United States Government Accountability Office

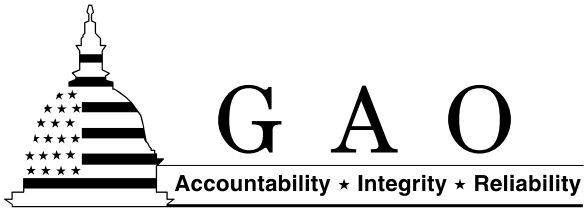
GAO

Report to the Subcommittee on Strategic Forces, Committee on Armed Services, House of Representatives

January 2007

NATIONAL NUCLEAR SECURITY ADMINISTRATION

Additional Actions Needed to Improve Management of the Nation's Nuclear Programs



GAO-07-36

January 2007

NATIONAL NUCLEAR SECURITY ADMINISTRATION

Additional Actions Needed to Improve Management of the Nation's Nuclear Programs

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-07-36, a report to the Subcommittee on Strategic Forces, Committee on Armed Services, House of Representatives

Why GAO Did This Study

In response to security and management weaknesses, in 1999 the Congress created the National Nuclear Security Administration (NNSA), a separately organized agency within the Department of Energy (DOE). NNSA is responsible for the nation's nuclear weapons, nonproliferation, and naval reactors programs. Since its creation, NNSA has continued to experience security problems, such as unauthorized access to a NNSA unclassified computer system, and cost and schedule overruns on its major projects, such as the National Ignition Facility. GAO reviewed the extent to which NNSA has taken steps to (1) improve security at its laboratories and plants and (2) improve its management practices and revise its organizational structure. To carry out its work, GAO reviewed legislation; NNSA policies, plans and budgets; and interviewed current and former NNSA and DOE officials.

What GAO Recommends

GAO is recommending that the Secretary of Energy and the Administrator, NNSA, (1) improve NNSA's security program, (2) develop and implement standard operating procedures for conducting business and resolving conflicts between DOE and NNSA, and (3) institute a series of initiatives to improve project, program, and financial management. NNSA generally agreed with the report's findings and corresponding recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-36.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gene Aloise at (202) 512-3841 or aloisee@gao.gov.

What GAO Found

Although NNSA has begun to build an effective security organization, it still cannot demonstrate that all of its security program objectives are being met at all of its sites. Specifically, the results of internal and independent security oversight assessments have identified weaknesses in physical security at several NNSA sites, including the Nevada Test Site, Sandia National Laboratories and the Y-12 National Security Complex, and weaknesses in cyber security throughout NNSA. The following factors have contributed to this situation:

- *Weak organization of headquarters security.* Until recently, NNSA did not have consistent leadership or direction at the headquarters level for its security program.
- *Security staffing shortages at NNSA site offices.* Since NNSA became operational, five of its six site offices have not been staffed at the required levels, according to GAO's analysis. Site offices oversee NNSA contractor security operations.
- *Inadequate security staff training.* NNSA has not implemented a training program that provides federal security officials with the skills needed to effectively oversee contractor security programs.
- *Incomplete security data.* DOE's database for tracking security deficiencies identified by security oversight assessments is incomplete, and, as a result, NNSA lacks a comprehensive understanding of the overall effectiveness of its security program.

NNSA has taken several actions to improve its management practices, including developing a planning, programming, budgeting and evaluation process. However, management problems continue, in part, because NNSA and DOE have not fully agreed on how NNSA should function within the department as a separately organized agency. This lack of agreement has resulted in organizational conflicts that have inhibited effective operations. GAO also identified the following areas where additional management improvements are needed:

- *Project management.* NNSA has not developed a project management policy, implemented a plan for improving its project management efforts, and fully shared project management lessons learned between its sites.
- *Program management.* NNSA has not identified all of its program managers and trained them to a certified level of competency.
- *Financial management.* NNSA has not established an independent analysis unit to review program budget proposals, confirm cost estimates, and analyze budget alternatives.

Contents

Abbreviations

DNS	Office of Defense Nuclear Security
DOD	Department of Defense
DOE	Department of Energy
FTE	full time equivalent
NIST	National Institute of Standards and Technology
NNSA	National Nuclear Security Administration
NSSP	Nuclear Safeguards and Security Program
OMB	Office of Management and Budget
PARS	Project Assessment and Reporting System
PPBE	planning, programming, budgeting, and evaluation process
SSIMS	Safeguards and Security Information Management System

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, D.C. 20548

January 19, 2007

The Honorable Ellen O. Tauscher
Chairman
The Honorable Terry Everett
Ranking Minority Member
Subcommittee on Strategic Forces
Committee on Armed Services
House of Representatives

During the late 1990s, the Department of Energy (DOE) experienced management difficulties with its nuclear weapons programs—particularly with the lack of clear management authority and responsibility—that contributed to security problems at the nation's nuclear weapons laboratories and significant cost overruns on major projects.[1] According to a June 1999 report by the President's Foreign Intelligence Advisory Board (the Board), DOE's management of the nuclear weapons laboratories, while representing "science at its best," also embodied "security at its worst" because of "organizational disarray, managerial neglect, and …a culture of arrogance."[2]

The Board urged the Congress to create a new organization to oversee the nuclear weapons complex and to insulate it from DOE. The Board stressed that the new organization, whether established as an independent agency or a semi-autonomous entity within DOE, should have a clear mission, streamlined bureaucracy, and drastically simplified lines of authority and accountability. Responding to the Board's recommendations, in 1999, the Congress created the National Nuclear Security Administration (NNSA) under Title 32 of the National Defense Authorization Act for Fiscal Year 2000—the NNSA Act—to correct the problems identified.[3]

[1]GAO, *National Nuclear Security Administration: Key Management Structure and Workforce Planning Issues Remain as NNSA Conducts Downsizing*, GAO-04-545, (Washington, D.C.: June 25, 2004).

[2]A special investigative panel, President's Foreign Intelligence Advisory Board, *Science at its Best, Security at its Worst: A Report on Security Problems at the U.S. Department of Energy* (Washington, D.C.: June 1999).

[3]Pub. L. No. 106-65, 113 Stat. 512, 953 (1999).

The NNSA Act established NNSA as a "separately organized agency" within DOE and made NNSA responsible for the management and security of the nation's nuclear weapons, nuclear nonproliferation, and naval reactor programs.[4] To implement its programs, NNSA relies on contractors to manage day-to-day site operations and to adhere to DOE policies when operating the laboratories, production plants, and other facilities within the complex. Because many NNSA sites handle special nuclear material, including nuclear weapons, plutonium, and highly enriched uranium, effective federal oversight is critical to ensuring that national security, human health and safety, and the environment are not harmed.

The NNSA Act also established the position of DOE Under Secretary for Nuclear Security, who was also designated as the Administrator of NNSA. The Secretary of Energy and the Deputy Secretary of Energy were allowed to establish policy for NNSA and to give direction to NNSA through the Administrator; however, other DOE employees were prohibited from directing the activities of individual NNSA employees. Furthermore, the NNSA Act established, within NNSA, deputy administrators for defense, nonproliferation, and naval reactors programs. Finally, the NNSA Act required that, among other things, NNSA develop a planning, programming, and budgeting process in order to ensure that the administration operated under sound financial management principles.

Since its inception, however, NNSA has continued to experience both security and overall management problems. For example, with respect to security, in 2003 we reported that NNSA had not been fully effective in managing its safeguards and security program.[5] Specifically, we found that NNSA had not fully defined the roles and responsibilities of officials in its security program and that NNSA had shortfalls in security staff at the site offices that oversee its contractors. In addition, two NNSA studies commissioned in July 2003 found ongoing problems with NNSA's security program, including weaknesses in its security culture, organization, and staffing and training.[6] Finally, DOE's Office of Inspector General found

[4]The Office of Naval Reactors is managed as a separate entity within NNSA reporting to both NNSA and the U.S. Navy.

[5]GAO, *Nuclear Security: NNSA Needs to Better Manage Its Safeguards and Security Program*, GAO-03-471 (Washington, D.C.: May 30, 2003).

[6]See *Strengthening NNSA Security Expertise: An Independent Analysis*, Henry G. Chiles et al., March 2004 and *NNSA Security: An Independent Review*, LMI Government Consulting, April 2005.

security problems with NNSA's contractors, including inadequate control of firearms inventories and improprieties in the testing of the officers who protect NNSA's sites. In terms of the management of major projects, the National Ignition Facility and the Dual Axis Radiographic Hydrodynamic Test Facility—two major facilities needed to support NNSA's nuclear weapons programs—experienced major delays and cost overruns because of problems with project management and are still not complete.[7]

To implement the NNSA Act and in response to these problems, NNSA has initiated a series of improvements, including recently creating a new NNSA headquarters unit to oversee security across the nuclear weapons complex; establishing a planning, programming, budgeting, and evaluation process; and putting in place a policy to improve program management. In addition, in December 2002, the Administrator reorganized NNSA. Specifically, the Administrator (1) removed a layer of management by abolishing NNSA's three operations offices located in New Mexico, Nevada, and California; (2) removed some functions from a fourth operations office at Oak Ridge, Tennessee, and established the Y-12 site office; (3) strengthened the oversight role of its site offices; (4) consolidated business and technical support functions, such as procurement and contracting, into a single "service center" organization located in Albuquerque, New Mexico; and (5) reduced NNSA's staff by about 17 percent by the end of fiscal year 2004.

In this context, you asked us to evaluate the extent to which NNSA has taken steps to (1) improve security at its laboratories and plants and (2) improve its management practices and revise its organizational structure.

