y-12 breach found ineffective federal oversight to be among the factors that had allowed the breach to occur.

Recognizing the risks associated with some of the 2009 to 2012 reforms, NNSA field officials and contractors told us that, in some cases, they did not implement certain actions or tailored their implementation to mitigate these risks. For example, of the 24 unique recommendations made during the DNS-led “deep dive” requirements review at Los Alamos National Laboratory in January 2012, contractor representatives reported they did not implement 5, in part, because doing so would have likely increased the site’s security risks.<sup>33</sup> Similarly, contractor personnel at Sandia National Laboratories told us their site opted not to allow its employees to leave classified information unattended for extended periods during the workday, as allowed by an NNSA Policy Letter, because the site did not want to create opportunities for security infractions, which had increased somewhat. Some NNSA field office officials told us they continued conducting their own security inspections, in addition to observing contractors’ self-inspections, and took steps to verify the information in their site’s contractor assurance system. According to some NNSA officials, they were sometimes able to independently tailor their implementation of the reforms because NNSA field offices, and not DNS, were ultimately responsible for administering NNSA’s contracts and directing and overseeing contractors’ day-to-day security performance, among other reasons.

While NNSA sites took steps to avoid or mitigate risks associated with some of the 2009 to 2012 reforms, an HSS-led review conducted after the Y-12 security breach found that the risks leading to the Y-12 breach were concentrated at Y-12 and were not prevalent among other DOE and NNSA Category I sites.<sup>34</sup> The review concluded that security at those

---

<sup>33</sup>The report for the “deep dive” requirements review at Los Alamos National Laboratory included 26 recommendations, 2 of which, however, were repeated in various sections of the report, leaving 24 unique recommendations. In addition to the 5 recommendations with likely security risks, laboratory contractor officials said the site avoided implementing 6 others because of high implementation costs or increased traffic hazards from automating certain vehicle gates, among other reasons.

<sup>34</sup>HSS, *Post Y-12 Security Incursion Extent of Condition Review* (undated). According to HSS officials, this report was released in June 2013.

---

sites was adequate for protecting Category I special nuclear material from a terrorist attack and, at the NNSA sites, would also likely preclude a nonterrorist security breach similar to the Y-12 breach.

---

## NNSA Initiated Actions to Improve Security Performance and Oversight but Has Not Developed a Clear Path Forward

In the wake of the July 2012 security breach at Y-12, NNSA took a number of actions designed to improve its security performance and oversight but did so without first developing a clear vision and path forward for its security program and an implementation strategy. After the Y-12 breach, DOE and NNSA halted, reversed, or modified a number of the previous security reforms. NNSA also initiated new actions to improve its security performance and oversight, including two successive headquarters reorganizations of its security office. Before undertaking these actions, however, NNSA did not carry out a priority recommendation by its own Security Task Force that it develop a security “road map,” including a clear vision and path forward for its security program and an implementation strategy. The recommendation also mirrors effective practices that we have previously identified for successfully implementing and sustaining management improvement initiatives.

---

## After the Y-12 Security Breach, DOE and NNSA Halted, Reversed, or Modified Implementation of Some of the Previous Security Reforms

After the Y-12 security breach in July 2012, and in response to some of the reform goals and recommendations identified by the 2012 NNSA Security Task Force, DOE and NNSA halted, reversed, or modified implementation of some of the 2009 to 2012 reforms. For example, HSS officials told us that, after the Y-12 breach, they halted their previous efforts to issue a revised version of DOE’s threat policy, which NNSA anticipated would eventually lead to reductions in sites’ security costs. HSS instead continued to revise the threat policy to reflect lessons learned from the Y-12 breach and other recent security incidents. As of March 2014, DOE had not issued a revised version of the policy. Similarly, NNSA halted further implementation of the security Policy Letters, which it had developed during the 2009 to 2012 reforms, and initiated actions to rescind the issued Policy Letters and reinstate DOE’s security directives. NNSA initiated these actions in response to a recommendation made in 2012 by the NNSA Security Task Force—a task force established by the NNSA Administrator in August 2012 to assess NNSA’s security organization and oversight in the wake of the Y-12 security breach. In December 2012, the Acting DNS Chief instructed NNSA’s sites to study the costs and other impacts of reinstating DOE directives. A follow-up memorandum further directed NNSA sites to prepare plans for implementing the DOE directives. As of March 2014,

---

NNSA sites were in varying stages of incorporating the DOE directives into their contracts and implementing the directives, according to DNS officials.

