



---

April 2017

# NUCLEAR SECURITY

## DOE Could Improve Aspects of Nuclear Security Reporting

# GAO Highlights

Highlights of [GAO-17-239](#), a report to congressional committees

## Why GAO Did This Study

DOE and NNSA operate sites with facilities holding special nuclear material that can be used to make nuclear weapons. The National Defense Authorization Act of 2014 requires the Secretary of Energy to submit to congressional committees a report detailing the status of security at sites holding key quantities of special nuclear material, along with a certification that the sites meet DOE's security standards and requirements by December 1 of each year. The law requires DOE's reports to include a similar report from NNSA. A report accompanying the legislation included a provision for GAO to evaluate these efforts. This report examines (1) the extent to which these DOE and NNSA reports meet the definition of quality information under federal internal control standards, and (2) any significant physical security challenges at sites that the reports or agency officials identified and the extent to which the agencies have addressed them. GAO reviewed the 2014 and 2015 reports and interviewed agency officials.

## What GAO Recommends

GAO recommends that DOE include more complete information in the reports, better align the review process and mandated deadlines, plan for infrastructure needs, and inform Congress of the reason for delays in implementing its June 2011 order and any identified vulnerabilities. DOE raised concerns with the first recommendation, generally agreed with the second and the third, and stated it had already implemented the fourth. In response, GAO modified the first recommendation and will assess DOE's implementation of the fourth.

View [GAO-17-239](#). For more information, contact Shelby S. Oakley at (202) 512-3841 or [oakleys@gao.gov](mailto:oakleys@gao.gov)

April 2017

## NUCLEAR SECURITY

### DOE Could Improve Aspects of Nuclear Security Reporting

#### What GAO Found

The Department of Energy's (DOE) and the National Nuclear Security Administration's (NNSA) annual reports for 2014 and 2015 on the security of nuclear facilities holding special nuclear material did not fully meet the definition of quality information under the federal internal control standards. These standards define quality information as appropriate, current, complete, accurate, accessible, and provided on a timely basis. GAO found that, in general, while the reports were based on current information and were accessible to Congress, they did not fully meet quality information standards because the reports:

- did not always contain complete information on the assessments used to support the agencies' certifications that sites are secure and
- were not provided to Congress in a timely manner.

For example, DOE's 2015 annual security report did not mention whether an important assessment was conducted at two of its four sites or include information regarding the date or outcome of the assessment at three of its four sites. NNSA's 2015 annual security report noted its sites conducted these assessments; however, it did not provide information regarding the date or outcome at one site. Without complete information on the assessments used to determine each site's overall security assessment, it was not always possible to determine the basis for the site security certification solely using the information contained in the reports. In addition, GAO found that DOE's and NNSA's annual 2014 and 2015 security reports were issued several months late. DOE officials told GAO the delay was partly due to the lengthy internal review process. DOE and NNSA stated that they would promptly report any serious security issues to Congress using means other than the annual security reports. When the reports are issued late, however, Congress may not routinely receive timely notice of issues so that it can take actions to improve sites' security.

GAO's review of the annual security status reports and interviews with agency officials indicated that DOE and NNSA share significant challenges that could affect their ability to maintain physical security at sites and certify them as secure. For example, security infrastructure, such as fences, alarms, and sensors, at many DOE and NNSA facilities is outdated and requires extensive maintenance to ensure proper functioning. NNSA is developing a physical security infrastructure plan to be issued in spring 2017, but DOE has not fully developed plans or estimated costs to address its needs. Additionally, DOE has not fully implemented a June 2011 order, which could result in some nuclear materials requiring additional security. GAO found that even though the order called for implementation plans within 6 months of its issuance, one DOE site, with the approval of the Deputy Secretary of Energy, will not have an implementation plan until 2018. Based on GAO's review and the comments of agency officials, neither the 2014 and 2015 security reports provided comprehensive risk and potential vulnerability information to Congress nor had these issues been communicated through other means.

---

# Contents

---

Letter		1
	Background	6
	DOE's and NNSA's 2014 and 2015 Annual Security Reports Did Not Fully Meet the Definition of Quality Information under the Federal Internal Control Standards	11
	Known Challenges Could Affect Some Sites' Physical Security, and DOE Could Take Additional Steps to Address Them	18
	Conclusions	22
	Recommendations for Executive Action	24
	Agency Comments and Our Evaluation	25
Appendix I	Comments from the Department of Energy and the National Nuclear Security Administration	30
Appendix II	GAO Contact and Staff Acknowledgments	35
Tables		
	Table 1: Extent to Which Assessments Used to Determine Each Site's Overall Security Assessment Are Reflected in DOE's and NNSA's Annual Security Reports	13
	Table 2: Required Completion Dates and Issue Dates for DOE's and NNSA's 2014 and 2015 Reports on the Security of Facilities Containing Category I and Category II Special Nuclear Material	16
Figure		
	Figure 1: Examples of Mission Activities at Department of Energy (DOE) and National Nuclear Security Administration (NNSA) Sites with Category I and Category II Special Nuclear Material	7

---

---

### **Abbreviations List**

DOE Department of Energy  
NNSA National Nuclear Security Administration  
OMB Office of Management and Budget

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.



April 11, 2017

Congressional Committees

The Department of Energy (DOE) and its National Nuclear Security Administration (NNSA) are responsible for protecting special nuclear material, including plutonium and highly enriched uranium, which can be used in nuclear weapons or to construct an improvised nuclear or radiological device.<sup>1</sup> A successful attempt by terrorists or others to steal, sabotage, or otherwise gain unauthorized access to special nuclear material could help them develop weapons that could be used against the United States. The security of DOE and NNSA facilities that store and process special nuclear material has raised concerns, particularly after a serious security incident in 2012 in which three trespassers gained unauthorized access to the protected area of NNSA's Y-12 National Security Complex in Oak Ridge, Tennessee. This incident led to a 2-week stand-down of that site's operations. According to DOE's Inspector General, the security incident was unprecedented and represented multiple system failures, including failures to maintain critical security equipment, respond properly to alarms, and understand security protocols.<sup>2</sup> In addition, in a fiscal year 2017 report, DOE's Office of Inspector General listed safety and security as one of the most significant management challenges the department faces.<sup>3</sup>

DOE classifies special nuclear material into categories according to its risk, threat, and consequence potential for direct use in producing a significant nuclear yield or the production of a device that could do so. When in specified forms and quantities, category I special nuclear material represents the highest level of consequence for misuse and loss, is of high strategic significance, and must be protected from theft, unauthorized use, diversion, or sabotage. Category II, the next highest

---

<sup>1</sup>NNSA is a separately organized agency within the Department of Energy. Special nuclear material includes plutonium and uranium enriched in the isotope 233 or in the isotope 235.

<sup>2</sup>Department of Energy, Office of Inspector General, *Inquiry into the Security Breach at the National Nuclear Security Administration's Y-12 National Security Complex*, DOE/IG-0868 (Washington, D.C.: Aug. 29, 2012).

<sup>3</sup>Department of Energy, Office of Inspector General, *Management Challenges at the Department of Energy—Fiscal Year 2017*, OIG-SR-17-02 (Washington, D.C.: Nov. 16, 2016).

---

level of consequence, is of moderate strategic significance because it could be, among other things, combined, or “rolled up,” to category I quantities. Other categories of nuclear material represent lower levels of consequence; they are not, by themselves, capable of producing a nuclear yield but must be secured to prevent theft or the accumulation of category I quantities, among other things.

DOE and NNSA, working through contractors, each manage four sites that have a number of facilities that store or process category I and category II special nuclear material. DOE’s four sites are managed by its Office of Environmental Management within the Office of Management and Performance, which is led by the Under Secretary for Management and Performance, as well as by its Office of Science and its Office of Nuclear Energy, which are both led by the Under Secretary for Science and Energy. NNSA, which is led by the Under Secretary for Nuclear Security, who also serves as the Administrator, manages its four sites.

DOE’s Office of the Associate Under Secretary for Environment, Health, Safety, and Security is responsible for comprehensive security policy for DOE and NNSA.<sup>4</sup> In addition, DOE’s Office of Enterprise Assessments, which reports directly to the Secretary of Energy, manages an independent oversight program for safety and security at DOE and NNSA sites.

In December 2013, Congress passed the National Defense Authorization Act of 2014.<sup>5</sup> The act, as amended, requires the Administrator of NNSA to, by September 30 of each year, submit to the Secretary of Energy a report detailing the status of security at NNSA facilities holding category I and category II quantities of special nuclear material, and provide written certification that the facilities are secure and meet DOE’s and NNSA’s security standards and requirements. In addition, the act requires the Secretary of Energy to submit to the congressional defense committees a report detailing the status of security at DOE’s atomic energy defense facilities holding category I and category II special nuclear material, and provide written certification that the facilities are secure and meet DOE’s

---

<sup>4</sup>NNSA has a separate Office of Defense Nuclear Security, which develops and implements NNSA programs to protect, control, and account for material, facilities, and information at its sites.

<sup>5</sup>Pub. L. No. 113-66, § 3121, 127 Stat. 672.