To evaluate the extent to which NNSA has taken steps to improve security at its laboratories and plants, we reviewed the security requirements contained in DOE directives. We met with security officials from NNSA headquarters and the NNSA Service Center in Albuquerque; and at the Lawrence Livermore National Laboratory, Nevada Test Site, Sandia National Laboratories, Los Alamos National Laboratory, Pantex and Y-12 National Security Complex site offices. We also met with security contractor officials at the Livermore, Nevada, Sandia, Los Alamos, and Y-12, as well as with officials from DOE's Office of Health, Safety, and Security (formerly the Office of Security and Safety Performance

[7]See, for example, GAO, *National Ignition Facility: Management and Oversight Failures Caused Major Cost Overruns and Schedule Delays*, GAO/RCED-00-271 (Washington, D.C.: Aug. 8, 2000).

Assurance). In addition, we met with former DOE and NNSA officials, including the Director of NNSA's Security Workforce Panel, and the Director of the NNSA Security Panel. In reviewing the extent to which NNSA has taken steps to improve security at its laboratories and plants, we collected and analyzed performance ratings contained in security oversight reports, issued by DOE's Office of Health, Safety and Security and NNSA site offices, from fiscal years 1996 through 2005. We used these performance ratings because there was wide agreement among NNSA and DOE security officials that these ratings represented the best available information on the overall performance of NNSA's safeguards and security program. To assess the reliability of security oversight report ratings, we (1) reviewed existing information about the methodology and timeframes used in making performance rating determinations; (2) interviewed knowledgeable agency officials; and (3) based on document reviews, ensured that we had received all available performance information. We determined that the data were sufficiently reliable for the purposes of this report. We also used reports on NNSA's security efforts prepared by GAO, the DOE Inspector General, and outside groups, such as a 2005 report commissioned by NNSA.[8] To address the extent of security staffing shortfalls, we collected and analyzed staffing data provided by NNSA site offices. We relied primarily on staffing data from the NNSA site offices, as this data was the most comprehensive and because these offices are responsible for processing and managing security staffing requirements. To assess the reliability of these data, we interviewed NNSA security officials who were responsible for compiling these data and performed basic reasonableness checks of the data. We determined that the data were sufficiently reliable for the purposes of our report. Finally, we reviewed documents related to NNSA's efforts to improve the organization and operation of its security oversight program.

To evaluate the extent to which NNSA has taken steps to improve its management practices and revise its organizational structure, we reviewed the NNSA Act as well as two House of Representatives reports in 2000 on

[8]See *NNSA Security, An Independent Review*, LMI Government Consulting, Apr. 2005. This effort was directed by Admiral Richard W. Mies USN (Retired).

the act's implementation.[9] Because the establishment of NNSA as a separately organized agency in DOE was a key provision of the NNSA Act, we met with officials from NNSA headquarters; the NNSA Service Center; the NNSA site offices; and DOE offices where NNSA and DOE need to interact, including DOE's Office of Intelligence and Counterintelligence (formerly the Office of Counterintelligence), Chief Financial Officer, Chief Information Officer, General Counsel, and Human Capital Management. To understand how NNSA and DOE were intended to interact, we interviewed officials and reviewed documents, such as DOE's January 2000 implementation plan for NNSA. We also interviewed officials with the Department of Commerce's National Oceanic and Atmospheric Administration, the Defense Advanced Research Projects Agency, the Defense Threat Reduction Agency, and the Department of Transportation's Federal Aviation Administration to obtain their views on the reporting relationships that need to be in place for an entity designated as a "separately organized agency" to succeed. We contacted the first two agencies cited because they were identified in the Board's June 1999 report as good models of a separately organized agency. We contacted the latter two agencies cited after consultation with staff in your offices. We also interviewed former NNSA and DOE officials, including the first and second Administrators and Deputy Secretary of Energy, who helped establish NNSA, to get their perspective on the difficulties involved in creating a separately organized agency within a department.

With respect to other management improvements, we met with officials from NNSA headquarters, the NNSA Service Center, NNSA site offices, and NNSA contractors; and various DOE offices, including the Office of Engineering and Construction Management. To develop information on the status of NNSA's efforts to improve project and program management, we analyzed DOE's annual performance and accountability reports; construction project data from NNSA's budget requests for fiscal years 1995 through 2005; and DOE program management performance information. Finally, we reviewed documents on NNSA's planning, programming, budgeting, and evaluation process and human capital efforts.

[9]House Armed Services Committee Special Panel on the Department of Energy Reorganization, 106th Cong., *Department of Energy National Nuclear Security Administration Implementation Plan* (Feb. 2000); House Armed Services Committee Special Panel on the Department of Energy Reorganization, 106th Cong., *Establishing the National Nuclear Security Administration: A Year of Obstacles and Opportunities* (Oct. 13, 2000).

We conducted our work from March 2005 to January 2007 in accordance with generally accepted government auditing standards, which included an assessment of data reliability and internal controls.

Results in Brief

Although NNSA has improved its headquarters oversight of security across the nuclear weapons complex, NNSA still cannot demonstrate that all of its security program objectives are being met at all of its sites, according to our review of NNSA site offices' surveys and DOE's independent inspections. We examined the results of the surveys and inspections because NNSA and DOE security officials generally agreed that the survey and inspection results represented the best available information on the overall performance of NNSA's security program. The surveys and inspections identify weaknesses with physical security at several NNSA sites, including the Nevada Test Site, Sandia National Laboratories, and the Y-12 National Security Complex, and weaknesses throughout NNSA in the cyber security area. We identified, through information review and interviews of various NNSA, DOE, and contractor officials, the following four factors that have contributed to problems with NNSA's security program:

- *Lack of consistent leadership and direction for its security activities.* For several years, the NNSA headquarters security organization experienced turnover in the position of Chief of the Office of Defense Nuclear Security (DNS). Specifically, four individuals have occupied the position since NNSA's creation, often in an acting capacity. In addition, these chiefs have reported to different levels within the organization. The current Chief is a permanent appointee, reporting directly to the NNSA administrator, and he has taken a number of steps to develop an effective headquarters security organization.

- *Security personnel staffing shortages at site offices.* Having sufficient staff to oversee the security programs of its contractors continues to be a problem. For example, since NNSA became operational, some site offices have experienced staffing shortfalls. As a result, sites are limited in their ability to effectively oversee contractors' security activities.

- *Lack of adequate training resources and opportunities for site office security staff.* NNSA has not implemented a training program that provides NNSA federal security officials with the skills needed to effectively oversee contractor security programs. In addition, NNSA site offices often do not have all the resources needed to meet training

needs. For example, according to site office officials, the Los Alamos Site Office did not receive training funds for fiscal year 2006 and the Nevada Site Office received a minimal training budget for its security staff.

- *Lack of data to gauge program effectiveness.* NNSA does not have complete data for tracking security deficiencies identified by security oversight reviews and, as a result, does not have information regarding the overall effectiveness of its safeguards and security program. NNSA officials told us that while they believe security across the weapons complex has improved, NNSA does not have sufficient data to support this assertion. In addition, NNSA has not implemented a formal process for sharing best practices or lessons learned to guide security improvements. While best practices and lessons learned have been communicated informally, a formal process could help ensure that previously identified security deficiencies, such as, for example, the retrieval of badges from terminated employees at one NNSA site, are reviewed and corrected as necessary at other NNSA field locations.

NNSA has taken several actions to improve its management practices, including issuing a program management policy; however, almost 7 years after its creation, NNSA and DOE have not developed procedures that govern how NNSA should function as a separately organized agency within the department. Most notably, DOE and NNSA's counterintelligence offices, whose missions were outlined in the original NNSA Act, continually disagreed over the scope and direction of the counterintelligence program. While DOE wanted to focus primarily on investigating counterintelligence breaches after they occur, NNSA sought to prevent intelligence leaks. Recent changes to the NNSA Act are intended to address these conflicts by placing all counterintelligence activities under the department.[10] We also identified the following four other management areas where additional NNSA actions could improve its effectiveness in managing the nuclear weapons complex:

- *Human capital.* NNSA has made progress in developing a human capital strategy. However, DOE and NNSA have not conducted a systematic, detailed analysis of how many staff NNSA needs in relation to DOE. As a result, we identified areas where potential staff imbalances have affected NNSA's ability to operate separately from DOE. For

[10]Pub. L. No. 109-364, § 3117 (2006).

example, NNSA's Office of General Counsel has 35 attorneys, including the General Counsel, to provide NNSA legal analysis, while the rest of DOE has 277 attorneys. According to NNSA's General Counsel, his office would need 15 to 20 additional attorneys to fully handle NNSA's legal workload with minimal assistance from DOE. Currently, NNSA relies on DOE's Office of General Counsel to perform a significant portion of its legal work.

- *Project management.* While both DOE and NNSA have initiated efforts to improve project management, NNSA reported in November 2006 that about 16 percent of NNSA projects were at risk of breaching their cost baseline, schedule baseline or both. We identified seven areas for improvement that would foster a stronger culture for effective project management. For example, while NNSA staff has proposed the development of a new plan to further improve project management, NNSA management indicated that it was not aware of this proposal; NNSA has not acted on this proposal. Furthermore, DOE's Project Assessment and Reporting System—a Web-based system for keeping DOE senior managers apprised of the performance of projects costing more than $5 million—does not include four major NNSA projects, estimated to cost over $100 million each. Consequently, these projects do not receive the senior management oversight that can be provided through that system.

- *Program management.* NNSA program managers are responsible for completing a set of activities by employing a working knowledge of such diverse areas as contracting, budgeting, and engineering. Recognizing the important role of program managers, NNSA has taken several actions, such as developing a program management policy. However, NNSA has yet to identify all of its program managers or train them to a certified level of competency. Indeed, DOE's most recent performance and accountability report for fiscal year 2006 showed that NNSA fully met only about 52 percent of its program goals while the rest of DOE achieved about a 79-percent success rate.