Implementation of other reforms from 2009 to 2012 continued generally as they had before the Y-12 breach or with modifications. For example, NNSA officials told us that efforts to put in place NNSA-wide protective force training requirements continued after the Y-12 breach, and sites have been implementing the new requirements, while the NNSA officials assessed the implementation and provided assistance. The officials also said that, in line with the earlier efforts to standardize site security budgets, they were developing a new tool for tracking the costs associated with operating and maintaining sites' security equipment, which NNSA and HSS officials said is aging and, in some cases, operating far beyond its intended life span. Concerning the previous actions to streamline federal oversight, quarterly reporting by NNSA field offices and contractors on the overall status and performance of their sites' security programs continued after the Y-12 breach, but modifications were made to the reporting format, according to NNSA officials, and data that was previously collected on various security-related performance measures was removed from the reporting requirements, while NNSA reexamined its performance measures. In addition, "hands-off, eyes-on" oversight practices—such as NNSA field office officials observing contractors' security inspections and relying on contractor assurance systems for security oversight—have generally continued, but according to HSS officials, some adjustments have been made since the Y-12 breach. However, NNSA modified aspects of its security oversight in 2013 when DNS began conducting its own security inspections regularly at NNSA sites, as recommended by the NNSA Security Task Force and directed by a previous Acting Administrator. NNSA later discontinued the inspections, after the subsequent Acting Administrator reexamined DNS's role and determined that inspections should not be a primary focus for DNS.

---

### NNSA Has Not Developed a Clear Vision or Path Forward for Improving Its Security Performance and Oversight

In addition to halting, reversing, or modifying previous actions, NNSA initiated new actions designed to improve its security performance and oversight, but it did so without first developing a clear vision and path forward for its security program and an implementation strategy. To improve NNSA's security performance and oversight after the Y-12 security breach, NNSA initiated a headquarters reorganization of its security office—as recommended by NNSA's Security Task Force—which, however, it later reversed under a second reorganization. Plans for

---

the first reorganization were formally approved by a previous Acting Administrator in May 2013 and became effective in July 2013, according to NNSA officials and documents. Under this reorganization, security program responsibilities were divided between DNS and a new headquarters-based security organization. Consistent with Security Task Force recommendations, NNSA shifted to the new organization many of the security program and policy implementation responsibilities traditionally carried out by DNS and, in turn, restructured DNS to focus mainly on conducting security inspections at NNSA sites and developing NNSA-specific security policies in line with DOE's security directives. According to NNSA officials and documents, these changes aligned with various reform goals that the task force had identified, including clarifying security roles and responsibilities and lines of authority and accountability; promoting more consistent security implementation; and strengthening the role of federal security assessment to improve oversight.

Months later, however, under the subsequent and most recent Acting Administrator, NNSA put this reorganization effort on hold and initiated a second reorganization that essentially reversed the previous effort. In September 2013, that Acting Administrator announced further organizational changes for NNSA, including security, which DNS officials said they took initial steps to implement, for example, by winding down DNS's new security inspection program. Under this second reorganization, NNSA's headquarters security would revert back to a single office—specifically, DNS—generally as it was before the previous reorganization and the Y-12 security breach. This office would be responsible for security program management responsibilities and would no longer focus on conducting security inspections or developing NNSA-specific policies. According to the Acting Administrator and DNS officials, these changes would further clarify NNSA's lines of authority and accountability by reducing the number of headquarters organizations responsible for security. And, the changes would reestablish the program and policy implementation role described in the NNSA Act for the position of Chief of Defense Nuclear Security and serve as a test case for broader organizational reforms, aimed at improving integration and collaboration between NNSA headquarters and the field. According to DNS, this second reorganization became effective in February 2014 under the most recent Acting Administrator.