---

security standards and requirements by December 1 of each year.<sup>6</sup> DOE is also to submit the unaltered report from NNSA at the same time. According to the law, if the Secretary or Administrator is unable to make the required written certification, they shall submit corrective action plans describing the deficiency resulting in being unable to make the certification, actions to be taken to correct the deficiency, and timelines for taking such action. The Secretary of Energy submitted DOE's and NNSA's annual security reports for 2014 and 2015 and certified in the reports that all relevant facilities are secure.<sup>7</sup>

The Senate Armed Services Committee report accompanying the National Defense Authorization Act for Fiscal Year 2014 included a provision for us to review and report on DOE and NNSA efforts related to the security of special nuclear material.<sup>8</sup> This report examines (1) the extent to which DOE's and NNSA's annual reports on the security of sites holding category I or category II special nuclear material meet the definition of quality information under federal internal control standards, and (2) any significant physical security challenges at these sites that the reports or DOE or NNSA officials identified, and the extent to which DOE and NNSA have addressed these challenges.<sup>9</sup>

---

<sup>6</sup>According to DOE, two of its non-NNSA sites are recognized as being "atomic energy defense facilities." These officials said that, for information completeness, DOE's reports include assessments of its other two non-NNSA sites containing category I and category II special nuclear material, which are not classified as atomic energy defense facilities.

<sup>7</sup>DOE provided its and NNSA's 2016 reports to Congress in January 2017 after we had completed audit work and delivered our draft report to the agencies for comment; therefore, we could not include an analysis of them for this report. We note the law does not specify a reporting period for the annual security reports. Officials from DOE's Office of Environment, Health, Safety, and Security and its Office of Environmental Management stated that, should an important matter arise toward the end of a certain year's annual security report development process, they would make every effort to include it in that year's report to Congress. To date, the reports issued by DOE and NNSA have been classified.

<sup>8</sup>S. Rep. No. 113-44 (2013).

<sup>9</sup>DOE is required to report on "atomic energy defense facilities" with category I and II special nuclear material. The law does not define "atomic energy defense facilities." However, under DOE Order 470.4B, a facility consists of one or more security interests under a single security management authority and a single facility security officer within a defined boundary that encompasses all the security assets at that location. A site consists of one or more facilities operating under a centralized security management, including a site security officer with consolidated authority and responsibility for the facilities. While a site may thus contain one or more facilities, DOE and NNSA report at the site level (e.g., Los Alamos National Laboratory).

---

To examine the extent to which DOE's and NNSA's annual reports on the security of sites holding category I or category II special nuclear material meet the definition of quality information contained in the information and communication standard under the federal internal control standards, we analyzed the act to determine the reporting requirements for DOE and NNSA and analyzed the content of DOE's and NNSA's 2014 and 2015 reports as compared with the definition. Federal internal control standards promulgated in 1999 were in effect until October 1, 2015, and contained a standard related to information and communication.<sup>10</sup> This standard stated that for an entity to run and control its operations, it must have relevant, reliable, and timely communications related to internal as well as external events. Federal internal control standards issued in 2014 and in effect as of October 1, 2015, define quality information under the information and communication standard as being appropriate, current, complete, accurate, accessible, and provided on a timely basis.<sup>11</sup> The 1999 federal internal control standards were in effect when NNSA and DOE completed reports in response to the December 1, 2014, and September 30, 2014, reporting requirements. However, DOE and NNSA completed reports in response to the December 1, 2015, and September 30, 2015, requirements after the revised federal internal control standards took effect in October 2015. Given that the 2014 and 2015 annual security reports were completed when different internal control standards applied, for ease of comparison between the reports, we applied the current, 2014, internal control standards to both reports. Further, we applied the 2014 internal control standards as they are the applicable standards moving forward, and DOE and NNSA have an annual requirement to provide the security reports to Congress. A federal control standard related to timeliness was in effect under the 1999 standards and is currently included in the internal control standards effective in October 2015. In addition, we obtained and reviewed DOE's order regarding its Safeguards and Security Program, which establishes DOE security program planning and management requirements.<sup>12</sup> We developed a data collection instrument to obtain information on the scope and currency of physical security information that was incorporated into the annual

---

<sup>10</sup>GAO, *Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: November 1999).

<sup>11</sup>GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: September 2014).

<sup>12</sup>Department of Energy, *Administrative Change to DOE O 470.4B, Safeguards and Security Program*, DOE Order 470.4B Change 1 (Washington, D.C.: Feb. 15, 2013).



---

security reports from DOE and NNSA program offices that operate the relevant sites. The information we requested included dates of the sites' most recent security plans, vulnerability assessments, and independent assessments by the Office of Enterprise Assessments. We relied on information contained in the annual security reports as well as on testimonial evidence from DOE and NNSA officials on the reporting of these dates, as well as on the extent to which site-level physical security measures may satisfy DOE's current and expected requirements and standards for nuclear material control and accountability or physical security. We did not independently review and verify whether site responses and the resulting reports were accurate.

To examine any significant physical security challenges at these sites and the extent to which DOE and NNSA have addressed these challenges, we reviewed the annual security reports and interviewed DOE and NNSA officials to identify any concerns about security challenges at their sites with category I or category II nuclear material. We reviewed DOE orders and documents that may affect DOE's and NNSA's standards and requirements for physical security, including DOE's design basis threat order, which specifies the potential size and capabilities of adversary forces against which the sites must defend; its nuclear material control and accountability order; and its order for its physical security program.<sup>13</sup> In addition, we interviewed DOE and NNSA officials to determine how the November 2016 design basis threat order may affect physical security arrangements at specific facilities at DOE and NNSA sites. We also interviewed DOE and NNSA officials to determine how the agencies have responded to any identified challenges. We compared this information with other relevant work, including leading practices for capital planning contained in GAO's *Executive Guide* and OMB's *Capital Programming Guide*.<sup>14</sup>

---

<sup>13</sup>The design basis threat order is a classified document. On November 23, 2016, DOE signed and issued the order. See Department of Energy, *Design Basis Threat Order*, DOE Order 470.3C (Washington, D.C.: Nov. 23, 2016). Department of Energy, *Nuclear Material Control and Accountability*, DOE Order 474.2 (Washington, D.C.: June 27, 2011). This order has been updated, most recently in September 2016. Both the original and updated orders required implementation plans within 6 months of the orders' issuance. For DOE's order for its physical security program, see *Administrative Change to DOE O 470.4B, Safeguards and Security Program*.

<sup>14</sup>GAO, *Executive Guide: Leading Practices in Capital Decision-Making*, [GAO/AIMD-99-32](#) (Washington, D.C.: December 1998) and Office of Management and Budget, *Capital Programming Guide, Supplement to Office of Management and Budget Circular A-11, Part 7: Planning, Budgeting, and Acquisition of Capital Assets* (Washington, D.C.: June 2006).

---

We conducted this performance audit from April 2016 to April 2017 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

This section provides information on key DOE and NNSA nuclear sites, key DOE security concepts and processes, and DOE and NNSA processes to develop their annual security reports.

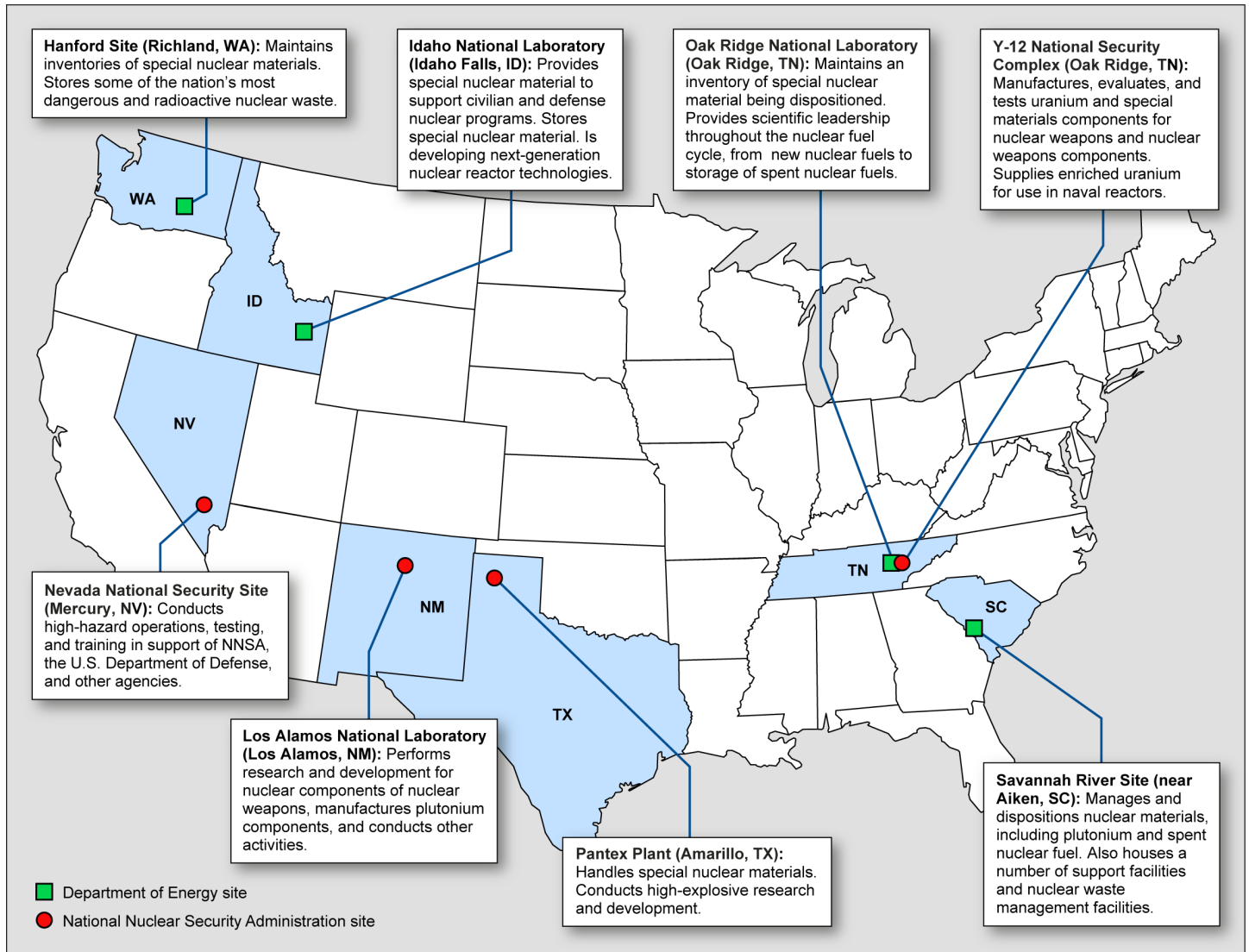
### Key DOE and NNSA Nuclear Sites, Locations, and Purpose