- *Financial management.* NNSA has made significant progress in implementing the planning, programming, budgeting, and evaluation process (PPBE) over the last 4 years, as mandated by the NNSA Act. However, several areas of improvement still have not been fully addressed. For example, NNSA has issued policy letters on PPBE, but some of these letters are still in draft form because, in part, NNSA is waiting to obtain DOE's views on certain matters. In addition, NNSA's

PPBE mechanism for centralized resource allocation relies on collegial decision making among senior NNSA managers, with the Administrator resolving disputes and deciding on the final resource allocation. However, the Administrator does not have an independent group to review program proposals, confirm cost estimates, and analyze alternatives. According to a 2003 DOE Inspector General report, most senior managers believe that such an analytical group would be of value.[11] While NNSA has taken some action in this direction, it is not clear when such a group will be established.

To improve the management of NNSA and its ability to oversee the nuclear weapons complex, we are making a series of recommendations to the Secretary of Energy and the Administrator, NNSA to, among other things, (1) improve various aspects of NNSA's security oversight program; (2) clearly define NNSA's status as a separately organized agency within DOE; and (3) institute a series of NNSA initiatives to improve project and program management, and the agency's planning, programming, budgeting, and evaluation process.

We provided NNSA with a copy of this report for their review and comment. NNSA generally agreed with the report and its corresponding recommendations. NNSA noted that it considers the agency to be a success but acknowledged that there was considerable work yet to be accomplished. NNSA and DOE also provided technical comments, which we have incorporated in this report as appropriate.

Background

NNSA conducts its activities at research and development laboratories, production plants, and other facilities (collectively referred to as the nuclear weapons complex). Specifically, NNSA operates three national laboratories that design nuclear weapons—Lawrence Livermore National Laboratory, California; Los Alamos National Laboratory, New Mexico; and the Sandia National Laboratories, New Mexico and California; and four nuclear weapons production sites—the Pantex Plant, Texas; the Y-12 National Security Complex, Tennessee; the Kansas City Plant, Missouri; and parts of the Savannah River Site, South Carolina; as well as the Nevada Test Site.

[11]National Nuclear Security Administration's Planning, Programming, Budgeting, and Evaluation Process, DOE/IG-0614, Aug. 2003.

To implement its programs, NNSA received about $9.1 billion for fiscal year 2006, including almost $6.4 billion for its nuclear weapons activities, about $1.6 billion for its defense nuclear nonproliferation programs, and about $782 million for the Naval Reactors program. NNSA's appropriation also included about $766 million to provide security at its sites. NNSA requested over $9.3 billion for fiscal year 2007, including $6.4 billion for its nuclear weapons activities, $1.7 billion for its defense nuclear nonproliferation programs, and $795 million for the Naval Reactors program. According to NNSA's Future Years Nuclear Security Program plan, between fiscal years 2007 and 2011, NNSA is proposing to spend almost $48.5 billion on its nuclear weapons, nuclear nonproliferation, and naval reactors programs.

For several years before NNSA was established, external studies found problems with the organization and operation of what is now NNSA's principal organization—DOE's Office of Defense Programs. These studies cited continuing problems in the areas of overall management, organization, priority setting, and maintenance of a viable infrastructure and workforce. For example, the Institute for Defense Analysis's March 1997 study, often called the "120-Day Study," cited ambiguities and overlaps between the roles of headquarters and the field as a primary source of inefficiencies and conflict.[12] Most influential in the creation of NNSA was the study conducted by a Special Investigative Panel of the President's Foreign Intelligence Advisory Board.[13] Prepared in response to a series of security problems, including public access to classified documents at the Los Alamos National Laboratory, the Board found that DOE was a dysfunctional bureaucracy incapable of reforming itself and that reorganization was clearly warranted to resolve security and counterintelligence problems. As noted earlier, the Board urged the Congress to create a new organization that, whether established as an independent agency or a semi-autonomous entity within DOE, should have a clear mission, streamlined bureaucracy, and drastically simplified lines of authority and accountability. To correct the problems identified by the Board and others, in 1999, the Congress created the NNSA.

[12]Institute for Defense Analysis, *The Organization and Management of the Nuclear Weapons Program* (Washington, D.C.: Mar. 1997).

[13]A special investigative panel, President's Foreign Intelligence Advisory Board, *Science At Its Best, Security At Its Worst: A Report on Security Problems at the U.S. Department of Energy* (Washington, D.C.: June 1999).

For the last several years, we have monitored various high-risk areas impacting NNSA operations and NNSA actions to implement the NNSA Act. In January 2001, and again in January 2003, we identified strategic human capital management as a governmentwide, high-risk area. We found that the lack of attention to strategic human capital planning had created a risk to the federal government's ability to perform its missions economically, efficiently, and effectively.[14] In that context, we have stated that strategic workforce planning is needed to address two critical needs: (1) aligning an organization's human capital program with its current and emerging mission and programmatic goals and (2) developing long-term strategies for acquiring, developing, and retaining staff to achieve programmatic goals.[15]

In April 2001, we testified that NNSA's efforts to establish a new organization looked promising.[16] However, we highlighted the need for NNSA to clearly define the roles and responsibilities of headquarters and field staff and to establish clear lines of authority between NNSA and its contractors, among other things. In May 2001, NNSA announced plans to reorganize its headquarters operations. In December 2001, we noted that NNSA had set several important goals for its overall reorganization efforts, including establishing clear and direct lines of communication, clarifying the roles and responsibilities of NNSA's headquarters and field offices, and integrating and balancing priorities across NNSA's missions and infrastructure.[17] However, we found that NNSA's plans for the headquarters reorganization did not contain a clear definition of the roles and responsibilities of the headquarters organizational units.

[14]See GAO, *High-Risk Series: An Update*, GAO-01-263 (Washington, D.C.: Jan. 2001), and GAO, *High Risk Series: An Update*, GAO-03-119 (Washington, D.C.: Jan. 2003). Also, see GAO, *Performance and Accountability Series—Major Management Challenges and Program Risks: A Governmentwide Perspective*, GAO-01-241 (Washington, D.C.: Jan. 2001). In addition, see the accompanying 21 reports (numbered GAO-01-242 through GAO-01-262) on specific agencies.

[15]GAO, *Human Capital: Key Principles for Effective Strategic Workforce Planning*, GAO-04-39 (Washington, D.C.: Dec. 11, 2003).

[16]GAO, *Department of Energy: Views on the Progress of the National Nuclear Security Administration in Implementing Title 32*, GAO-01-602T (Washington, D.C.: Apr. 4, 2001).

[17]GAO, *NNSA Management: Progress in the Implementation of Title 32*, GAO-02-93R (Washington, D.C.: Dec. 12, 2001).

In addition to reorganizing its headquarters, in February 2002, NNSA proposed reorganizing its entire operation to solve important, long-standing issues. Specifically, NNSA proposed a new organizational structure that would (1) remove a layer of management by converting existing operations offices to one support office, (2) locate NNSA operational oversight close to laboratories and plants by strengthening its site offices, and (3) streamline federal staff and hold federal staff and contractors more accountable. In February 2002, we testified that, with the proposed new organizational structure, resolution of NNSA's long-standing organizational issues appeared to be within NNSA's grasp.[18] However, we noted that NNSA's lack of a long-term strategic approach to ensuring a well-managed workforce precluded it from identifying its current and future human capital needs, including the size of the workforce; its deployment across the organization; and the knowledge, skills, and capabilities needed to fulfill its mission. In December 2002, the Administrator of NNSA implemented the proposed reorganization.

Our May 2003 report on the management of NNSA's security program identified similar concerns about NNSA's security organization and management.[19] Specifically, we found that NNSA (1) had not fully defined clear roles and responsibilities for its headquarters and site security operations and (2) had shortfalls at its site offices in the total number of staff and in expertise, which could make it more difficult for the site offices to effectively oversee security activities. We therefore concluded that NNSA could not be assured that its contractors were working to maximum advantage to protect critical facilities and material from individuals seeking to inflict damage.

In June 2004, we found that NNSA's reorganization had addressed some past problems by better delineating lines of authority and improving communication. However, we also found that NNSA's reorganization had not ensured that the agency had sufficient staff with the right skills in the right places because it had downsized its federal workforce by about 17 percent without first determining the critical skills and capabilities needed to meet its mission and program goals.[20]

[18]GAO, *Department of Energy: NNSA Restructuring and Progress in Implementing Title 32*, GAO-02-451T (Washington, D.C.: Feb. 26, 2002).

[19]GAO-03-471.

[20]GAO-04-545.

Recently, in response to a July 2005 report by the Secretary of Energy's Advisory Board's Nuclear Weapons Complex Infrastructure Task Force on the nuclear weapons complex of the future, NNSA changed the reporting relationship of the site office managers.[21] To facilitate the transformation of the nuclear weapons complex, the Task Force recommended that the site office managers begin reporting to the Deputy Administrator for Defense Programs instead of to the Administrator. The Task Force believed that the Deputy Administrator was the primary line manager with mission responsibility for the work conducted at the sites and that this change would better align responsibility and management of the program. In May 2006, the Administrator made this change.

