



May 13, 2016

Congressional Committees

Nuclear Security: Status of the National Nuclear Security Administration's Effort to Develop a Security Infrastructure Plan

A successful attempt by terrorists or others to steal, sabotage, or gain unauthorized access to classified information or special nuclear material—including plutonium and highly enriched uranium—could harm U.S. national security.¹ Congress created the National Nuclear Security Administration (NNSA) in 2000 to, among other things, maintain and enhance the safety and reliability of the U.S. nuclear weapons stockpile.² NNSA—a semiautonomous agency within the Department of Energy (DOE)—seeks to ensure the security of classified information, nuclear weapons, and materials at its eight sites, collectively known as the nuclear security enterprise (enterprise). NNSA's sites include three national laboratories, four production plants, and the Nevada National Security Site.³ The condition of the enterprise's security infrastructure has been an area of concern in recent years. In 2012, NNSA found that a serious security incident in which three trespassers gained access to its Y-12 National Security Complex in Oak Ridge, Tennessee, resulted from, among other things, failure to maintain critical physical security infrastructure, such as cameras.

For nearly a decade, Congress has required NNSA to produce a Security Technology and Infrastructure Life-Cycle Management Plan (Security Infrastructure Plan). Specifically, since 2008, NNSA has been required to annually submit to Congress a plan for the research and development, deployment, and life cycle sustainment of the technologies employed within the enterprise to address physical security and cybersecurity threats during the upcoming 5-year fiscal period.^{4,5}

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

²Pub. L. No. 106-65, § 3211 (1999).

³NNSA oversees three national nuclear weapons design laboratories—Lawrence Livermore National Laboratory in California, Los Alamos National Laboratory in New Mexico, and Sandia National Laboratories in New Mexico and California. It also oversees four nuclear weapons production plants—the Pantex Plant in Texas, the Y-12 National Security Complex in Tennessee, the Kansas City Plant in Missouri, and tritium operations at DOE's Savannah River Site in South Carolina. NNSA also oversees the Nevada National Security Site, formerly known as the Nevada Test Site.

⁴The National Defense Authorization Act for Fiscal Year 2008, Pub. L. No. 110-181, § 3123 (2008), codified at 50 U.S.C. § 2453(b)(5). Office of Management and Budget 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 future costs for maintenance, operation, and disposal.

⁵More recently, in May 2015, the House Armed Services Committee directed the Administrator for Nuclear Security to provide a report to the defense committees by September 30, 2016, containing a 10-year plan to recapitalize the nuclear security enterprise's physical security systems. H.R. Rep. No. 114-102 (2015), accompanying a bill for the National Defense Authorization Act for Fiscal Year 2016. According to NNSA officials, NNSA plans to meet both its statutory requirement and this more recent direction with a single Security Infrastructure Plan.

All of NNSA's enterprise sites have physical security infrastructure to protect classified information. Four of these sites also protect Category I special nuclear materials, which may include nuclear weapons or nuclear materials, according to NNSA officials. Continued operations, especially nuclear operations, at NNSA sites depend on the successful performance of physical security systems and their integration with other security elements, such as security guard forces, known in NNSA as protective forces. NNSA's Office of Defense Nuclear Security (ODNS) is responsible for developing programs to protect, control, and account for materials, information, and facilities across the enterprise. In the last 3 years, NNSA's Defense Nuclear Security budget has totaled nearly \$2 billion, averaging approximately \$652 million annually. On average \$81 million was budgeted each year for maintaining and repairing physical security infrastructure. The remainder of the annual Defense Nuclear Security program funding was budgeted for activities such as information security, material control and accountability, and protective forces, with protective forces receiving an average of approximately \$390 million, or 60 percent of the security budget, each year.

NNSA develops several long-range planning and budget documents that provide information on security. For example, requested funding for NNSA security and its other programs are included in the agency's annual justification supporting the President's budget request. NNSA's Future Years Nuclear Security Program (FYNSP) provides program information and budget estimates for the next 5 fiscal years and is approved by the Office of Management and Budget.⁶ In addition, NNSA's Stockpile Stewardship and Management Plan (SSMP) provides information on modernization and operations plans and budget estimates over the next 25 years. NNSA sites also maintain 10 Year Site Plans, which are nonbinding planning documents and represent possible paths to support enterprise missions.