There are four DOE and four NNSA sites holding category I and category II special nuclear material to carry out the agencies' nuclear missions: DOE's Hanford Site, Idaho National Laboratory, Oak Ridge National Laboratory, and Savannah River Site and NNSA's Los Alamos National Laboratory, Nevada National Security Site, Pantex Plant, and Y-12 National Security Complex. DOE's Under Secretary for Management and Performance, DOE's Under Secretary for Science and Energy, and NNSA's Administrator are to ensure that each of the sites they manage has a safeguards and security program with the necessary protections to protect security interests against malevolent acts such as theft; diversion; sabotage; compromise; or unauthorized access to nuclear weapons, nuclear weapons components, or special nuclear material.<sup>15</sup> Figure 1 provides information on the missions of DOE and NNSA sites containing category I and category II special nuclear material.

---

<sup>15</sup>DOE's Office of Environmental Management, which operates two relevant sites, reports to the Under Secretary for Management and Performance.

**Figure 1: Examples of Mission Activities at Department of Energy (DOE) and National Nuclear Security Administration (NNSA) Sites with Category I and Category II Special Nuclear Material**



Sources: DOE, NNSA, Map Resources (map). | GAO-17-239

Note: Special nuclear material is material that can be used for nuclear weapons or to construct an improvised nuclear or radiological device. Special nuclear material includes plutonium and uranium enriched in the isotope 233 or in the isotope 235.

---

## Key DOE Security Concepts and Processes

DOE orders establish requirements that must be met for all DOE and NNSA operations except under certain conditions, with appropriate approvals.<sup>16</sup> DOE's overall risk-based security directive is contained in *DOE Order 470.4B, Safeguards and Security Program*, and was updated in February 2013, and most recently in January 2017.<sup>17</sup> A key component of DOE's approach to security is the design basis threat order, a classified document that identifies the characteristics of the potential threats to DOE and NNSA assets.<sup>18</sup> The design basis threat order is based on a classified, multiagency intelligence community assessment of potential terrorist threats.

DOE and NNSA counter the terrorist threat specified in the design basis threat order with a multifaceted protective system. All protective systems at DOE's and NNSA's most sensitive sites employ a defense-in-depth concept with 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. The protection strategy also includes personnel security, information security, and material control and accountability elements. According to the *DOE Standard: Nuclear Materials Control and Accountability*, a material control and accountability program is to ensure that all accountable nuclear materials are in their authorized location and are being used for their intended

---

<sup>16</sup>DOE directives, including orders, are the primary means to establish, communicate, and institutionalize policies, requirements, and procedures for multiple departmental elements, including NNSA. The NNSA Administrator has the authority to establish NNSA-specific policies, known as policy letters, unless disapproved by the Secretary of Energy. From 2009 until 2012, NNSA issued two such policy letters on the protection of classified information and on physical security, to include special nuclear material. Following the July 2012 Y-12 security incident, however, NNSA initiated actions to rescind these policy letters and reinstate DOE security directives. NNSA is in the process of completing these actions.

<sup>17</sup>*Administrative Change to DOE O 470.4B, Safeguards and Security Program*, and Department of Energy, *Minor Change to DOE Order 470.4B, Safeguards and Security Program*, DOE Order 470.4B Chg 2 (Washington, D.C.: Jan. 17, 2017).

<sup>18</sup>DOE signed the new order on November 23, 2016. See Department of Energy, *Design Basis Threat Order*, DOE Order 470.3C (Washington, D.C.: prepared Feb. 17, 2016, approved Nov. 23, 2016). This order replaced what was known as the graded security protection policy, which had been in effect since 2008. See Department of Energy, *Graded Security Protection (GSP) Policy*, DOE Order 470.3B (Washington, D.C.: Aug. 12, 2008). Since September 11, 2001, DOE security policies have been under frequent examination and have undergone considerable change. For example, DOE issued updated design basis threat orders in 2003, 2004, 2005, and 2008. Since DOE issued its revised design basis threat order in November 2016, for the purposes of this report, we will refer to the policies as the design basis threat order throughout.

---

purposes such that single component failures will not result in significant vulnerabilities.<sup>19</sup> These various security measures typically include physical security features and systems, such as integrated cameras, alarms, and motion sensors; fences and anti-vehicle barriers; and numerous access control points, such as turnstiles, badge readers, and vehicle inspection stations. At most sites, these measures are integrated into perimeter intrusion detection systems. Each site generally has a heavily armed protective force that is often equipped with such items as automatic weapons, night vision equipment, body armor, and chemical protective gear. In addition, each site is to follow a specific protection strategy based on the type of special nuclear material it must protect.<sup>20</sup>

According to NNSA officials, the performance of protective systems is to be formally and regularly examined through vulnerability assessments, which are systematic risk-based evaluations in which qualitative and quantitative techniques are applied to detect vulnerabilities and determine how to effectively protect specific assets, such as special nuclear material.

The results of the vulnerability assessments, other performance assessments, and expert analysis are to be used to establish the specific security measures, equipment, and requirements for a site, which are to be documented at each site in a classified security plan. In addition to identifying known vulnerabilities, risks, and protection strategies for mitigating these risks and vulnerabilities for the site, the plan formally acknowledges how much residual risk DOE is willing to accept. For more than 2 decades, DOE has employed a risk-based approach to security that seeks to direct resources to its most critical assets—in this case category I special nuclear material—and mitigate risks to these assets to an acceptable level. According to DOE officials, levels of risk—high, medium, and low—are assigned classified numerical values and are derived from a mathematical equation that compares a terrorist group's capabilities with the overall effectiveness of the crucial elements of the site's protective forces and systems.

---

<sup>19</sup>Department of Energy, *DOE Standard: Nuclear Materials Control and Accountability*, DOE-STD-1194-2011 Change 3 (Washington, D.C.: October 2013).

<sup>20</sup>Department of Energy, *Protection Program Operations*, DOE Order 473.3A (Washington, D.C.: Mar. 23, 2016).

---

---

## Overview of DOE and NNSA Processes to Develop Annual Security Reports

Through a variety of complementary inspections and assessments, DOE ensures that its contractors are implementing its safeguards and security policies and that its systems are performing as intended. Contractors perform regular self-assessments. DOE's safeguards and security order also requires relevant security offices to comprehensively survey contractors' operations for safeguards and security regularly. In addition, DOE's Office of Enterprise Assessments is to conduct independent assessments that appraise, among other things, DOE and NNSA physical security systems, personnel security, protective forces, and nuclear material control and accountability practices to identify gaps and vulnerabilities. According to DOE Office of Enterprise Assessments officials, they assess security at DOE and NNSA category I sites about every 2 years.

In general, DOE and NNSA have employed similar processes to develop and produce their annual security reports. DOE's Office of the Associate Under Secretary for Environment, Health, Safety, and Security and NNSA's Office of Security Operations and Performance Assurance within the Office of the Associate Administrator for Defense Nuclear Security coordinate each agency's report development effort. According to DOE and NNSA officials in those offices, in the summer of each calendar year the agencies request information from sites containing category I or category II special nuclear material. The agencies give their sites about 3 weeks to respond to these requests and to provide the requested documentation.<sup>21</sup> Officials said that once the responses are received, DOE Office of Environment, Health, Safety, and Security and NNSA Office of Defense Nuclear Security officials synthesize the relevant sites' responses and respectively develop the DOE and NNSA draft reports, which then are submitted for review by General Counsel and the relevant Under Secretaries, including the NNSA Administrator. NNSA then sends its report to DOE for transmittal, and the Secretary of Energy transmits both reports to Congress, along with his certification.

---

<sup>21</sup>Officials said that, in practice, DOE sites compile and send information to their relevant program office, which reviews the information. The program offices then send the information to the Office of Environment, Health, Safety, and Security.