NNSA undertook the various actions after the Y-12 security breach, including the successive reorganizations, without first carrying out a priority recommendation from its Security Task Force, according to NNSA

---

and HSS officials. Specifically, in its report to the NNSA Administrator, the Security Task Force recommended that NNSA develop a security “road map” that would articulate a clear vision and path forward for NNSA’s security program, as well as an implementation strategy, including regular monitoring, to help ensure that its actions will lead to sustainable solutions. The task force further specified that NNSA make developing and implementing the security road map a priority over other actions and, in developing the road map, consider both the task force’s other recommendations and ones from other sources. The recommendation mirrors effective practices that we have previously identified for successfully implementing and sustaining management improvement initiatives in DOE. These practices include establishing clearly defined goals for improvement initiatives; developing an implementation strategy, including milestones and responsibilities for carrying them out; and establishing results-oriented outcome measures and data.<sup>35</sup> However, according to NNSA and HSS officials, such a road map was neither developed before initiating the first reorganization, nor have we observed clear evidence of such a road map guiding NNSA’s actions. For example, documents related to the current reorganization, including a December 2013 memorandum from the Acting Administrator, have specified how NNSA’s headquarters security office will be reorganized, but it did not articulate a clear vision and path forward for NNSA’s security program and an implementation strategy.

Without developing a clear vision and path forward for its security program, NNSA risks putting in place another short-lived or ineffective response to its security problems, on which we and others have

---

<sup>35</sup>Specifically, the practices—which we previously identified from our review of various studies by the National Academy of Public Administration, the Project Management Institute, and others on the practices of leading organizations—include (1) establishing clearly defined goals for the improvement initiative; (2) developing an implementation strategy that sets milestones and establishes responsibility for carrying out the initiative; (3) establishing results-oriented outcome measures to gauge progress toward the goals; and (4) using results-oriented data to evaluate the initiative’s effectiveness and make changes as warranted. See GAO, *Contract Reform: DOE Has Made Progress, but Actions Needed to Ensure Initiatives Have Improved Results*, [GAO-02-798](#) (Washington, D.C.: Sept. 13, 2002), and [GAO-12-347](#).

---

previously reported,<sup>36</sup> and which the Security Task Force has highlighted in its other recommendations from 2012. For example, we have long reported on DOE and NNSA's efforts to address weaknesses in organizational culture, including safety and security,<sup>37</sup> which other studies, including ones that NNSA commissioned in 2003, have also identified. In particular, one of the 2003 studies found weaknesses in NNSA's security culture, including the failure by many managers and employees, particularly at national laboratories, to properly value security as integral to NNSA's missions or to embrace an enterprise-wide security approach.<sup>38</sup> More recently, in the September 2012 report from its independent oversight inspection of Y-12 conducted in response to the security breach, HSS raised concerns that NNSA had fostered an organizational culture at Y-12 not adequately focused on meeting high standards for security performance. And, during March 2013 testimony before the House Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, the leader of NNSA's Security Task Force noted that NNSA's leaders had allowed a culture to develop in NNSA, which emphasized cost containment "to the detriment" of security program execution. The task force leader further noted that NNSA's previous attempts to address security issues have not properly emphasized effective security performance, and effective leadership in DOE and NNSA would be crucial for assuring performance in the long term. In its report to the NNSA Administrator, the Security Task Force