Additional Action Needed to Improve NNSA's Security Program

Although NNSA has improved its headquarters oversight of security across the nuclear weapons complex, NNSA continues to experience difficulties in developing a safeguards and security program that provides reasonable assurance that all protection objectives are being met, especially at certain locations and in several topical areas, most notably cyber security, according to our review of NNSA site office surveys and independent inspections by DOE's Office of Independent Oversight. We analyzed the results of the surveys and inspections because NNSA and DOE security officials generally agreed that the survey and inspection results represented the best available information on the overall performance of NNSA's security program. While the results of the surveys and inspections are not entirely consistent, they do identify weaknesses with physical security at several NNSA sites, including the Nevada Test Site, Los Alamos National Laboratory, and the Y-12 National Security Complex, and weaknesses throughout NNSA in the cyber security area. Over the last several years, NNSA's security program has been hampered by several factors, including (1) the lack of an effective headquarters organization, (2) security staffing shortages at its site offices, (3) the lack of adequate training resources and opportunities for its site office security staff, and (4) the lack of metrics to gauge program effectiveness.

[21]DOE, Secretary of Energy Advisory Board, *Report of the Nuclear Weapons Complex Infrastructure Task Force: Recommendations for the Nuclear Weapons Complex of the Future* (Washington, D.C.: July 13, 2005).

NNSA Is Experiencing Difficulty in Meeting All Security Program Objectives

According to DOE Manual 470.4-1, *Safeguards and Security Program Planning and Management*, NNSA must develop a safeguards and security program that ensures NNSA has the necessary protections in place to protect its security interests against malevolent acts, such as theft, diversion, sabotage, modification, compromise, or unauthorized access to nuclear weapons, nuclear weapons components, special nuclear materials, or classified and unclassified information. NNSA's DNS is responsible for developing the administration's security program.

To determine the overall effectiveness of NNSA's safeguards and security program, NNSA and DOE principally rely on two types of evaluations. Specifically, NNSA site offices conduct surveys of contractors' performance while the Office of Independent Oversight conducts periodic inspections, typically every 18 months. These evaluations identify the strengths and weaknesses of NNSA's security program and provide a basis for line management to decide on program implementation activities, including allocating resources and correcting security deficiencies.

Site Office Surveys. NNSA's site offices assess the extent to which day-to-day security activities at its contractor-operated laboratories and production facilities ensure that program objectives are met. According to DOE's *Safeguards and Security Program Planning and Management* manual, the frequency of these surveys varies from 12 months to 24 months, depending on the site's importance rating and type of materials stored at that location. The site office surveys cover 8 topical areas and 33 subtopical areas and are based on observations of performance, including compliance with DOE and NNSA security directives. Table 1 shows the 8 topical and 33 subtopical safeguards and security areas covered.

Table 1: Safeguards and Security Program Areas Covered in NNSA Surveys

Safeguards and security program areas	Program definition
Program management and support • Protection management program • Safeguards and security planning and procedures • Management control • Program-wide support	Establishes a standardized approach for protection program planning that will provide an information baseline for use in integrating departmental safeguards and security considerations, facilitating management evaluation of program elements, determining resources for needed improvements, and establishing cost-benefit bases for analyses and comparison.
Protective forces • Management • Training • Duties • Facilities and equipment	Protect security interests from terrorist or other adversarial actions that could have major national security consequences.
Physical security • Access controls • Intrusion detection and assessment systems • Barriers and delay mechanisms • Testing and maintenance • Communications	Protect departmental assets from malevolent acts such as theft, diversion, and sabotage events, such as civil disorder, by considering site and regional threats, protection planning strategies, and protection measures.
Information protection • Basic requirements • Technical surveillance and countermeasures • Operations security • Classification guidance • Classified matter protection and control	Protect and control classified and controlled sensitive matter that is generated, received, transmitted, used, stored, reproduced, or destroyed.
Cyber security • Classified cyber security • Telecommunications security • Unclassified cyber security	Protect automated information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, against loss of accountability for information and user actions, and against the denial of service to authorized users, including those measures necessary to protect against, detect, and counter such threats.
Personnel security • Access authorizations • Human reliability program • Control of classified visits • Safeguards and security awareness	Ensure that granting an individual access to classified matter, special nuclear material, or both would not endanger the common defense and security and would be clearly consistent with the national interest.
Unclassified visits and assignments by foreign nationals • Sponsor program management and administration • Counterintelligence requirements • Export controls/technology transfer requirements • Security requirements • Approvals and reporting	Document and track visits and assignments by foreign nationals to DOE sites or involving DOE information or technologies.
Control and accountability of nuclear materials • Program administration • Material accountability • Materials control	Provide information on, control of, and assurance of the presence of nuclear materials, including those systems necessary to establish and track nuclear material inventories, control access to and detect loss or diversion of nuclear material, and ensure the integrity of those systems and measures.

Source: DOE orders and manuals.

The surveys assign the following color-coded performance ratings to communicate the extent of performance and compliance with required procedures and practices, as well as the impact of any deficiencies along with other mitigating factors:

- *Satisfactory (Green).* The element being evaluated meets protection objectives or provides reasonable assurance that protection objectives are being met.

- *Marginal (Yellow).* The element being evaluated partially meets protection objectives or provides questionable assurance that protection objectives are met.

- *Unsatisfactory (Red).* The element being evaluated does not meet protection objectives or does not provide adequate assurance that protection objectives are being met.

Office of Independent Oversight Inspections. The Office of Independent Oversight independently evaluates DOE sites, facilities, organizations, and operations in the areas of safeguards and security, cyber security, emergency management, and environment, safety, and health programs. The Office of Independent Oversight inspects both federal and contractor operations at a site and identifies findings, issues, and opportunities for improvement. It also performs follow-up reviews to ensure corrective actions are effective and that weaknesses in the safeguards and security program are appropriately addressed. As shown in table 2, the Office of Independent Oversight's inspections cover eight topical and 36 subtopical safeguards and security areas.

Table 2: Safeguards and Security Program Areas in Office of Independent Oversight Inspections

Safeguards and security program areas	Program definition
Protection program management • Planning process • Organization and staffing • Budget process • Program direction • Control systems • Survey program	Programs are designed to ensure that security interests are provided an appropriate degree of protection from hostile acts. It is an iterative process, whereby activities related to planning, staffing, budget, direction, and feedback are integrated with overall strategic and near-term operational planning.
Physical security systems • Intrusion detection assessment • Entry and search controls • Badges, passes, and credentials • Barriers • Communications • Testing and maintenance	Programs are designed to use intrusion detection and assessment, entry and search control, barriers, communications, testing and maintenance, and supporting systems and interfaces to deter, detect, annunciate, assess, delay, and communicate an unauthorized activity.
Protective forces • Management • Training • Equipment and facilities • Duties	Programs are designed to protect both DOE security interests from theft, sabotage, and other hostile acts that may adversely impact national security or the health and safety of the public, as well as life and property at DOE facilities.
Classified matter protection and control • Program management • Control of secret and confidential documents • Control of top secret documents • Control of classified materials • Special programs • Operations security • Technical surveillance countermeasures • Classification management	Programs are designed to provide protection against unauthorized disclosure of classified matter and for sensitive information from its inception to destruction or decontrol.
Material control and accountability • Administration • Accounting • Measurements • Inventories • Containment	Programs are designed to provide an information and control system for nuclear material. These programs encompass those systems and measures necessary to establish and track nuclear material inventories, control access, detect loss or diversion of nuclear material, and ensure the integrity of those systems and measures.
Personnel security • Management • Personnel clearance program • Security education program • Visitor control program • Human reliability program	Programs are designed to ensure that access to sensitive information, classified matter, and special nuclear material will be granted only after it has been determined that such access will not endanger security and is consistent with the national interest.
Cyber security—classified and unclassified	Programs are designed to prevent deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, modification, or loss of information contained within computer networks and systems, as well as measures designed to prevent denial of authorized use of the system.

Source: Office of Independent Oversight inspector's guides.

As shown in table 2, the Office of Independent Oversight examines areas that are comparable to those that NNSA site offices assess through their surveys. Similarly, the Office of Independent Oversight's rating scale is comparable to the one NNSA site offices use. Specifically, the Office of Independent Oversight may assign the following color-coded ratings to overall programs, selected topical areas, or both:

- *Effective performance (Green).* The system inspected provides reasonable assurance that the identified protection needs are met. That is, (1) the protection meets all applicable standards, (2) the protection did not meet all standards, but other systems or compensatory measures provide equivalent protection, or (3) the failure to fully meet a standard does not significantly degrade the protection. Line managers are expected to effectively address any specific deficiencies identified.

- *Needs improvement (Yellow).* The system inspected only partially meets identified protection needs or provides questionable assurance that the identified protection needs are met. That is, one or more applicable standards are not met and are only partially compensated for by other systems, and the resulting deficiencies degrade the effectiveness of the inspected system. Line managers would be expected to significantly increase their attention to the identified areas of weakness.

- *Significant weakness (Red).* The system inspected does not adequately assure that identified protection needs are met. That is, one or more applicable standards are not met, no compensating factors reduce the impact on system effectiveness, and the deficiencies seriously degrade the system's effectiveness. Line managers are expected to apply immediate attention, focus, and resources to the deficient program areas.

In addition to ratings, NNSA site office surveys and Office of Independent Oversight inspection reports develop findings that identify validated security deficiencies associated with a contractor's safeguards and security program. In response to these findings, DOE requires that contractors develop corrective actions to correct the security deficiencies. These corrective actions include risk assessment, root cause and cost-benefit analyses. To facilitate the tracking of security findings and the development of corrective actions by the responsible organization, DOE Manual 470.4-1 requires site office and the Office of Independent Oversight staff to ensure that findings are entered into the Safeguards and Security Information

Management System (SSIMS) —a centralized information management system—in a timely manner.