---

## DOE's and NNSA's 2014 and 2015 Annual Security Reports Did Not Fully Meet the Definition of Quality Information under the Federal Internal Control Standards

DOE's and NNSA's 2014 and 2015 Annual Security Reports Were Based on Current Information and Were Accessible

DOE's and NNSA's 2014 and 2015 annual reports on the security of nuclear facilities holding category I and category II quantities of special nuclear material did not fully meet the definition of quality information in the 2014 federal internal control standards.<sup>22</sup> Under the 2014 federal standards for internal control, management should use quality information to achieve the entity's objectives. The information and communication standard defines quality information as appropriate, current, complete, accurate, accessible, and provided on a timely basis.<sup>23</sup> DOE's and NNSA's reports met certain aspects of the definition of quality information in that they were based on current information and were accessible. However, the reports did not always contain complete information on the important assessments that the agencies used in their certification of sites' security. Moreover, they were not provided in a timely manner as called for by both the 1999 and 2014 federal internal control standards.

We found that, in general, the 2014 and 2015 annual security reports—in which DOE and NNSA certified that their sites met current security requirements and standards—partially met the definition of quality information in the 2014 federal standards for internal control in that they were based on what was currently available information at the time they were prepared. For example, DOE and NNSA attested through responses to our data collection instrument that their assessments were based on the most current reviews of a site's security plan, vulnerability assessments, security surveys, and independent assessments that were available when the reports were being drafted. Moreover, DOE and NNSA officials told us that the agencies prepare their annual security reports by drawing on existing and well-established DOE processes for verifying the adequacy of security at facilities, such as formally approved security plans and independent assessments. With respect to being

---

<sup>22</sup>As noted earlier, the 1999 federal internal control standards in effect until October 1, 2015, stated that for an entity to run and control its operations, it must have relevant, reliable, and timely communications related to internal as well as external events. These standards were in effect when NNSA and DOE completed reports in response to the December 1, 2014, and September 30, 2014, reporting requirements. However, DOE and NNSA completed reports in response to the December 1, 2015, and September 30, 2015, requirements after the 2014 revised federal internal control standards took effect in October 2015. Given that the 2014 and 2015 annual security reports were conducted when different internal control standards applied, we applied the current, 2014, internal control standards to both reports for ease of comparison. Further, we applied the 2014 internal control standards as they are the applicable standards moving forward, and DOE and NNSA have an annual requirement to provide the security reports to Congress.

<sup>23</sup>[GAO-14-704G](#).

---

DOE's and NNSA's 2014 and 2015 Annual Security Reports Did Not Always Contain Complete Information on the Important Assessments Used to Certify Sites' Security

---

accessible, we verified that NNSA provided its annual security reports to DOE, and DOE provided both agencies' reports to the appropriate congressional committees. While the reports are classified and thus not publicly available, DOE delivered the reports to the respective committees' security offices, where they were available to recipients with the appropriate clearances and need to know.<sup>24</sup> In addition, a DOE official provided us with evidence that DOE had briefed congressional staff on the reports.

We found that DOE's and NNSA's 2014 and 2015 annual security reports did not always meet the definition of quality information as called for in the 2014 federal internal control standards because they did not always contain complete information that provided the basis for the agencies' certifications in the reports that sites are secure. Generally, we found that NNSA's reports included information on a wider range of individual site security assessments than did DOE's reports. However, neither DOE's nor NNSA's reports contained complete information to support the agencies' assessments that all of the relevant sites were secure. For example, DOE's 2015 annual security report did not mention whether a vulnerability assessment was conducted at two of its four sites or include any information regarding the date or outcome of the most recent vulnerability assessments at three of its four sites. NNSA's 2015 annual security report noted that its four sites conducted vulnerability assessments, but one site did not provide information regarding the most recent completion date of its vulnerability assessment. Table 1 indicates the extent to which DOE's and NNSA's reports contained complete information regarding the important assessments—security plans, vulnerability assessments, independent assessments, and other assessments—that officials said were used to certify that sites are secure.

---

<sup>24</sup>According to the *National Industrial Security Program Operating Manual* published by DOE and other federal agencies, "need to know" is a determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, or knowledge or possession of, certain classified information in order to perform tasks or services essential to the fulfillment of an official government program.



**Table 1: Extent to Which Assessments Used to Determine Each Site’s Overall Security Assessment Are Reflected in DOE’s and NNSA’s Annual Security Reports**

**2014 Reports**

Agency	Site	Security plan	Vulnerability assessment	Independent assessment by DOE’s Office of Enterprise Assessment	Other assessment measures
DOE	Hanford Site (Richland, WA)	○	○	◐	◐
DOE	Savannah River Site (near Aiken, SC)	○	◐	○	○
DOE	Idaho National Laboratory (Idaho Falls, ID)	○	○	○	○
DOE	Oak Ridge National Laboratory (Oak Ridge, TN)	○	●	◐	◐
NNSA	Los Alamos National Laboratory (Los Alamos, NM)	●	◐	●	●
NNSA	Nevada National Security Site (Mercury, NV)	●	◐	●	●
NNSA	Pantex Plant (Amarillo, TX)	◐	○	●	●
NNSA	Y-12 National Security Complex (Oak Ridge, TN)	●	●	●	◐

**2015 Reports**

DOE	Hanford Site (Richland, WA)	●	●	◐	◐
DOE	Savannah River Site (near Aiken, SC)	○	○	●	◐
DOE	Idaho National Laboratory (Idaho Falls, ID)	○	◐	○	◐
DOE	Oak Ridge National Laboratory (Oak Ridge, TN)	○	◐	○	◐

Agency	Site	Security plan	Vulnerability assessment	Independent assessment by DOE's Office of Enterprise Assessment	Other assessment measures
<b>2015 Reports</b>					
NNSA	Los Alamos National Laboratory (Los Alamos, NM)	○	●	●	○
NNSA	Nevada National Security Site (Mercury, NV)	●	●	●	○
NNSA	Pantex Plant Amarillo, TX	●	○	●	●
NNSA	Y-12 National Security Complex (Oak Ridge, TN)	●	●	●	●

● = Agency's annual security report mentions this assessment and provides details regarding the assessment measure. (For "other assessment measures," this symbol denotes that the report mentions at least one other assessment measure, such as a site self-assessment, contractor self-assessment, or site office survey, and that the report provides further details, such as the number of self-inspections that a contractor conducted during a given period.)

○ = Agency's annual security report mentions this assessment but does not provide details regarding the key assessment measure, such as the date the site security plan was most recently updated or the month and year that a vulnerability assessment was most recently conducted. (For "other assessment measures," this symbol denotes that the report mentions at least one other assessment measure but does not provide further details regarding the measure.)

○ = Agency's annual security report does not mention this assessment, nor does it provide details regarding the outcome of the key assessment measure, such as the date the site security plan was most recently updated or the month and year that a vulnerability assessment was most recently conducted. (For "other assessment measures," this symbol denotes that the report does not mention another type of assessment measure.)

DOE = Department of Energy

NNSA = National Nuclear Security Administration

Source: GAO analysis of DOE and NNSA data. | GAO-17-239

Note: According to NNSA officials, DOE sites are required to demonstrate that their protective systems are capable of defending special nuclear material against certain terrorist forces through a variety of assessments. The performance of protective systems is to be formally and regularly examined through vulnerability assessments—that is, systematic risk-based evaluations in which qualitative and quantitative techniques are applied to detect vulnerabilities and determine the effective protection of specific assets, such as special nuclear material. A site's security plan is a classified document that identifies a site's vulnerabilities, risks, and protection strategies and formally acknowledges how much risk DOE is willing to accept. An independent assessment is an independent appraisal by DOE's Office of Enterprise Assessment of, among other things, DOE and NNSA physical security systems, personnel systems, protective forces, and nuclear material control and accountability practices to identify gaps and vulnerabilities in security at DOE and NNSA sites.

In general, without complete information on the assessments—that is, security plans, vulnerability assessments, independent assessments, and other assessments—that officials said were used to determine each site's overall security assessment, it was not always possible to determine the basis for the site security certification solely using the information contained in the reports. To better understand the basis for the agencies' certifications that relevant sites were secure, we requested and were provided additional information from relevant DOE and NNSA sites regarding key dates for assessments, including dates for a site's most recent security plan, most recent vulnerability assessment, and last independent assessment by the Office of Enterprise Assessments. We

---

found that all this information was available for all the DOE and NNSA sites covered in our review.

As noted earlier, to develop the reports, DOE and NNSA request information from sites on, among other things, the outcomes of site-level assessments, such as site vulnerability assessments and independent assessments. According to NNSA documentation, the information NNSA requested included:

- a summary of the state of security at the relevant category I or category II site;
- a summary listing of the equivalencies and exemptions in place for DOE security orders at the site; and
- a description of the most recent site security plan and vulnerability assessment; results of inspections, such as independent assessments, by DOE's Office of Enterprise Assessments and contractor self-assessments; and descriptions of any vulnerabilities or challenges the site identified that might hamper its ability to certify it is secure at present or in coming years.

A DOE Office of Corporate Security Strategy official told us that, unlike NNSA, DOE does not use a standard data request to solicit information from its sites. Instead, a DOE Office of Environment, Health, Safety and Security official stated that each program office requests essentially the same information from its respective sites, as detailed above in the NNSA request.