The Senate Armed Services Committee report accompanying the Senate version of the National Defense Authorization Act for Fiscal Year 2015 includes a provision for GAO to report on NNSA's effort to develop a Security Infrastructure Plan.⁷ Our report examines (1) the status of NNSA's efforts to develop a statutorily required Security Infrastructure Plan and (2) the extent to which NNSA's future physical security infrastructure needs are included in the agency's current budget and planning documents.

To determine the status of NNSA's efforts to develop a Security Infrastructure Plan, we examined past as well as current NNSA planning and management documents associated with physical security infrastructure. In addition, to determine the extent to which NNSA's future physical security infrastructure needs are reflected in the agency's current budget and planning documents, we analyzed a variety of documents, including the fiscal year 2016 and fiscal year 2017 justifications supporting the President's budget request and associated FYNSPs, the associated SSMP, and 10 Year Site Plans for NNSA's four sites that protect nuclear weapons or other Category I special nuclear material. We also interviewed NNSA officials, including ODNS officials responsible for developing a Security Infrastructure Plan, and interviewed supporting contractors responsible for planning and managing NNSA's physical security repairs and upgrades. We visited NNSA's Nevada National Security Site, which protects Category I special nuclear material. We interviewed NNSA site officials and contractors at the Nevada National

⁶NNSA is required to submit a FYNSP "at or about the time the President's budget is submitted to Congress." 50 U.S.C. § 2453.

⁷S. Rep. No. 113-176, at 283 (2014).

Security Site and the Y-12 National Security Complex, which also protects Category I special nuclear material, to help us determine the extent to which NNSA physical security management and planning documents are consistent with DOE and other generally accepted program life cycle management plan requirements. We selected these sites because each protects Category I special nuclear materials and has significant ongoing or planned physical infrastructure projects.

We conducted this performance audit from February 2015 to May 2016 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.

NNSA Has Not Yet Completed a Security Infrastructure Plan but Has Efforts Under Way to Do So

Although it has initiated several efforts, NNSA has not completed a Security Infrastructure Plan as required by law. Following enactment of the requirement in 2008, according to NNSA reports and officials, NNSA initiated planning efforts from 2009 through 2015 to assess physical security infrastructure needs, but these efforts either did not fully address the statutory requirement for a Security Infrastructure Plan or have yet to be completed. For example, in 2010 and 2011, NNSA submitted partial security infrastructure plans (titled Physical and Cyber Security Technology Management Plans) to Congress. However, according to agency officials, NNSA discontinued this effort after the 2011 report and focused on developing a comprehensive and statutorily compliant plan. Specifically, in 2009 ODNs tasked Sandia National Laboratories with assessing the known security needs at NNSA's sites and develop an enterprise-wide Physical Security Technology Management Plan. This plan called for collecting data on the technologies deployed and assessing the condition of physical infrastructure at all eight NNSA sites. However, according to an ODNs document, the information collected was not sufficiently detailed and comparable between NNSA sites and was therefore not useful in developing the required Security Infrastructure Plan.⁸ In 2013 NNSA instituted an effort to modernize physical infrastructure on a routine basis and to improve security at its sites. NNSA calls this effort the Physical Security Supplemental project. Through this project, NNSA intended to create a recurring, formal program document to help federal management ensure that security systems and infrastructure were consistent with NNSA-approved protection strategies and DOE requirements and that the systems were modern, adequately maintained, effective, and reliable. Though viewed as an important step, NNSA officials acknowledged that this project fell short of the Security Infrastructure Plan called for by law because it did not include all needed physical security infrastructure repairs, upgrades, and replacements, or the estimated total cost and schedule for executing such a plan.