NNSA Site Office Survey and Office of Independent Oversight Inspection Results, While Not Entirely Consistent, Identify Several Problem Areas

To evaluate the extent to which NNSA has addressed security issues at its laboratories and plants, we reviewed and compared the results of NNSA's site office surveys and DOE's Office of Independent Oversight inspections for the 5-year period before the administration became operational—fiscal years 1996 through 2000—and the 5-year period after it became operational—fiscal years 2001 through 2005. While the results of these surveys and inspections are not entirely consistent, they do indicate that NNSA continues to experience difficulties in implementing a safeguards and security program that provides reasonable assurance that all protection objectives are being met, especially at certain locations and in several topical areas, most notably cyber security.

Initially, we totaled the ratings given to each topical area shown in table 2 and determined the cumulative percent of ratings that resulted in either a satisfactory, marginal, or unsatisfactory rating. With respect to the site office surveys, the cumulative percentage of topical areas that received a satisfactory rating declined slightly between the two periods. Specifically, as shown in table 3, 86 percent of the areas covered by the survey received a satisfactory rating for the period before NNSA became operational, while 81 percent received a satisfactory rating after NNSA was established.

Table 3: Site Office Survey and Office of Independent Oversight Inspection Results of NNSA's Overall Security Performance, Fiscal Years 1996 through 2000, Compared with Fiscal Years 2001 through 2005

	Fiscal years 1996 through 2000		Fiscal years 2001 through 2005	
Ratings	Site office surveys	Office of Independent Oversight inspections	Site office surveys	Office of Independent Oversight inspections
Satisfactory	86%	82%	81%	52%
Marginal	12%	16%	17%	39%
Unsatisfactory	2%	2%	2%	9%
Total number of assigned ratings	**209**	**50**	**221**	**74**

Source: GAO analysis of NNSA site office survey and Office of Independent Oversight inspection reports.

The results for our analysis of the overall Office of Independent Oversight results showed a different picture. Specifically, while 82 percent of the areas covered by the Office of Independent Oversight inspections received a satisfactory rating for the period before NNSA became operational, only 52 percent received a satisfactory rating after NNSA was established. Most notably, the percentage of areas receiving a marginal rating increased from 16 percent for the period 1996 through 2000 to 39 percent for 2001 through 2005.

Because of (1) the importance of physical security in response to the terrorist attacks of September 11, 2001, and (2) ongoing concerns about the vulnerability of DOE computer systems to cyber security attacks, and to identify where the differences were occurring between the NNSA site office survey and the Office of Independent Oversight inspection results, we analyzed the results for the physical security and cyber security topical areas in the NNSA site office surveys and the Office of Independent Oversight inspections for the 5-year period before the administration became operational—fiscal years 1996 through 2000—and the 5-year period after it became operational—fiscal years 2001 through 2005.[22]

With respect to physical security, as shown in table 4, for the site office surveys, the cumulative percentage of physical security topical areas that received a satisfactory rating remained relatively unchanged between the two periods for the seven sites we reviewed. In each period, slightly more than 80 percent of the assessments resulted in a satisfactory rating, even as physical security requirements have been strengthened in response to the September 11, 2001 attacks.

[22]Physical security combines security equipment, personnel, and procedures to protect facilities, information, documents or material against theft, sabotage, diversion, or other criminal acts. For the purposes of analyzing trends in NNSA's physical security ratings we combined the ratings for the following topical areas: Protection Program Management; Physical Security Systems; Protective Force; Classified Matter Protection and Control, Materials Control and Accountability; and Personnel Security.

Table 4: Site Office Survey and Office of Independent Oversight Inspection Results of NNSA's Physical Security Performance, Fiscal Years 1996 through 2000, Compared with Fiscal Years 2001 through 2005

	Fiscal years 1996 through 2000		Fiscal years 2001 through 2005	
Ratings	Site office surveys	Office of Independent Oversight Inspections	Site office surveys	Office of Independent Oversight inspections
Satisfactory	84%	80%	82%	49%
Marginal	14%	17%	15%	41%
Unsatisfactory	2%	3%	3%	10%
Total number of assigned ratings	**163**	**36**	**168**	**59**

Source: GAO analysis of NNSA site office survey and Office of Independent Oversight inspection reports.

While the site surveys showed relatively little change between the periods reviewed, the Office of Independent Oversight's evaluation of physical security showed a pronounced decline. Specifically, as shown in table 4, while about 80 percent of the Office of Independent Oversight's physical security assessments resulted in a satisfactory rating for the period between fiscal years 1996 and 2000, only about 49 percent of the Office of Independent Oversight's physical security ratings were satisfactory for the period of fiscal year 2001 through 2005.

Several factors contributed to the differences between the NNSA site office ratings and the Office of Independent Oversight inspections for physical security. First, while more site offices surveys were performed in fiscal years 2001 through 2005 than the Office of Independent Oversight inspections, proportionately more Office of Independent Oversight ratings were marginal and unsatisfactory. In particular, we found that at three sites—the Nevada Test Site; Sandia National Laboratories, New Mexico; and the Y-12 National Security Complex—over half of the Office of Independent Oversight ratings were either marginal or unsatisfactory. In contrast, only the Y-12 National Security Complex's site office surveys had more than 50 percent of the ratings as marginal or unsatisfactory over the same period. Moreover, the Office of Independent Oversight inspections had a higher percentage of marginal and unsatisfactory ratings in the Physical Security Systems, Classified Matter Protection and Control, and Materials Control and Accountability topical areas than did the site office surveys.

With respect to cyber security, both the site office surveys and the Office of Independent Oversight inspections show declines. Specifically, as shown in table 5, 92 percent of the cyber security assessments in NNSA site office surveys resulted in a satisfactory rating for both classified and unclassified cyber security before NNSA was operational, but only 77 percent of the assessments resulted in a satisfactory rating after NNSA became operational.

Table 5: Site Office Survey and Office of Independent Oversight Inspection Results of NNSA's Cyber Security Performance, Fiscal Years 1996 through 2000, Compared with Fiscal Years 2001 through 2005

	Fiscal years 1996 through 2000		Fiscal years 2001 through 2005	
Ratings	Site office surveys	Office of Independent Oversight inspections	Site office surveys	Office of Independent Oversight inspections
Satisfactory	92%	86%	77%	60%
Marginal	4%	14%	23%	33%
Unsatisfactory	4%	0%	0%	7%
Total number of assigned ratings	**46**	**14**	**53**	**15**

Source: GAO analysis of NNSA site office survey and Office of Independent Oversight inspection reports.

Similarly, Office of Independent Oversight inspection results also indicated that cyber security performance had declined. Before NNSA became operational, 86 percent of cyber security assessments resulted in satisfactory ratings, compared with only 60 percent after NNSA became operational.

With respect to the individual sites, the Office of Independent Oversight inspections gave the most marginal or unsatisfactory ratings for cyber security to four sites: Los Alamos National Laboratory; Pantex; Sandia National Laboratories, New Mexico; and the Y-12 National Security Complex. In contrast, the NNSA site office surveys assigned marginal ratings to every NNSA site.

Concerns about cyber security were also raised in one of the two independent analyses NNSA commissioned in July 2003 and by NNSA officials with whom we spoke. Specifically, one analysis, *NNSA Security:*

An Independent Review, found that NNSA cyber security policies, procedures and practices were less mature than their counterparts in other security disciplines. Furthermore, the review found that NNSA was "resource poor" and cyber security implementation varied widely throughout NNSA because of inadequate funding, insufficient cyber security personnel and expertise, and inadequate collaboration between DOE and NNSA cyber security organizations. According to current and former NNSA officials, and several site office security directors, the cyber security program has received inadequate attention and was poorly implemented because NNSA lacks a risk-based approach to physical and cyber security. In this regard, in June 2006, DOE officials revealed that a hacker had attacked an unclassified computer system at NNSA's Service Center in Albuquerque, New Mexico, and had gained access to a file containing the names and social security numbers of over 1,500 NNSA employees.

More recently, in September 2006, DOE's Inspector General reported on the weaknesses associated with the department's cyber security programs, including NNSA's. According to the Inspector General, while DOE has made progress in addressing some cyber-related problems, ongoing problems continue to place DOE's critical information systems and data at risk of compromise. The report cited weaknesses in the following areas: systems inventory, certification, and accreditation; contingency planning; access controls; and configuration management and change controls. These problems occurred, in part, because program and field offices did not always implement departmental and federal cyber security requirements. For example, the Inspector General reported, NNSA site officials stated that they were required to comply with NNSA cyber security policy, rather than standards established by the National Institute of Standards and Technology (NIST). However, the DOE Inspector General also found that NNSA sites had not fully implemented NNSA's cyber security policy and that many NNSA field sites were permitted to follow a less thorough certification and accreditation process that did not include all NIST or NNSA requirements.

Some of the differences between the site office survey and the Office of Independent Oversight inspection results may be due to continued differences in how each organization conducts its evaluations. We and other oversight organizations have reviewed this issue over the last 6 years. For example, in February 2000, we reported that from 1994 through 1999, the Los Alamos National Laboratory and the Lawrence Livermore National Laboratory received inconsistent oversight ratings.[23] During a given year, Los Alamos National Laboratory received ratings ranging from marginal to excellent, depending on the DOE organization conducting the assessment. Similarly, the Lawrence Livermore National Laboratory received ratings ranging from marginal to far exceeds expectations. We reported that this inconsistency resulted, in part, from various organizations' use of different criteria as well as the timing of the rating. Similarly, in May 2000, DOE's Office of Inspector General reported on various factors affecting the safeguards and security ratings and found that certain security ratings were changed without a documented rationale.[24]

More recently, in 2005, the Office of Independent Oversight issued a report on the inconsistencies in safeguards and security ratings.[25] Specifically, the report noted that the Office of Independent Oversight tended to identify significant safeguards and security program deficiencies that the site office surveys did not detect. Furthermore, the report identified several major weaknesses commonly found in survey programs, including a lack of comprehensiveness in conducting surveys; insufficient, or insufficiently rigorous, performance testing; a reluctance to assign formal findings when deficiencies were identified; and the lack of sufficient detail to justify, or even to explain, the assigned ratings in some survey reports.