DOE Office of Environment, Health, Safety and Security and NNSA officials told us that responses by sites to these requests varied in terms of the types of information and level of detail provided. This may contribute to the variation of information contained in the report for each site. In addition, according to DOE officials, the draft report was more detailed in the first internal draft and modified to adjust to the recommended report size and level of detail by the DOE Executive Secretariat templates and standards. However, DOE officials from the Office of Environment, Health, Safety, and Security stated that the final level of detail provided in the annual security reports is consistent with the law. These and other DOE officials stated that although the annual security reports may not always contain all the specific details of the information used to inform the Secretary's security certification, DOE's assessment of security is based on a wide array of data and information from the sites and from headquarters. The officials also stated that report

preparers had access to such sources of information at the time they developed the report content. These officials stated that including all these sources in the report would be overwhelming and would distract from the substantial issues important to ensure the continued security of special nuclear material. Nonetheless, DOE officials also acknowledged the desirability of incorporating greater detail in order to create a greater degree of transparency. Furthermore, they said that DOE is open to exploring ways of expanding the level of detail and transparency in future reports. For example, DOE Office of Environmental Management officials suggested that DOE include a bibliography in its reports to list the sources it consulted while developing them.

With such additional detail available in the reports, users of the report would be more readily able to determine if DOE's certification that its sites are secure is based on current and complete information. Additional detail would also provide better evidence that similar complete information was assessed across the DOE and NNSA sites to make the certifications, and it would be more consistent with DOE's mandate to submit reports that detail the status of security of atomic energy defense facilities holding category I and category II quantities of special nuclear material.

**DOE's and NNSA's 2014 and 2015 Reports Were Not Provided in a Timely Manner**

We further found that DOE's and NNSA's annual security reports for 2014 and 2015 were not provided in a timely manner as called for by both the 1999 and 2014 federal internal control standards. To date, neither agency has met the mandated deadlines for submitting the reports. The Administrator of NNSA is required to provide NNSA's report to DOE by September 30, and the Secretary of Energy is required to submit NNSA's and DOE's reports to Congress by December 1 of each year. Table 2 lists the required completion date for the 2014 and 2015 yearly report and, where available, the month and year each report was provided to the relevant entity.

**Table 2: Required Completion Dates and Issue Dates for DOE's and NNSA's 2014 and 2015 Reports on the Security of Facilities Containing Category I and Category II Special Nuclear Material**

Agency	Required completion date	Month and year provided to relevant entity <sup>a</sup>
DOE, 2014 report	December 1, 2014	September 2015
NNSA, 2014 report	September 30, 2014	November 2014 <sup>b</sup>
DOE, 2015 report	December 1, 2015	July 2016 <sup>c</sup>
NNSA, 2015 report	September 30, 2015	March 2016

Note: The annual security reports are required under 50 U.S.C. § 2657, which directs the Secretary of Energy to submit to the congressional defense committees a report detailing the status of security at atomic energy defense facilities holding category I and category II special nuclear material, along with written certification that the facilities meet DOE's security standards and requirements by December 1 of each year. In addition, DOE must submit a similar report from NNSA. The law does not specify a reporting period for the annual security reports. DOE Office of Environment, Health, Safety, and Security and Office of Environmental Management officials told us that should an important matter arise toward the end of a certain year's annual security report development process, they would make every effort to include it in that year's report to Congress.

<sup>a</sup>For NNSA, the relevant entity is DOE. For DOE, the relevant entity is the congressional defense committees.

<sup>b</sup>The cover of NNSA's 2014 annual security report listed October 2014 as its publication date. However, according to information NNSA provided, the report was provided to DOE in November 2014.

<sup>c</sup>The cover of DOE's 2015 annual security report listed March 2016 as its publication date. However, according to DOE officials, the report was provided to Congress in July 2016.

DOE and NNSA officials told us the 2014 and 2015 reports were issued late in part because the requirement did not provide guidance on the information that should be contained in the report. As a result, the agencies struggled internally to determine the content of the reports in response to the requirement to report and certify the security of DOE and NNSA sites. In addition, lengthy internal review times also contributed to delays in issuance. For example, DOE officials stated that the 2014 and 2015 DOE annual security reports were substantially drafted, and contained virtually all of what would become the final submitted content, by mid-October of the reporting year but were delayed by the internal review process. The officials stated that, despite the delay, the lengthy internal review process served some good in that it provided substantial opportunity for multiple DOE managers and organizations to engage with the content of the reports. DOE and NNSA officials said that they were working on improving the timeliness of the reports and noted that the 2016 reports had been submitted to Congress on a more timely basis.

When the reports are issued late, Congress may not receive information detailing identified deficiencies and corrective actions that the agencies are taking or are planning to take to address such deficiencies in a timely fashion. DOE officials told us that they would promptly report any serious security issues to Congress using means other than the annual security reports. In addition, officials said any problems would be immediately addressed by employing compensatory measures, which are generally temporary because of their high cost. However, agency officials acknowledged it may take the agencies several years to secure the

---

funding necessary to implement long-term solutions to the problems.<sup>25</sup> For example, a DOE Office of Science and Nuclear Energy official stated that funding for problems identified in the fall of 2016 would not be reflected in the budget cycle until fiscal year 2019 because the department would have already largely developed its fiscal year 2018 budget request. By continuing to focus on better aligning the internal review process and report publication deadlines, DOE and NNSA could help ensure that Congress routinely receives timely notice of any deficiencies to enable it to take actions to improve sites' security.

---

## Known Challenges Could Affect Some Sites' Physical Security, and DOE Could Take Additional Steps to Address Them

The annual security reports and our interviews with agency officials indicate the agencies have identified challenges that could affect physical security at some NNSA and DOE sites but that DOE has not completed plans to address these challenges. More specifically, DOE and NNSA share two significant challenges that could affect their abilities to maintain physical security and certify sites holding category I and category II special nuclear material as secure, and DOE faces an additional challenge. The shared challenges are (1) fully analyzing and meeting security requirements contained in the new design basis threat order, a classified document issued in November 2016 that specifies the potential size and capabilities of adversary forces that the sites must defend against, and (2) maintaining and updating aging physical security infrastructure.<sup>26</sup> The additional challenge for DOE is to complete implementation of a 2011 order for nuclear material control and accountability. DOE officials told us they believe that the DOE annual security reports have made a significant positive contribution by highlighting these key challenges and served a valuable function in identifying emerging concerns.

Concerning the first shared challenge, DOE's and NNSA's annual security reports and officials at the agencies noted that the issuance of a new design basis threat order presents a challenge to most sites because it will require significant time and resources for officials to fully analyze and meet the new requirements and possibly drive new or different

---

<sup>25</sup>Compensatory measures are designed to address security shortcomings, such as deploying protective forces in areas where equipment is not fully operational.

<sup>26</sup>In November 2016, DOE signed and issued a new design basis threat order that supersedes the 2008 Graded Security Protection Policy. See *Design Basis Threat Order*, DOE Order 470.3C, and Department of Energy, *Graded Security Protection Policy*, DOE Order 470.3B (Washington, D.C.: Aug. 12, 2008).

---

security requirements for some facilities and materials. Agency officials told us it may take 2 or more years to plan for and make the necessary changes to security at sites in response to the recently issued design basis threat order.<sup>27</sup> For example, they said that each site plans to conduct new vulnerability assessments and develop and validate a new security plan in response to the new design basis threat order.<sup>28</sup> Further, DOE officials confirmed that it may take several years to develop the justification and obtain resources for these changes. According to DOE officials, DOE and NNSA sites are required by the 2016 design basis threat order, within 180 days of approval, to either inform the cognizant Under Secretary that the site is in compliance with the order or submit a timeline to develop an implementation plan.

Concerning the second shared challenge, DOE's and NNSA's annual security reports and officials at the agencies noted that the physical security infrastructure at many DOE and NNSA facilities is outdated and requires extensive continued maintenance to ensure proper functioning. This outdated infrastructure includes perimeter intrusion detection and assessment systems and alarm stations, which are important components of DOE's defense-in-depth concept. According to agency officials and documents, addressing such upgrades could require significant time and funding. While this challenge is shared by both DOE and NNSA sites, NNSA is in the process of developing a security infrastructure plan, as required by law, that will outline and prioritize the costs and time frames necessary to address physical security challenges at its sites.<sup>29</sup> Such a plan is to provide the basis for NNSA to request the additional funds necessary to address physical security infrastructure challenges at its sites. NNSA in March 2017 projected it may need more than \$1 billion over the next 10 years to upgrade essential security

---

<sup>27</sup>Office of Environmental Management officials told us that DOE's briefing package regarding the forthcoming design basis threat order has been using 3 to 5 years for the anticipated implementation period.

<sup>28</sup>Office of Environmental Management officials told us that the new design basis threat (DBT) policy is a substantial update to the previous threat policy, and will be a significant undertaking to implement. However, the impacts to Office of Environmental Management's Category I or Category II special nuclear material facilities will not be nearly as significant as at other DOE assets, these officials stated.

<sup>29</sup>50 U.S.C. § 2453(b)(5).