---

<sup>36</sup>From 2006 through 2009, for example, we issued three reports on high-profile security incidents at Los Alamos and Lawrence Livermore National Laboratories, which—despite precipitating a 10-month stand-down of operations at Los Alamos in 2004 and a change in that site's contractor in 2005, among other attempts at correcting security problems—may not have resulted in sustained improvements. See, [GAO-06-83](#); GAO, *Los Alamos National Laboratory: Long-Term Strategies Needed to Improve Security and Management Oversight*, [GAO-08-694](#) (Washington, D.C.: June 13, 2008); and *Nuclear Security: Better Oversight Needed to Ensure That Security Improvements at Lawrence Livermore National Laboratory Are Fully Implemented and Sustained*, [GAO-09-321](#) (Washington, D.C.: Mar. 16, 2009). More recently, in March 2013, we compared security performance and oversight problems identified by the NNSA Security Task Force to similar problems we had reported on in 2003. See [GAO-13-482T](#).

<sup>37</sup>See, for example, GAO, *Department of Energy: Views on the Progress of the National Nuclear Security Administration in Implementing Title 32*, [GAO-01-602T](#) (Washington, D.C.: Apr. 4, 2001); *National Nuclear Security Administration: Additional Actions Needed to Improve Management of the Nation's Nuclear Programs*, [GAO-07-36](#) (Washington, D.C.: Jan. 19, 2007); [GAO-10-275](#); and [GAO-12-347](#).

<sup>38</sup>See LMI Government Consulting and SAGE Systems Technologies, *NNSA Security: An Independent Review* (April 2005).



---

recommended that NNSA's leaders prioritize actions to strengthen NNSA's security culture and integrate security into its other missions, in addition to developing the security road map and other priority recommendations.

Furthermore, some NNSA officials or contractors commented that the absence of a clear vision or path forward may have exacerbated a difficult period for NNSA's security program since the Y-12 breach, which some of the NNSA officials have described as "chaotic" or "dysfunctional." During this period, top officials left NNSA or transferred to other positions, including the NNSA Administrator and the DNS Chief, to be replaced, in some cases, by a succession of officials acting in those positions. Field office officials and contractors at several sites told us that communication with, and direction from, headquarters became far less frequent after the security breach, although the officials were able to continue carrying out or overseeing their sites' security programs. Other NNSA security officials said that the leadership changes have been disruptive and have lowered morale. Some of these same NNSA officials also said that NNSA has been without an effective headquarters security organization since the Y-12 breach and were skeptical that NNSA had found an effective organizational structure, even with the latest changes. Others, however, said that these changes may provide a better organizational structure with clearer lines of authority and accountability.

---

## Conclusions

Since Congress created NNSA more than 13 years ago, NNSA has made important progress in securing its sites and developing an NNSA-wide security program. However, its efforts to-date have not prevented several serious security incidents, and NNSA has struggled to balance its security risks with concerns over costs and other needs, such as improved productivity. While legitimate, such concerns have at different times been allowed to drive its security management and oversight approach with limited quantifiable data on the benefits achieved. In addition, some of the 2009 to 2012 reforms—perhaps, most notably, NNSA's implementation of "hands-off, eyes-on" oversight and HSS's pause in conducting independent security inspections—left sensitive sites with less federal oversight, and aspects of that oversight approach likely contributed to the July 2012 security breach at Y-12. Since the Y-12 breach, NNSA has initiated actions to improve its security performance and oversight, partly in response to recommendations from its own Security Task Force, but it did not carry out the task force's priority recommendation that NNSA develop a security road map, including a clear vision and path forward for its security program and an implementation strategy, including regular

---

monitoring, to help ensure that its actions will lead to sustainable solutions—a recommendation that mirrors effective practices we previously identified for successfully implementing and sustaining management improvement initiatives. Instead, two successive headquarters reorganizations of NNSA’s security office have essentially led NNSA back to the organization in place before the Y-12 breach. While the current reorganization effort may eventually lead to improvements in NNSA’s security performance and oversight, the goals for security appear to be less clearly defined and less focused than previous attempts at security reform. Furthermore, without first developing the recommended security road map, NNSA risks putting in place another short-lived and potentially ineffective response to security problems and prolonging, inadvertently, a difficult period for its security program.