[23]GAO, *Nuclear Security: Improvements Needed in DOE's Safeguards and Security Oversight*, GAO/RCED-00-62 (Washington, D.C.: Feb. 24, 2000).

[24]Inspection of Allegations Relating to the Albuquerque Operations Office Security Survey Process and the Security Operations' Self-Assessment at Los Alamos National Laboratory, DOE/IG-0471, May 2000.

[25]*Review of the National Nuclear Security Administration's Federal Line Management Oversight of Security Operations*, Office of Independent Oversight and Performance Assurance, DOE, 2005.

Several Factors Have Contributed to Problems in NNSA's Safeguards and Security Program

Because many NNSA sites handle special nuclear material, including nuclear weapons, plutonium, and highly enriched uranium, effective federal oversight is critical to ensuring that the national security is not harmed. While NNSA has recently improved its headquarters oversight of security, it has been hampered over the last 7 years by several factors, including (1) the lack of an effective headquarters organization, (2) security staffing shortages at its site offices, (3) lack of adequate training resources and opportunities for its site office security staff, and (4) the lack of a complete security information database and framework for evaluating security review results.

NNSA Has Had Difficulty Developing an Effective Headquarters Security Organization

Under GAO's *Standards for Internal Control in the Federal Government*, federal agencies must establish and maintain an effective system of internal controls over their operations.[26] Such a system is the first line of defense in safeguarding assets and preventing and detecting errors. Under our standards, managers should, among other things, ensure that (1) the organizational structure clearly defines key areas of authority and responsibility, (2) staff have the required skills to meet organizational objectives, (3) progress can be effectively measured, and (4) operations can be effectively monitored. However, during much of its history, NNSA's security program has experienced the following organizational issues:

- *Initial organizational arrangements were not productive*. The NNSA Act established the position of Chief of DNS to advise the NNSA Administrator on security-related matters and implement the security policies directed by the Secretary and the Administrator. NNSA also established the Nuclear Safeguards and Security Program (NSSP) within NNSA's Facilities and Operations organization to provide assistance to NNSA's site offices on such issues as implementing the Design Basis Threat and developing budget requests for security.[27] However, the heads of the two offices had strained relations and often disagreed on how to improve physical security at NNSA facilities. In September 2002, the NSSP Director was replaced and his position eventually terminated, and other NSSP staff either retired or left NNSA. As a result, the

[26]GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: Nov. 1999).

[27]The Design Basis Threat is a classified document that identifies the potential size and capabilities of a terrorist force that DOE protective forces must be able to defeat.

effectiveness of the NSSP program was greatly reduced and the field lost a source of guidance and leadership in NNSA headquarters.

- *Leadership turned over several times*. NNSA's headquarters security organization experienced considerable turnover in the position of Chief of DNS and changes in the reporting level of that position within NNSA. Specifically, four individuals have occupied that position since NNSA's creation, often in an acting capacity. In addition, these Chiefs have reported to different levels within NNSA. For example, the original Chief reported directly to the Administrator of NNSA. However, when he retired in 2003, his replacement occupied two positions—Chief of DNS and Associate Administrator for Facilities and Operations—a practice often referred to as "dual-hatting." When NNSA reorganized its headquarters security organization in 2004, the Chief of DNS once again reported directly to the Administrator. The second Administrator, who resigned in January 2007, told us that he regretted having dual-hatted the Chief of DNS position because it lowered the position's visibility within NNSA. He believed that it was correct to elevate the current Chief to serve as an Associate Administrator reporting directly to the Administrator.[28]

- *Without effective leadership, important oversight activities were ignored*. The third Chief of DNS employed only a small staff and took the position that virtually all headquarters oversight responsibility rested with the Office of Independent Oversight. This approach was strongly criticized in the April 2005 *NNSA Security, An Independent Review*, which noted that the Office of Independent Oversight had little, if any, direct responsibility, authority, and accountability for day-to-day supervision of the NNSA complex and that the Office of Independent Oversight's principal role was one of periodic independent performance assessment.

[28]Section 3232 of the NNSA Act requires that the Chief of DNS report to the Administrator and have direct access to the Secretary and every departmental official on security matters. See 50 U.S.C. § 2422.

To his credit, the current Associate Administrator for DNS has taken numerous steps to build an effective headquarters security organization. Specifically, he has

- issued a program management plan to establish an integrated, NNSA-wide, performance-based management approach for implementing work and defining security performance expectations among DNS, NNSA site offices, and their contractors to ensure full integration of security requirements with the programmatic missions of NNSA;

- issued specific requirements for NNSA's Performance Assurance Program, which provides a multi-tiered system of self-assessments and other reviews of security performance and is aimed at assuring comprehensive assessments of safeguards and security interests;

- improved interaction between NNSA headquarters and site office security elements. For example, the Associate Administrator established the Defense Nuclear Security Leadership Coalition, which comprises all safeguards and security directors and meets regularly to address security implementation challenges. He also conducts monthly teleconferences with both federal and contractor security officials at NNSA sites;

- established the Office of Security Oversight to assess safeguards and security performance, serve as the point of contact for correcting security deficiencies identified during surveys and independent inspections, ensure the quality and consistency of federal oversight of contractor activities, and identify areas for improvement throughout the weapons complex; and

- adopted a more proactive approach to security through stronger accountability. For example, within the last 2 years, NNSA has replaced three federal security directors at the Los Alamos, Nevada and Y-12 site offices.

NNSA Continues to Experience Security Staffing Shortfalls

Having sufficient staff to oversee the security programs of its contractors has been a persistent problem since NNSA's creation. For example, in our May 2003 report on the management of NNSA's security program, we found, among other things, that NNSA had shortfalls at its site offices in the total number of security staff and in security expertise, which may have made it more difficult for the site offices to effectively oversee security activities. Given this situation, we concluded that NNSA could not be assured that its contractors were working to maximum advantage to protect critical facilities and material from individuals seeking to inflict damage.[29] We raised a similar concern in our June 2004 report on NNSA's reorganization. Specifically, we found that NNSA's reorganization had not ensured that the agency had sufficient staff with the right skills in the right places because it had downsized its federal workforce without first determining the critical skills and capabilities needed to meet its mission and program goals. For example, we noted that some site offices, namely Pantex, Y-12, and Los Alamos, were having difficulty filling critical skills in the safety and security disciplines.[30]

Complementing our work was an independent analysis commissioned by NNSA. Specifically, in a March 2004 report, the "Chiles Commission" identified a number of challenges that NNSA faces in recruiting, training, and retaining enough skilled federal staff members to fill the current and future security positions needed to effectively oversee the security of its weapons complex.[31] These challenges included identifying the (1) number and skills mix of the security staff, (2) near-term retirement eligibility of a significant percentage of the security workforce, (3) lack of professional development and training programs, and (4) lack of adequate resources. The commission found that federal security personnel were managed on a site-specific basis, noting that NNSA lacked a comprehensive human capital plan to identify the areas of needed experience, ensure timely hiring, and manage the skills mix of the federal security workforce across the complex.

As part of this review, we assessed the continuing extent of security staffing shortfalls at NNSA site offices. Specifically, we requested

[29]GAO-03-471.

[30]GAO-04-545.

[31]*Strengthening NNSA Security Expertise: An Independent Analysis*, Henry G. Chiles et al., Mar. 2004.

information on the number of full-time equivalent (FTE) security positions required to conduct effective oversight versus the actual number of FTEs on board for fiscal years 2001 through 2005. As table 6 shows, three of the six site offices—the Los Alamos, Livermore and Sandia Site Offices—did not report information on the required level of staffing needed to effectively oversee contractors' security performance for at least 3 of the 5 years for which we requested data. According to site office security officials at these locations, they could not find the records showing official staffing shortfalls.

Table 6: NNSA Site Office Security Staffing Shortages, Fiscal Years 2001 through 2005

	Fiscal year 2001		Fiscal year 2002		Fiscal year 2003		Fiscal year 2004		Fiscal year 2005	
Site office	Required FTEs	Actual FTEs	Required FTEs	Actual FTEs	Required FTEs	Actual FTEs	Required FTEs	Actual FTEs	Required FTEs	Actual FTEs
Los Alamos	[a]	8	[a]	4	[a]	6	[a]	8	18	9
Livermore	[a]	27	[a]	27	[a]	26	20	18	20	19
Nevada	25	23	25	20	23	15	20	13	21	14
Pantex	8	7	8	7	8	7	8	7	8	8
Sandia	[a]	7	[a]	7	[a]	9	[a]	10	[a]	11
Y-12	11	6	11	10	10	12	11.5	11	14	13

Source: Analysis of NNSA site office staffing data.

[a]Required FTE numbers were unknown at these sites.