---

infrastructure.<sup>30</sup> DOE officials told us they do not have a similar requirement to develop a physical security infrastructure plan and that, while several of their sites face significant physical security issues related to aging infrastructure, they have not fully developed plans that would allow them to prioritize decisions based on infrastructure needs or estimated costs to address those needs.<sup>31</sup> One DOE site has attempted to address its challenges and minimize its investment in physical security infrastructure needs by disposition of its special nuclear material into other forms or by transferring it to other sites, but it has been delayed in doing so. Specifically, as we reported in July 2005, Oak Ridge National Laboratory originally planned to dispose of its category I special nuclear material by 2014; however, DOE officials we interviewed for this review told us that this disposition has been delayed until 2023, and funding constraints could delay the date until 2027.<sup>32</sup>

Although DOE sites are in various stages of addressing physical security infrastructure challenges, without a DOE physical security infrastructure plan to address these issues across sites, including major projects, expected costs, and time frames, DOE officials and Congress will not have a comprehensive view of the challenge, and the future security of DOE sites holding category I and category II special nuclear material may be compromised. We have previously identified leading practices for making capital planning and investment decisions, drawn primarily from GAO's *Executive Guide and OMB's Capital Programming Guide*.<sup>33</sup> These leading practices include undertaking a comprehensive needs

---

<sup>30</sup>As we previously found in May 2016, NNSA has initiated a process that is specifically designed to meet the requirements for a Security Infrastructure Plan. NNSA officials said that they expect to complete this plan in the spring of 2017. Further, NNSA will begin to include this plan and its costs in its long-range planning and budgeting documents—its Future Years Nuclear Security Program and its Stockpile Stewardship Management Plan—in fiscal year 2018. See GAO, *Nuclear Security: Status of the National Nuclear Security Administration's Effort to Develop a Security Infrastructure Plan*, [GAO-16-447R](#) (Washington, D.C.: May 13, 2016).

<sup>31</sup>Office of Environmental Management officials stated that DOE had requested, and received, \$10 million under its fiscal year 2015 appropriation to address certain critical infrastructure needs at the Savannah River Site.

<sup>32</sup>GAO, *Nuclear Security: DOE's Office of 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). DOE had originally planned to convert the category I special nuclear material and downgrade the security of the site but now plans to move the category I special nuclear material to certain NNSA sites.

<sup>33</sup>[GAO/AIMD-99-32](#) and *Capital Programming Guide*.



---

assessment to determine immediate requirements as well as future needs, and developing a long-term capital plan.<sup>34</sup> Further, OMB capital planning and budgeting guidance to executive agencies emphasizes that when planning and budgeting for infrastructure asset investments, agencies should consider the full costs of ownership over the life of an asset, to include a life-cycle assessment of a project's initial costs as well as the longer-term costs for maintenance, operation, and disposal.

Concerning the additional challenge for DOE, the June 2011 nuclear material control and accountability order update required sites to develop implementation plans within 6 months of its issuance, including timelines and resources needed to implement the order and a description of the vulnerabilities and impacts created by any delayed implementation of the requirements. According to *DOE Standard: Nuclear Materials Control and Accountability*, each site or facility operator needs to establish a sustainable, effective graded safeguards program for the control and accounting of nuclear materials to detect and deter theft and diversion, and to prevent the unauthorized control of a weapon, test device, or materials that can be used to make an improvised nuclear device.<sup>35</sup> Material control and accountability programs are to ensure that all accountable nuclear materials are in their authorized location and are being used for their intended purpose such that single component failures will not result in significant vulnerabilities. According to DOE, an effective and efficient material control and accountability program is based on the consequences of the loss or misuse of nuclear materials. Although the new order was issued in 2011, DOE officials told us that the security strategy at two sites changed in 2015, which resulted in new implementation plans in 2016. Officials stated that both sites are currently undertaking implementation activities, which should be complete by the middle of 2017. With respect to the third site, in 2014 the Deputy Secretary of Energy, citing other more pressing security concerns at the site, approved the delayed completion of the site's implementation strategy and plan until 2018. DOE officials said that full implementation of the order at this site could result in the need for additional and potentially costly security measures to mitigate potential vulnerabilities. They also

---

<sup>34</sup>We have found that such a plan should cover 5 years or more and should reflect decision makers' priorities for the future, among other things. See GAO, *Federal Buildings Fund: Improved Transparency and Long-Term Plan Needed to Clarify Capital Funding Priorities*, [GAO-12-646](#) (Washington, D.C.: July 12, 2012).

<sup>35</sup>*DOE Standard: Nuclear Materials Control and Accountability*.

---

said that even when plans for this site are complete, implementing them will likely take many years.<sup>36</sup>

The full implications of DOE's delay in completing plans and implementing security strategies associated with the June 2011 order have not been fully determined. For example, sites may have to recategorize nuclear material from category II to category I as a result of implementing the order, and would then be potentially responsible for funding and implementing additional measures to ensure that those nuclear materials are protected at a higher level as detailed in DOE's Safeguards and Security Program. The 2011 order required sites to develop implementation plans within 6 months. Further, according to the order, if implementation of all requirements under a site's implementation plan was not possible within 6 months of the order's issuance, sites were supposed to document any requirements that could not be implemented within 6 months of the effective date of the order or within existing resources and submit to the relevant program officers and relevant Under Secretaries. According to the order, this documentation was to include timelines and resources needed to implement the order, and a description of the vulnerabilities and impacts created by the delayed implementation of the requirements. DOE officials told us that although the 2014 and 2015 DOE annual security reports discussed this issue, neither report fully conveyed the potential seriousness of it nor had any of the detailed information—timelines and resources needed to implement the 2011 order, and a description of the vulnerabilities and impacts created by the delayed implementation of the requirements of the order—been communicated to Congress through the reports or through other means. Our review of the 2014 and 2015 reports confirmed that the discussion of this issue had been limited. DOE officials said they believe that the 2016 report provides a more detailed discussion of the issue.<sup>37</sup> Because all required implementation plans have not been developed, nor have they been fully implemented, DOE may have unaddressed security risks.

---

## Conclusions

Special nuclear material could be used by terrorists to make a nuclear weapon or to construct an improvised nuclear or radiological device, and

---

<sup>36</sup>According to DOE officials, the fourth DOE site did not complete an implementation plan because it was compliant with the order at the time of its issuance in June 2011.

<sup>37</sup>DOE provided its and NNSA's 2016 reports to Congress in January 2017 after we had completed audit work and delivered our draft report to the agencies for comment; therefore, we could not include an analysis of them for this report.

---

protecting this material is vital to our national security. The serious security incident at the Y-12 National Security Complex in 2012 demonstrated unacceptable security problems at one site but also raised questions about the security of other DOE and NNSA sites that hold category I and category II special nuclear material. As a result of increased scrutiny and at the direction of Congress, DOE and NNSA officials examined the security of their category I and II special nuclear material sites and certified in their 2014 and 2015 reports that they were secure. Officials of both agencies said that they have improved their process for producing the reports over time and are open to incorporating other improvements. In addition, DOE and NNSA officials told us they believe that the annual security reports have made a significant positive contribution by highlighting key security challenges. We found that while annual reports were based on current information and were accessible, they were not always complete in terms of the assessments—security plans, vulnerability assessments, independent assessments, and other assessments—used to support the agencies’ assertions that all of the relevant sites were secure. In addition, the reports have not been provided in a timely manner, in part because of a lengthy internal review process. Providing more complete information would allow Congress to better determine whether DOE’s and NNSA’s certification that their sites are secure is based on complete and current information. Additional information in the reports would also provide better evidence that similar information was assessed across the DOE and NNSA sites to make the certifications. Further, providing additional information would be more consistent with DOE’s mandate to submit reports that detail the status of security of facilities holding category I and category II special nuclear material. In addition, delays in issuing the reports may in turn affect congressional efforts to address any issues identified in the reports. While DOE and NNSA have made some progress in providing Congress with reports in a timelier fashion, by continuing to focus on better aligning the internal review process and mandated deadlines, DOE and NNSA further ensure that Congress receives timely notice of any deficiencies to enable it to take actions to improve sites’ security.

The quality of information contained in the reports is increasingly important as DOE and NNSA communicate significant challenges that could affect their ability to certify that their category I and II facilities holding special nuclear material are secure. For example, DOE and NNSA share the common challenge of an aging physical security infrastructure at some sites. While NNSA is currently developing a plan that will identify the cost of, and time frames for, addressing the physical security infrastructure challenges at its sites, DOE has not done so.

---

Without a similar DOE physical security infrastructure plan that would allow the agency to prioritize decisions based on infrastructure needs, DOE officials and Congress will not have a comprehensive view of the challenge, and the future security of DOE sites holding category I and category II special nuclear material may be compromised. DOE also faces a long-standing challenge in planning for and implementing a June 2011 nuclear material control and accountability order. DOE officials told us that although the 2014 and 2015 annual security reports discussed this issue, neither of the reports fully conveyed the potential seriousness of it. DOE officials said that their 2016 annual security report provides a more detailed discussion of the issue. Because all required implementation plans have not been developed, nor have they been fully implemented, DOE may have unaddressed security risks.

---

## Recommendations for Executive Action

We are making four recommendations in this report.

We recommend that the Secretary of Energy, working with the Administrator of the National Nuclear Security Administration, take the following two actions.