---

## Recommendation for Executive Action

To help ensure NNSA’s actions to improve its security performance and oversight will be successfully implemented and sustained, we recommend that the Secretary of Energy direct the NNSA Administrator to develop and implement the NNSA security road map, including a clear vision and path forward for NNSA’s security program and an implementation strategy, including regular monitoring, to help ensure that its actions will lead to sustainable solutions.

---

## Agency Comments and Our Evaluation

We provided a draft of this product to DOE and NNSA for comment. NNSA’s comments are reproduced in appendix II. In these comments, NNSA agreed with our recommendation and stated that it has already initiated an effort to develop a security road map for NNSA, including a vision and path forward for its security program. NNSA estimated completing this effort by December 31, 2014. We find it encouraging that NNSA has already initiated an effort to develop a security road map. As NNSA moves forward in addressing our recommendation, it will be important for the agency to develop an implementation strategy for its road map, including regular monitoring. This is consistent with the 2012 recommendation of NNSA’s Security Task Force and will help NNSA implement its plan as intended. In addition to the NNSA comments reproduced in this report, both HSS and NNSA provided technical comments and corrections, which we have incorporated into the report, as appropriate.

---

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

If you or your staff members have any questions about this report, please contact me at (202) 512-3841 or [trimbled@gao.gov](mailto:trimbled@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 key contributions to this report are listed in appendix III.



David C. Trimble  
Director, Natural Resources and Environment

---

*List of Requesters*

The Honorable Fred Upton  
Chairman  
The Honorable Henry A. Waxman  
Ranking Member  
Committee on Energy and Commerce  
House of Representatives

The Honorable Tim Murphy  
Chairman  
The Honorable Diana DeGette  
Ranking Member  
Subcommittee on Oversight and Investigations  
Committee on Energy and Commerce  
House of Representatives

The Honorable Joe Barton  
House of Representatives

The Honorable Michael C. Burgess  
House of Representatives

---

# Appendix I: Key Changes from DOE Security Directives in NNSA's 2010 Policy Letters

---

As part of its 2009 to 2012 security reforms, the National Nuclear Security Administration (NNSA) issued two security-related Policy Letters on the control of classified information and physical protection of security interests in place of the Department of Energy's (DOE) directives on these topics.<sup>1</sup> NNSA issued the Policy Letters in July 2010 to improve efficiency by realigning security requirements that may be impeding its sites' productivity. Key changes from DOE's directives are in table 1. DOE's Office of Health, Safety and Security (HSS), which had developed the DOE directives that were later replaced by the Policy Letters, has frequently disagreed with NNSA that such changes were needed and expressed concerns that the Policy Letters may not always ensure adequate security protection. After the security breach in July 2012 at NNSA's Y-12 National Security Complex, NNSA initiated actions to rescind the Policy Letters and reinstate DOE's security directives.

---

<sup>1</sup>NNSA's policies included Policy Letter 70.2, *Physical Protection*, and 70.4, *Information Security*, which were approved in July 2010 and replaced, respectively, DOE M 470.4-2A, *Physical Protection Manual* (July 2009), and DOE M 470.4-4A, *Information Security Manual* (Jan. 2009). As part of its own reform effort, DOE subsequently canceled and replaced the manuals and other DOE directives with DOE Order 473.3, *Protection Program Operations* (June 2011) and Order 471.6, *Information Security* (June 2011). However, one section of DOE M 470.4-4A on technical surveillance countermeasures was retained as policy.