According to NNSA's data, five of the six site offices have experienced security staffing shortfalls during at least one fiscal year. For example, since fiscal year 2001, the Nevada Site Office has been increasingly understaffed, and in fiscal year 2005, the Los Alamos Site Office had half of the required staff it needed to conduct oversight. Consequently, according to site office security officials, most site offices have only one staff member responsible for a safeguards and security topical area and do not have additional staff on board to fill in if necessary. Site offices have compensated in various ways. For example, the Los Alamos Site Office has recently obtained detailees from other site office elements to assist in conducting oversight. According to one Safeguards and Security Director, security personnel have to work excessive overtime to complete assigned tasks. Finally, because it does not have a dedicated survey team, the Nevada Site Office has had to request survey assistance from other site offices to conduct surveys. According to a former NNSA official involved in the administration's initial organization, NNSA did not tailor security

staffing numbers to actual needs and could have better planned its allocation of staff to site offices during the reorganization.

To address the lack of security staff, NNSA has taken two actions. First, it has implemented the Defense Nuclear Security Intern Program. This program, which was established in 2004 and is administered by the Pacific Northwest National Laboratory, is designed to attract and train individuals to fill critical NNSA security positions and support the development of a qualified, experienced pool of security professionals to supplement site office staffing. Participants are assigned to a specific NNSA site for 12 to 15 months. Successful interns may have an opportunity for permanent placement as federal employees within NNSA's safeguards and security program if they successfully complete the program. To date, four participants have done so, with three of the four converted to permanent positions at the Pantex, Y-12, and Nevada site offices. According to site office officials, the most significant challenge associated with successfully implementing the intern program is obtaining clearances in a timely manner.

Second, in April 2005, NNSA held a staffing summit to determine site offices' needs. Headquarters and site offices provided their end-of-year staffing levels, the number of additional FTE staff needed to meet critical needs based on available resources, and an estimate of the optimal FTE levels. Based on available resources, NNSA site offices were granted authority for six FTE security staff. However, according to site office officials, site offices remain understaffed for security.

Training for Security Staff Can be Improved

NNSA has not implemented an appropriate training program to meet the needs of its security personnel. As a result, the number of security staff with adequate training and the right skills continues to be a problem. According to our *Standards for Internal Control in the Federal Government*, managers should ensure that their personnel possess and maintain a level of competence needed to accomplish their assigned duties. Specifically, skill needs must be continually assessed, and training should be aimed at developing and retaining the skills needed to achieve changing organizational goals. In addition, DOE requires that critical training needs for federal staff are identified and met and that a systematic mechanism for providing training be established. Training needs are both organizationally and individually driven. Site offices are required to identify performance gaps for newly hired employees and specialized training for subsequent years and are responsible for ensuring that training requirements are met. For their part, employees are required to develop an individual

development plan and discuss their training needs with their supervisors, who are responsible for authorizing all training.

In March 2004, the Chiles Commission reported that NNSA's federal security workforce was forgoing needed training because of the press of urgent business and a shortage of resources. The Commission found that over 50 percent of NNSA personnel surveyed believed that the existing training and education of the federal security workforce was not adequate. In addition, the Commission reported that staffing plans did not have the built-in flexibility needed to allow for professional development and training. NNSA officials told us that problems associated with site office workloads resulted from the 2002 reorganization where all oversight responsibilities formerly at the operations offices were transferred to the newly formed site offices without sufficient allocation of staff. In addition, site office security directors told us training budgets do not address the needs of their staff. For example, according to NNSA officials, the Los Alamos Site Office did not receive training dollars for fiscal year 2006, and the Nevada Site Office received only a minimal training budget for its security staff. According to a human resource official at the NNSA Service Center, there is an "enormous disconnect" between training needs and budgets, noting that training needs are not addressed systematically. To address this issue, Safeguards and Security directors at each site office have recently developed site-specific technical qualifications programs for their staffs. While these efforts are important, we found no NNSA-wide formal training program that provides NNSA federal security officials with the skills needed to conduct effective oversight.

NNSA Lacks Security Metrics to Gauge the Effectiveness of Its Safeguards and Security Program and Has Not Effectively Communicated Lessons Learned to Guide Security Improvements

NNSA does not have comprehensive metrics regarding the overall effectiveness of its safeguards and security program and is not communicating lessons-learned to guide security improvements across the complex. According to our *Standards for Internal Control*, for an agency to run and control its operations, it must have relevant, accurate information that is recorded and communicated to management in a form and within a time frame that enables managers to carry out their operational responsibilities. According to NNSA officials, NNSA has not developed a framework for evaluating the results of independent and internal security reviews. NNSA officials told us that while they believe that security across the weapons complex has improved, NNSA does not have good metrics to support the assertion that security has improved. DNS is currently working to develop performance metrics that will allow NNSA to track processes and make decisions about its safeguards and security

program, but NNSA does not plan to develop an overall indicator of its security status to assist in efforts to gauge program effectiveness.

In addition, NNSA does not have complete data for tracking security deficiencies identified by security oversight reviews. According to NNSA security officials, not all security deficiencies have been entered into SSIMS because (1) the database is very difficult to use, (2) connections to it are slow because of the lack of high-speed encrypted modems, and (3) it often crashes once a connection is established. Therefore, some site office officials questioned SSIMS's usefulness as a management tool and suggested that it be replaced. As a result, most site offices have begun to use their own tracking systems, or those developed by contractors, to track identified security deficiencies. For example, the Los Alamos National Laboratory uses REDBOOK, a custom-designed classified system operating on an ACCESS platform to internally track the status of security deficiencies and associated corrective action plans. Previously, Los Alamos had read-only access to SSIMS, but lost its connection after the 2004 stand-down of operations because of missing computer disks. Similarly, during the summer of 2004, the Y-12 Site Office developed PEGASUS—an interactive tracking system that is tailored to the site office's oversight efforts and links all oversight-related correspondence. According to Y-12 site office officials, the system informs site office security staff electronically about their daily oversight tasks, reduces the amount of paperwork associated with resolving security deficiencies, and allows the security director to track whether federal security personnel are performing their oversight duties. In addition, PEGASUS, which is updated weekly, has the ability to automatically identify recurring security deficiencies and provides better quality data than SSIMS. According to one security contractor official, the difficulty associated with logging onto SSIMS results in security deficiencies being reported 6 to 12 months after they are resolved.

In commenting on our report, officials in the Office of Health, Safety, and Security indicated that NNSA sites offices have not reported to the SSIMS helpdesk any logon problems that would result in a 6- to 12-month reporting delay. In addition, the officials said that (1) a significantly high percentage of the officials who have taken SSIMS training have indicated that SSIMS is one of the best, if not the best, computer database experiences they have had, (2) since July 2004, SSIMS has offered high speed encrypted connectivity to all NNSA sites, and (3) NNSA sites would not lose their SSIMS connection if the sites installed and used this high speed encrypted connectivity. The Director of the Office of Security

Technology and Assistance in the Office of Health, Safety, and Security agreed that the SSIMS database was not complete and therefore not useful for providing oversight; however, he felt the problem was with how the NNSA site offices were using the database.

Finally, NNSA has not implemented a formal process for sharing best practices or lessons learned to guide security improvements across the weapons complex. According to site office security officials, lessons learned have been informally shared in some instances, including monthly meetings with NNSA safeguards and security directors, teleconferences with contractor security officials, and the review of results from the Office of Independent Oversight inspections conducted at other sites. According to the Associate Administrator, he has taken the initiative to informally communicate lessons learned throughout the complex, but these lessons have yet to be fully implemented. For example, as early as February 2005, the DOE Inspector General identified problems with the retrieval of badges from terminated employees at the Los Alamos National Laboratory.[32] After the report was issued, the Associate Administrator sent the findings to NNSA site offices and requested that they review their respective processes. Nevertheless, the DOE Inspector General identified similar problems at other NNSA sites in subsequent reviews of their respective badge retrieval processes.[33]

While best practices and lessons learned have been communicated informally, it is important that NNSA sites have a formal means for communicating these lessons. Absent updated information in SSIMS, or a sufficient connection to it, it is difficult to determine whether proven corrective actions for security deficiencies identified have been implemented across the complex. Utilizing the existing SSIMS capability to identify how other sites address security deficiencies would significantly help alleviate redundancy of effort in addressing similar problems identified throughout the weapons complex.

[32]Inspection Report: Security and Other Issues Related to Out-Processing of Employees at Los Alamos National Laboratory, DOE/IG-0677 (Washington, D.C., Feb. 22, 2005).

[33]Inspection Report: Security Clearance Terminations and Badge Retrieval at the Lawrence Livermore National Laboratory, DOE/IG-0716 (Washington, D.C., Jan. 19, 2006) and Inspection Report: Badge Retrieval and Security Clearance Termination at Sandia National Laboratory—New Mexico, DOE/IG-0724 (Washington, D.C., Apr. 18, 2006).

Several Management Issues Need to be Resolved for NNSA to Become Fully Effective

NNSA and DOE have not yet addressed all of the problems that need attention to improve the management of the nation's nuclear programs. Problems continue, in part, because NNSA and DOE have not yet fully agreed on how NNSA should function within the department. In addition to addressing this underlying issue, NNSA could strengthen its ability to manage the nuclear weapons complex if it took additional action in four other areas: (1) human capital, (2) project management, (3) program management, and (4) financial management.

DOE and NNSA Have Not Yet Fully Determined How NNSA Should Operate as a Separately Organized Agency within DOE

NNSA has focused considerable attention on reorganizing its internal operations, but it and DOE continue to struggle with establishing how NNSA should operate as a separately organized agency within the department. Several factors have contributed to this situation. First, DOE and NNSA did not have a useful model to follow for establishing a separately organized agency in DOE. Second, the January 2000 implementation plan, required by the NNSA Act, did not define how NNSA would operate as a separately organized agency within DOE. As a result, although some NNSA programs have set up procedures for interacting with DOE, other programs have not, resulting in organizational conflict. Even where formal procedures have been developed, interpersonal disagreements have hindered effective cooperation. In this environment, concerns about NNSA's organizational status persist, with a January 2006 report by the Defense Science Board calling for the creation of a new, independent National Nuclear Weapons Agency. However, former senior DOE and NNSA officials with whom we spoke generally did not favor removing NNSA from DOE.