Most recently, in May 2015 NNSA initiated the Enterprise Security Systems Assessment that according to NNSA officials, is specifically designed to meet the requirements for a Security Infrastructure Plan. NNSA officials said that they expect to complete this plan in December 2016. According to these officials, this plan will consider the scope of work identified through the Physical Security Supplemental project as well as some costs (additional repairs, upgrades, and

⁸Historically, we have found that comparing costs across sites is difficult because DOE and NNSA contractors use different methods for tracking costs. See GAO, *Modernizing the Nuclear Security Enterprise: The National Nuclear Security Administration's Proposed Acquisition Strategy Needs Further Clarification and Assessment*, [GAO-11-848](#) (Washington, D.C.: Sept. 20, 2011).

replacement of physical security infrastructure and associated supporting costs) that were excluded from that review. NNSA officials said they also believe that the new effort will probably identify additional needs. For example, at a number of enterprise sites, the fiber-optic communications cable and wiring necessary to support physical security systems need to be replaced or upgraded. NNSA is in the process of collecting the data that will be included in the plan. According to NNSA officials, the data collection for this effort was completed in February 2016, and NNSA is currently analyzing and prioritizing the physical security infrastructure needs to be included in this plan. NNSA will, according to agency officials, develop an overall Ten-Year Plan incorporating a cost and schedule estimate for the effort by December 2016. It will then incorporate cost and schedule estimates for repairing, upgrading, and replacing physical security infrastructure into the annual NNSA budget request and other long-range planning documents.

NNSA's Current Budget and Planning Documents Include Limited Information on Its Future Physical Security Needs

NNSA has recently begun to include some information on potential physical security infrastructure improvements in its current budget and planning documents. For example, NNSA's fiscal year 2017 budget request for Defense Nuclear Security notes that Congress provided an additional \$30 million in appropriations during fiscal year 2016 to improve physical security. According to the request, NNSA will use the fiscal year 2016 funding to meet immediate physical security needs, while developing a funding plan and list of prioritized upgrade projects to address security infrastructure in future years.⁹ The fiscal year 2017 budget request for Defense Nuclear Security also states that NNSA projects it may need more than \$2 billion over the next 15 years to upgrade essential security infrastructure. According to NNSA officials, this estimate includes approximately \$1.3 billion for major line-item capital acquisition projects at its Pantex Plant in Texas and at its Y-12 National Security Site in Tennessee, and an additional \$700 million for other required repairs and upgrades to physical security infrastructure that will be needed over the next 15 years.¹⁰ However, according to NNSA officials, specific cost and schedule information for these potential projects is not included in the fiscal year 2017 budget request or the associated FYNSP or SSMP.¹¹ In its fiscal year 2017 budget request for Defense Nuclear Security, NNSA requests an additional \$20 million for security and adds about \$141 million for security over the course of the current fiscal years 2017-2021 FYNSP. This represents about a 4 percent increase over the previous fiscal years 2016-2020 FYNSP.

⁹The explanatory statement accompanying the 2016 Consolidated Appropriations Act provides that \$30 million of the funds appropriated for Defense Nuclear Security shall be for a Security Improvements Program to address the backlog of needed security infrastructure upgrades. Section 4 of the Consolidated Appropriations Act, Pub. L. No. 114-113 (2015), provides that the explanatory statement printed in the House of Representatives section of the Congressional Record on December 17, 2015, by the Chairman of the House Committee on Appropriations, shall have the same effect with respect to the allocation of funds as if it were a joint explanatory statement of a committee of conference.

¹⁰According to NNSA officials, the major line-item capital acquisition projects include Areas 4 and 12 Perimeter Intrusion Detection and Surveillance Replacement Projects at the Pantex site and the Y-12 Security Area Boundary Enhancement and Reduction Project. Pantex areas 4 and 12 and Y-12 security areas conduct nuclear weapons-related activities, including storing, assembling, and disassembling weapons; conducting enriched uranium activities; producing uranium-related components for nuclear warheads and bombs; and processing nuclear fuel for the U.S. Navy.

¹¹The fiscal years 2017-2042 SSMP includes preliminary estimates for some security projects. However, based on our review it does not include them as part of a Security Infrastructure Plan.