- Include more complete information on the assessments—that is, security plans, vulnerability assessments, independent assessments, and other assessments—used in the annual reports to support the agencies' assessments that DOE and NNSA sites are secure.
- Better align the internal review process and mandated report publication deadlines.

Additionally, we recommend that the Secretary of Energy take the following two actions.

- Develop a plan for addressing the physical security infrastructure needs at DOE sites. Similar to a report under development by NNSA, this plan could identify cost and time frames and enable DOE and the Congress to prioritize these projects.
- In future annual security certification reports, inform Congress of the reasons for the delayed implementation of the June 2011 DOE material control and accountability order at some sites, as well as the steps DOE and its sites are taking to implement it. DOE should also provide Congress with information on any vulnerabilities or deficiencies in the security at sites that may potentially exist while the sites complete implementation of the order as well as information on any concomitant adjustment to their security posture that is required.

---

## Agency Comments and Our Evaluation

We provided DOE and NNSA a draft of this report for comment. DOE and NNSA provided a coordinated written response, which is reproduced in appendix I. In the comments, which DOE transmitted, DOE raised concerns about the first finding and recommendation, stated it accepted the second, agreed with the third, and said it had already implemented the fourth, as discussed below. DOE and NNSA also provided technical comments, which we incorporated as appropriate.

In overarching comments, DOE stated that some statements in the draft report inaccurately imply that DOE and NNSA annual reports do not meet OMB Circular A-123 (A-123) federal internal control standards and that the assessments are not supported by documentation of internal control assessments, and that these statements should be removed from the report. DOE, in its comment letter, states that the department has a robust, A-123 compliant internal control program under which rigorous annual internal control testing is conducted by all DOE program offices and sites. We acknowledge the agency's point as we did not review DOE's annual process for conducting internal control assessments and have deleted any mention of A-123 from the report.

In commenting on our recommendations, DOE stated that our first recommendation about the need to include more complete information in the annual security reports would be more beneficial if it were rewritten to use only the congressional language of the fiscal year 2014 NDAA in evaluating what the report should do. DOE stated that it was also concerned by the assertions that the level of detail in the 2014 and 2015 reports was insufficient to meet the legislative requirement for the Secretary of Energy to certify that nuclear materials are secure, that the relevant security standards and requirements are being met, and that any existing deficiencies have been acknowledged and corrective actions outlined. DOE also stated that the legislative intent of this requirement was to produce an executive level summary report. DOE suggested that it would be more appropriate for us to assess the reports against the intent of the legislative requirement contained in the NDAA. DOE also stated the agencies' security certifications were based on recent information and were well-founded.

As noted earlier, the Senate Armed Services Committee report accompanying the National Defense Authorization Act for Fiscal Year 2014 included a provision for us to review and report on DOE and NNSA efforts related to the security of special nuclear material; this provision did not require us to assess the legal sufficiency of DOE's reports, nor did it confine us to focusing on compliance with legislative requirements. We do

---

not state that the agencies' reports fail to meet legislative requirements. However, we believe that the reports could be improved. As such, we stand by our analysis and believe that using the definition of quality information under federal internal controls standards is useful and appropriate criteria for assessing the 2014 and 2015 security reports. Furthermore, based on discussions with agency officials, we specified in our report and modified our recommendation to include exactly the kinds of assessment information—security plans, vulnerability assessments, independent assessments, and other assessments— DOE could consistently include in the reports that would make them more complete. Through our review, we verified that this information is readily available from each of the 8 sites.

In its letter, DOE stated that it is committed to strengthening the reports by providing more useful detail and is working with Congress to facilitate its efforts to do so. For example, in its letter DOE stated that, as a result of discussions with congressional committees, the National Defense Authorization Act for Fiscal Year 2017 amended the original legislative requirement to make certification requirements identical for DOE and NNSA, a change that DOE describes as a significant improvement to ensure consistency in certification across sites with category I and II special nuclear material. DOE also stated in its letter that it may consider development of a proposal to Congress regarding modification of the frequency of the current reporting requirement. When we met with agency officials in February 2017 to discuss the draft report, they suggested that a biennial reporting period would better align with important security assessment schedules and would assist in providing current and complete information on site security. We are encouraged by DOE's stated focus on efforts to improve the reports and their belief that such improvements would better help ensure consistency in certification across all the sites. We believe that implementing our recommendation to include more complete information in the reports would support these efforts.

DOE stated that it accepted our second recommendation about better aligning the internal review process and mandated report publication deadlines for annual security reports. DOE also notes, however, that the report suggests that the lack of timely reporting deprives the Secretary and Congress of information they need to act in response to potential deficiencies. DOE stated that the department and NNSA do not rely on the annual report to provide all levels of higher management with information about urgent issues the moment they are identified, but that they also interact with congressional staff across the gamut of security issues. This is acknowledged in our report, but we continue to believe that

---

when the reports are issued late, Congress may not receive information detailing identified deficiencies and corrective actions that the agencies are taking or are planning to take to address in a timely fashion. Our report also notes that because of the annual budget cycle, once a security problem is identified, it can take as many as two years before Congress can take actions, such as providing additional funding, to address the problem. Our report further describes how some of these actions can take many years and resources and sustained effort to implement. In its comments, DOE stated it has already accomplished significant improvement in the timeliness of its internal review process, as evidenced by the more timely completion of its 2016 annual security report. Our report acknowledges DOE's more timely submission of the 2016 reports. We continue to believe, however, that when reports are issued late, Congress may not routinely receive timely notice of issues so that it can take actions to improve sites' security.

DOE agreed with our recommendation about developing a plan for addressing the physical security infrastructure needs at DOE sites, which could identify cost and time frames and enable DOE and Congress to prioritize these projects. DOE stated that its Security Committee, which is responsible for developing security policy, has made this a priority and is developing strategies to resolve this and future enterprise-wide security concerns.

DOE stated it has already implemented our last recommendation to include in future annual security certification reports the reasons for the delayed implementation of the June 2011 order at some sites, as well as the steps DOE and its sites are taking to implement it and provide Congress with information on any vulnerabilities or deficiencies in the security at sites that may potentially exist while the sites complete implementation of the order as well as information on any concomitant adjustment to their security posture that is required. In its letter, DOE said its 2014 report provided a detailed narrative explanation of the rationale for the 2011 order change and an explanation of how its sites had initiated the process to determine potential security impacts. DOE further stated that its 2015 report summarized its evolving understanding of the impact of this issue, and that its 2016 report is even more explicit in characterizing the extent of potential problems and suggesting the shape of emerging solutions. DOE also said that its future reports would more clearly explain why implementation has extended over multiple years.

Our review of the 2014 and 2015 reports and the comments of agency officials interviewed during the course of our review, however, indicate

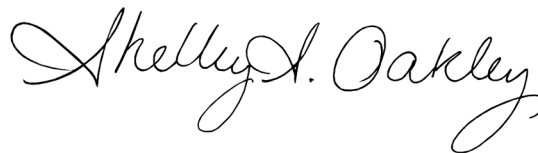
---

that neither of the reports fully conveyed the potential seriousness of the issue. In addition, neither report communicated to Congress the timelines and implementation resources needed and a description of the vulnerabilities and impacts created by the delayed implementation of the requirements of the order. As discussed earlier, DOE provided its and NNSA's 2016 reports to Congress in January 2017 after we had completed our audit work and delivered our draft report to the agencies for comment. As a result, we have not yet assessed DOE's position that the 2016 report, in combination with the 2014 and 2015 reports, addresses our fourth recommendation. We will assess DOE's efforts, including the 2016 report, as part of our monitoring of the implementation of these recommendations.

---

We are sending copies of this report to the appropriate congressional committees, the Secretary of Energy, the Administrator of the National Nuclear Security Administration, and other interested parties. In addition, the report is 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 [oakleys@gao.gov](mailto:oakleys@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 II.



Shelby S. Oakley  
Acting Director, Natural Resources and Environment



---

---

*List of Committees*

The Honorable John McCain  
Chairman  
The Honorable Jack Reed  
Ranking Member  
Committee on Armed Services  
United States Senate

The Honorable Lamar Alexander  
Chairman  
The Honorable Dianne Feinstein  
Ranking Member  
Subcommittee on Energy and Water Development  
Committee on Appropriations  
United States Senate

The Honorable Mac Thornberry  
Chairman  
The Honorable Adam Smith  
Ranking Member  
Committee on Armed Services  
House of Representatives

The Honorable Mike Simpson  
Chairman  
The Honorable Marcy Kaptur  
Ranking Member  
Subcommittee on Energy and Water Development,  
and Related Agencies  
Committee on Appropriations  
House of Representatives

# Appendix I: Comments from the Department of Energy and the National Nuclear Security Administration



Department of Energy  
Washington, DC 20585

March 17, 2017

Ms. Shelby Oakley, Acting Director  
Natural Resources and Environment  
U.S. Government Accountability Office  
441 G Street, NW  
Room 2T23A  
Washington, DC 20548

Dear Ms. Oakley:

This letter transmits the coordinated response from the U.S. Department of Energy (DOE) and the National Nuclear Security Administration (NNSA) to the January 19, 2017 Government Accountability Office (GAO) draft report, *GAO-17-239, NUCLEAR SECURITY: DOE Could Improve Aspects of Nuclear Security Reporting*. We appreciate the opportunity for comment on the draft report. Our comments are offered for consideration to enhance the factual accuracy of the report.