**Table 1: Key Changes from DOE Security Directives to the Security-Related Policy Letters NNSA Issued in 2010**

| <b>DOE requirements</b>   | <b>Changes to the DOE requirements in NNSA's security-related Policy Letters</b>   |
|---|--|
| Classified matter—including paper documents, electronic media, or other forms of classified information—may not be left unattended for extended periods, even in locked security areas.   | NNSA authorized sites to allow employees working in locked security areas to leave classified matter (“secret” level or below) unattended in these areas during the workday, without having to lock it in an approved storage container, before taking lunch, for example, or attending to other business.   |
| Sites’ capability to detect intrusion into “vault-type rooms”—which may house classified matter or special nuclear material—must be comprehensive, and intrusion detection equipment, such as alarms and motion sensors, must be tested thoroughly and often. | For classified matter, NNSA replaced “vault-type rooms” with “closed areas” in its policies—a concept NNSA said is used in national industrial security standards, which DOE has also recognized in some of its policies—and refocused the intrusion detection requirements on doors and other “credible pathways” of entry and exit. NNSA also allowed for less rigorous testing of detection equipment and provided more options for storing classified matter in already secured areas. |
| Certain classified, removable electronic media, such as “thumb” drives, must be tracked in an accountability system.  | NNSA eliminated this requirement for such matter classified at the “secret” level or below. Subsequently, DOE eliminated this requirement from its security directives, according to HSS officials, and was in the process of doing so when NNSA’s Policy Letters were being implemented.  |
| There must be accountability systems for locks and keys used in areas with varying levels of security risks, and site personnel must log in and out of secure areas, including areas where they normally work, among other things.                            | NNSA eliminated or modified these and other such requirements, for example, by eliminating requirements that keys for lower-risk facilities be tracked in an accountability system or by exempting staff who normally work in certain secure areas from needing to log in and out of those areas.  |

Sources: GAO analysis of DOE and NNSA data.

# Appendix II: Comments from the National Nuclear Security Administration



Department of Energy  
National Nuclear Security Administration  
Washington, DC 20585



May 20, 2014

Mr. David C. Trimble  
Director  
Natural Resources and Environment  
Government Accountability Office  
441 G Street  
Washington, DC 20548

Dear Mr. Trimble:

Thank you for the opportunity to review the Government Accountability Office (GAO) draft report titled "NUCLEAR SECURITY: National Nuclear Security Administration (NNSA) Should Establish a Clear Vision and Path Forward for Its Security Program, GAO-14-208." I understand the GAO began this review in response to a request from the House Committee on Energy and Commerce to examine: (1) Department of Energy (DOE), NNSA, and contractors' implementation of the 2009 to 2012 security reforms, including any benefits or drawbacks they identified for NNSA and its sites, and (2) NNSA's actions or plans to improve security performance and oversight after the Y-12 security breach.

GAO made one recommendation for NNSA Action to "develop and implement the NNSA security road map, including a clear vision and path forward for NNSA's security program and an implementation strategy, including regular monitoring, to help ensure that its actions will lead to sustainable solutions." NNSA agrees with the GAO's recommendation and has already initiated an effort to develop a security roadmap for NNSA which will clearly delineate the NNSA security vision and the path forward for the security program. The estimated completion date for this effort is December 31, 2014.

Technical and general comments for GAO's consideration to enhance the clarity and factual accuracy of the report have been provided under separate cover. If you have any questions regarding this response, please contact Dean Childs, Director, Audit Coordination and Internal Affairs, at (301) 903-1341.

Sincerely,

Frank G. Klotz  
Under Secretary for Nuclear Security  
Administrator, NNSA



---

# Appendix III: GAO Contact and Staff Acknowledgments

---

## GAO Contact

David C. Trimble, (202) 512-3841 or [trimbled@gao.gov](mailto:trimbled@gao.gov)

---

## Staff Acknowledgments

In addition to the contact named above, Jonathan Gill (Assistant Director), Nancy Kintner-Meyer, and Jeff Rueckhaus made key contributions to this report. Technical assistance was provided by Kevin Bray, Cynthia Norris, Steven Putansu, Dan Royer, and Kiki Theodoropoulos.



---

---

## 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 website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <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 website, <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.

---

## Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at [www.gao.gov](http://www.gao.gov).

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <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

Katherine Siggerud, Managing Director, [siggerudk@gao.gov](mailto:siggerudk@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