According to NNSA officials, in fiscal year 2018 NNSA will begin to add more detailed estimates to the annual NNSA budget request and other long-range planning documents. Furthermore, according to agency officials, the fiscal year 2019 budget request and long-range planning documents will include the full details and costs of NNSA's Security Infrastructure Plan. If NNSA is unable to maintain its physical security infrastructure sufficiently to meet DOE and NNSA requirements, then, according to NNSA officials, the agency may have to initiate what NNSA calls compensatory measures. Compensatory measures are designed to address security shortcomings, such as deploying protective forces in areas where equipment is not fully operational, usually at a high cost, according to NNSA officials. According to the DOE Inspector General, this is already occurring to an extent. For example, an August 2015 Inspector General report on the security of the Y-12 site states that until deficiencies in aging infrastructure are addressed, the facility will continue to compensate for the deficiencies by using additional personnel at significant additional cost.¹²

We are not making new recommendations in this report. We recommended in December 2013 that NNSA include a range of budget estimates for preliminary projects and programs in its future modernization plans.¹³ NNSA does this for many of its future modernization projects and programs in its budget and planning documents, but NNSA has not done this for its potential physical security infrastructure needs. We continue to believe that providing Congress with budget estimates that reflect long-term plans and the expected funding needed to execute these plans, even if preliminary, helps in prioritizing projects and funding and aids in congressional decision making.

Agency Comments

We provided NNSA a draft of this report for review and comment. In written comments, which are reprinted in the enclosure, NNSA describes the ongoing Enterprise Security System Assessment. NNSA also provided technical comments that we incorporated as appropriate.

— — — —

We are sending copies of this report to the appropriate congressional committees, the Secretary of Energy, and other interested parties. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

¹²Department of Energy, Office of Inspector General, *Audit Report: Security Improvements at the Y-12 National Security Complex*, DOE/IG-0944 (Aug. 28, 2015).

¹³GAO, *Modernizing the Nuclear Security Enterprise: NNSA's Budget Estimates Do Not Fully Align with Plans*, [GAO-14-45](#) (Washington, D.C.: Dec. 11, 2013).

If you or your staff members have any questions concerning this report, please contact me at (202) 512-3841 or trimbled@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report were Jonathan Gill (Assistant Director), Richard Burkard, Greg Campbell, Ray Rodriguez, and Peter Ruedel.

A handwritten signature in black ink, reading "David C. Trimble". The signature is written in a cursive style with a large, stylized 'D' and 'T'.

David C. Trimble
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
Subcommittee on Energy and Water Development,
and Related Agencies
Committee on Appropriations
House of Representatives

Enclosure: Comments from the National Nuclear Security Administration



Department of Energy
Under Secretary for Nuclear Security
Administrator, National Nuclear Security Administration
Washington, DC 20585



May 3, 2016

Mr. David C. Trimble
Director, Natural Resources
and Environment
U.S. Government Accountability Office
Washington, DC 20548

Dear Mr. Trimble:

Thank you for the opportunity to review the Government Accountability Office's (GAO) draft report, "Nuclear Security: Status of the National Nuclear Security Administration's Effort to Develop a Security Infrastructure Plan" (GAO-16-447R). As noted in the report, we are in the process of conducting an Enterprise Security Systems Assessment. This review, along with supplemental quarterly reporting, will support production of an annual Security Technology and Infrastructure Life-Cycle Management Plan. It will also address the May 2015 House Armed Services Committee requirement for a 10-year recapitalization plan.

We appreciate the auditors' recognition of National Nuclear Security Administration's efforts, and will continue to pursue enhanced reporting in infrastructure plans and in our future budget materials. Technical and general comments have been provided under separate cover for your consideration in enhancing the clarity and accuracy of the report. If you have any questions, please contact Dean Childs, Director, Audits and Internal Affairs, at (301) 903-1341.

Sincerely,

A handwritten signature in black ink, reading "Frank G. Klotz", is positioned above the printed name.

Frank G. Klotz



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.

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 (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 www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

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

Congressional Relations

Katherine Siggerud, Managing Director, 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, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