The GAO statements on pages 1, 4 and 11 of the draft report inaccurately imply the DOE and NNSA annual reports do not meet OMB Circular A-123 (A-123) Federal Internal Control Standards and that the assessments are not supported by documentation of internal control assessments. These statements should be removed from the report. DOE has a robust, A-123 compliant internal control program under which rigorous annual internal control testing is conducted by all DOE program offices and sites. Each office consolidates the results of the annual testing from across its sites and submits those results and an assurance statement from each office head to the Secretary that the office's internal controls are operating effectively.

Further, as indicated in the enclosed responses, the Department has interpreted the National Defense Authorization Act (NDAA) for Fiscal Year 2014 as calling for an executive level report, with the understanding that supplemental detail would be provided upon request. The DOE reports have been completed in accordance with the FY 14 NDAA language, and Congress has accepted each successive report as fulfilling its expectations.

DOE and NNSA have made process improvement a fundamental aspect of our overall annual report process. Each reporting cycle has included a robust internal after action review process, and, as a result, each successive report has improved upon its predecessor and has been delivered in a more timely manner—the 2016 report significantly so. In



---

**Appendix I: Comments from the Department of  
Energy and the National Nuclear Security  
Administration**

---

addition, DOE may consider development of a proposal regarding modification of the frequency of the current reporting requirement and, should it do so, would submit that proposal to Congress following appropriate procedures for submission of any such proposal.

As a result of discussions with the Congressional Committees, the 2017 NDAA amended the original legislative requirement to make certification requirements identical for both DOE and NNSA. This is a significant improvement that ensures consistency in certification across sites with Category I and II special nuclear material.

We are committed to improving our annual report process, and we understand that GAO supports us in our efforts to do so. We welcome their process improvement insights, while encouraging them forthrightly acknowledge the strengths evident in our current reports.

If you have any questions about our planned actions and improvement initiatives, please contact me at (202) 586-5175.

Sincerely,



Matthew Moury  
Associate Under Secretary  
For Environment, Health, Safety and Security  
Office of Environment, Health, Safety and Security

Attachment

**DOE Response to GAO Draft Report Recommendations  
NUCLEAR SECURITY: DOE Could Improve Aspects of Nuclear  
Security Reporting (GAO-17-239)**

DOE appreciates the insights offered in the draft GAO report; we have carefully considered them and offer the following overall response.

**Recommendation 1:** DOE and NNSA should ensure that the reports “include more complete, appropriately detailed, sufficient information in the annual reports to support the Secretary’s assessment that DOE and NNSA sites are secure.”

**DOE Response:** The GAO statements on pages 1, 4 and 11 of the draft report inaccurately imply the DOE and NNSA annual reports do not meet OMB Circular A-123 (A-123) Federal Internal Control Standards and that the assessments are not supported by documentation of internal control assessments. These statements should be removed from the report. DOE has a robust, A-123 compliant internal control program under which rigorous annual internal control testing is conducted by all DOE program offices and sites. Each office consolidates the results of the annual testing from across its sites and submits those results and an assurance statement from each office head to the Secretary that the office’s internal controls are operating effectively.

DOE is also concerned by the assertions (pages 11-18 of the GAO report) that the level of detail in the 2014 and 2015 reports was insufficient to meet the intent of the legislative requirement. Regardless of the specific wording of a particular report section, in every instance the DOE and NNSA certifications were based upon the most recent system reliability data for determining an acceptable level of security.

The original legislative language requires certification that nuclear materials are secure, that relevant security standards and requirements are being met, and that where deficiencies exist, they are acknowledged and corrective actions outlined. The Department has interpreted this legislative language as calling for an executive level summary report, with the understanding that supplemental detail would be provided upon request. Our reporting process has been conducted accordingly, and Congress has accepted each successive report as fulfilling its expectations. The GAO report would be substantially improved if it evaluated the DOE and NNSA reporting processes in accordance with the underlying statutory requirements in the language of the FY14 NDAA, rather than applying—in our view inappropriately—OMB Circular A-123 and the associated 1999 and 2014 versions of the Standards for Internal Control in the Federal Government. Our understanding is that these standards were designed and implemented in a different context (e.g., Federal Manager’s Financial Integrity Act) and for fundamentally different purposes. Consequently, we believe our security certifications have been well founded and their basis clearly articulated.

---

**Appendix I: Comments from the Department of Energy and the National Nuclear Security Administration**

---

We are committed to making each annual report better than the last and believe we will be able to with the recommended changes. In particular, our process improvement discussions have endeavored to find ways to strengthen the reports, not by simply providing more detail, but instead by providing more useful detail. In this, we see a convergence between our own goals and GAO's desires. For these reasons, we believe that the GAO report would be much more beneficial if Recommendation 1 was rewritten to, first, use only the Congressional language of the FY14 NDAA in evaluating what the report should do, and, second, explicitly endorse our proposed process improvements for the upcoming reports.

**Recommendation 2:** DOE and NNSA should "better align the internal review process with mandated report publication deadlines."

**DOE Response:** DOE accepts this recommendation, while noting that the submission date of the 2016 Annual Report provides *prima facie* evidence that DOE has already accomplished significant improvement in the timeliness of its internal review process. We remain committed to the proposition that deadlines are meant to be kept.

While we accept this recommendation, we also note that throughout the report GAO suggests that our lack of timeliness effectively deprives the Secretary and Congress of information they need to act in response to potential deficiencies. These suggestions apparently derive from a fundamental misunderstanding of the role of these annual reports in our overall process of communication. DOE and NNSA do not rely on the annual report to provide all levels of higher management with information about urgent issues the moment they are identified. We also interact with Congressional staff across the gamut of security issues, and we take our obligation seriously to directly report rapidly developing security concerns to Congress.

It is our understanding from Congress that the annual special nuclear material (SNM) report requirement was never intended to replace or obviate these essential and immediate communication paths; indeed, the very notion of an "annual" reporting requirement argues that the annual reports can only be a complement to these other paths. Instead, the annual reports are an exercise in line management accountability, the accountability of subordinate line managers to the Secretary and the accountability of the Secretary to Congress. By the time the reports are submitted to Congress, every level of responsible line management certified that SNM at its location is secure. We have embraced this requirement precisely because it compels a higher level of accountability, but this is not the process we employ to ensure that urgent needs or concerns are communicated in a timely manner as they occur.

**Recommendation 3:** The Secretary should "develop a plan for addressing the physical security infrastructure needs at DOE sites. Similar to a report under development by NNSA, this plan could identify cost and time frames and may enable DOE and the Congress to prioritize these projects."

---

**Appendix I: Comments from the Department of Energy and the National Nuclear Security Administration**

---

**DOE Response:** DOE agrees with this recommendation. The need for management involvement at the enterprise level strongly argues for an enterprise approach to depicting needs and developing priorities. Such an approach also offers potential benefits in terms of avoiding duplication of effort, leveraging commonly applicable solutions, and achieving acquisition economies of scale. DOE's Security Committee has made this a priority and is developing strategies to resolve this and future enterprise-wide security concerns.

DOE reiterates, program offices evaluate the need for additional physical security infrastructure or maintenance as part of each annual budget formulation process, and these are all funded in separate appropriations. NNSA is different because it can prioritize across the categories. The highest priority needs are funded in the Safeguards and Security budget.

**Recommendation 4:** The Secretary should "ensure that future annual security certification reports inform Congress of the reasons for the delayed implementation of the June 2011 DOE material control and accountability order at some sites as well as the steps the Department and its sites are taking to implement it, include granting exemptions to the order. DOE should also provide Congress with information on any vulnerabilities or deficiencies in the security at sites that may potentially exist while the sites complete implementation of the order and any concomitant adjustment to their security posture."

**DOE Response:** DOE has already implemented this recommendation. There have been multiple reasons for delayed implementation of the order, and these reasons vary from program to program and site to site. The 2014 report provided a detailed narrative explanation of the rationale for the 2011 order change and an explanation of how the sites had initiated the process of determining the extent to which this change would necessitate corresponding change in the physical protection afforded for certain materials at particular locations. The 2015 report summarized the evolving understanding of the impact of this issue, and the 2016 report is even more explicit in characterizing the extent of the potential problems and suggesting the shape of emerging solutions. The 2016 report reflects the maturation of the overall Departmental response to this complex and challenging issue. DOE will continue to discuss the implementation of the 2011 order in future reports will more clearly explain why implementation has extended over multiple years.

---

# Appendix II: GAO Contact and Staff Acknowledgments

---

## GAO Contact

Shelby S. Oakley, (202) 512-3841 or [oakleys@gao.gov](mailto:oakleys@gao.gov)

---

## Staff Acknowledgments

In addition to the individual named above, Jonathan Gill (Assistant Director), Antoinette Capaccio, Justin Fisher, Michelle Munn, and Cynthia Norris made key contributions to this report.

---

---

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's 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](#), [LinkedIn](#), [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) and read [The Watchblog](#).

---

## 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

---

## Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, [spel@gao.gov](mailto:spel@gao.gov), (202) 512-4707, U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548



Please Print on Recycled Paper.