Other Federal Agencies Did Not Provide a Useful Model for How a Separately Organized Agency Should Be Structured

In its June 1999 report recommending the establishment of NNSA, the President's Foreign Intelligence Advisory Board suggested that the NNSA could be constructed in one of two ways: (1) by remaining an element of DOE, but becoming semi-autonomous, that is, separately organized within the department, or (2) by becoming completely independent, with its administrator reporting directly to the President. The Board cited several models for either course of action. If the first approach were chosen, the Board identified as potential models the National Security Agency, the Defense Advanced Research Projects Agency within the Department of Defense (DOD), and the National Oceanic and Atmospheric Administration within the Department of Commerce. If an independent agency approach were chosen, the Board cited the National Aeronautics and Space Administration and the National Science Foundation as potential models.

To determine if the agencies the Board cited could have provided useful models for how NNSA should be established as a separately organized agency within DOE, we met with officials from the Defense Advanced Research Projects Agency and the National Oceanic and Atmospheric Administration, as well as with officials from the Defense Threat Reduction Agency in DOD and the Federal Aviation Administration in the Department of Transportation. None of the officials associated with these four agencies considered their agency to be separately organized or believed that their agency's operational methods were transferable to NNSA. Officials of the respective agencies told us the following:

- *Defense Advanced Research Projects Agency*: The organization is not a separately organized agency but simply a part of DOD. The agency's internal operational staff is kept to a minimum, with considerable reliance on the department for many activities. For example, the Defense Finance and Accounting Service provides support for the agency's financial operations.

- *National Oceanic and Atmospheric Administration*. The Administration is considered a bureau within the Department of Commerce with no higher status than any other departmental bureau. In operational areas such as budget or personnel, both the Administration and the Department of Commerce have comparable offices, but it is understood that the Administration office is subordinate, with the Department of Commerce office having final decision-making authority.

- *Defense Threat Reduction Agency.* The agency is part of DOD. For all operational activities, guidance comes from DOD headquarters, and the agency is expected to follow the normal military chain of command.

- *Federal Aviation Administration.* The Administration is an operating administration under the Department of Transportation. It has no higher status than any other departmental administration, such as the Federal Highway Administration or the Federal Railroad Administration. In operational areas, such as the chief information officer, chief financial officer, and general counsel, the Administration receives direction from the cognizant departmental office. However, the Federal Aviation Administration does have separate authority for human resources and procurement.

Former and current senior DOE and NNSA officials also told us they had difficulty identifying any federal role model for a separately organized

agency. Absent such a role model, these officials said, NNSA was created using their best judgment about how a separately organized agency should be established.

DOE and NNSA Have Not Systematically Developed Standard Operating Procedures to Define Their Relationship

GAO's standards require federal agencies to establish and maintain an effective system of internal controls over agency operations.[34] We have noted that internal controls are particularly important for managing risk during organizational change, and we have emphasized one control—an agency's organizational structure—that we believe should clearly define key areas of authority and responsibility.

Section 3297 of the NNSA Act required DOE to submit a plan implementing the act's provisions to the relevant congressional committees.[35] However, DOE's January 1, 2000, implementation plan did little to define NNSA's status as a separately organized agency. Reflecting the opposition of the then DOE senior leadership to the creation of NNSA, the implementation plan dual-hatted virtually every significant statutory position in NNSA with DOE officials, including the Director of NNSA's Office of Defense Nuclear Counterintelligence and General Counsel. As we testified in April 2001, this practice caused considerable concern about NNSA's ability to function with the independence envisioned in the NNSA Act.[36] In its October 2000 report on the establishment of NNSA, the Special Oversight Panel on Department of Energy Reorganization noted that the Secretary, facing criticism for having impeded NNSA's autonomy, retreated from the dual-hatting philosophy and appointed separate individuals to NNSA offices. Dual-hatting was subsequently forbidden by an amendment to the NNSA Act.[37]

[34]GAO/AIMD-00-21.3.1.

[35]50 U.S.C. § 2401 note.

[36]GAO-01-602T.

[37]Pub. L. No. 106-398, § 3157, 114 Stat. 1654, 1654A-468 (2000) (codified as amended at 50 U.S.C. § 2410).

In a July 2000 hearing before the Special Oversight Panel, the incoming NNSA Administrator testified that establishing NNSA as a semi-autonomous entity would require developing a single, interconnected set of policies and principles that permeated the entire NNSA and minimized outside inputs. Nevertheless, DOE and NNSA have not systematically developed standard operating procedures to define their relationship. Consequently, although some NNSA programs have set up specific policies and procedures for how they will interact with their DOE counterparts, other programs have not. Without formal procedures, several functions—budgeting, procurement, information technology, management and administration, and safeguards and security—have not been effectively or efficiently implemented, as the following points detail.[38]

- *Budgeting*. DOE and NNSA do not have a formal order defining how DOE's and NNSA's budgeting requirements would be combined into a practicable process. As a result, according to NNSA officials, NNSA has had to follow both DOE's and NNSA's budgeting processes.

[38]In commenting on our draft report, DOE's Office of General Counsel indicated that it believed the prohibitions contained in the NNSA Act regarding "authority, direction, and control" prevented DOE and NNSA from better defining their working relationship. Sections 3202 and 3220 of the NNSA Act shield NNSA personnel, except for the NNSA Administrator and NNSA intelligence and counterintelligence personnel, from the authority, direction, and control of DOE personnel. See 42 U.S.C. § 7132, 50 U.S.C. § 2410. The Administrator is subject to the authority, direction, and control of the Secretary or Deputy Secretary of Energy, who cannot redelegate those powers. NNSA intelligence and counterintelligence personnel were also recently subjected to DOE authority, direction, and control, as we describe later in this report. In the view of DOE's Office of General Counsel, this statutory structure is the reason for ongoing coordination problems, regardless of whether formal procedures have been put in place between DOE and NNSA offices.

- *Procurement.* Although DOE made a commitment to issuing NNSA-specific acquisition procedures in its January 2000 implementation plan for NNSA, it has not done so. According to DOE Office of General Counsel officials, the department subsequently determined that the proposed NNSA-specific procedures were inconsistent with Federal Acquisition Regulations, the NNSA Act, and the January 2000 implementation plan. According to both DOE and NNSA officials, since 2004 the Department has blocked NNSA's efforts to issue its own acquisition regulations. As a result, according to NNSA officials, NNSA has had to issue a series of deviations to the DOE acquisition regulations to carry out NNSA acquisition policies in areas such as negotiating a more effective contract fee arrangement and awarding additional years to a contract's term.[39]

- *Information technology.* The DOE and NNSA offices of the Chief Information Officer have yet to reach agreement on a DOE order drafted in September 2004 to define the relationship between the two offices. According to DOE and NNSA officials, the draft order has not been made final because of DOE's concern that the NNSA office would have too great a role in tasks that should be performed by DOE's chief information officer. Absent this order, certain problems have developed. For example, according to a NNSA official, the two information offices verbally agreed that all direction given to NNSA contractors about information technology must come from NNSA, not DOE. However, because this guidance was not formally documented, NNSA contractors continue to receive dual requests for data from both the DOE and NNSA offices of the Chief Information Officer. According to an NNSA official, these dual requests have continually forced the contractors to rank the requests.

- *Management and administration.* DOE and NNSA do not have a formal process for obtaining DOE approval of NNSA-specific procedures, although the Congress authorized the Administrator to establish NNSA-specific policies unless disapproved by the Secretary of Energy.[40] However, DOE's Office of General Counsel has delayed the development of this process because it believes that NNSA should not be treated any

[39]Section 3262 of the NNSA Act requires the Administrator to establish procedures to comply with Federal Acquisition Regulations. See 50 U.S.C. § 2462.

[40]See 50 U.S.C. § 2402(d).

differently than any other departmental element and should thus be limited to using the flexibility already available in DOE orders. As a result, NNSA's efforts to promulgate Administration-specific procedures have become entangled in a cumbersome review process with no certainty that closure of that review will occur, according to NNSA officials. NNSA officials cited instances in which the Administration has attempted to promulgate NNSA-specific procurement regulations and policies on the roles of the DOE and NNSA Offices of the Chief Information Officer. In these instances, the review bogged down because a formal process for establishing NNSA-specific procedures did not exist.

- *Safeguards and security.* DOE and NNSA have not established formal procedures outlining the relative safeguards and security responsibilities of the DOE and NNSA offices that oversee contractor security activities. As a result, security officials at contractor facilities told us they have received safeguards and security oversight from a number of sources, including DOE; DNS; and the NNSA site offices that oversee the contractor facilities. Furthermore, the oversight they receive from these various sources can conflict. For example, DNS requires contractors to demagnetize electronic media before disposing of it. However, DOE Manual 470.4-4 requires physical destruction of electronic media through pulverization or other appropriate methods. Uncertain about which requirement to follow, the Sandia National Laboratories requested, and was subsequently granted by the NNSA Sandia site office manager, an exemption to DOE's physical destruction requirement. However, the Office of Independent Oversight reported that Sandia National Laboratories, the NNSA Sandia site office, and DNS had not fully evaluated the risks associated with following alternative destruction procedures. Sandia National Laboratories now follows the DOE requirement.

While the lack of formal procedures has adversely affected some functions, the presence of formal procedures has not always ensured that the roles and responsibilities of DOE and NNSA offices are clearly defined and that the offices operate together effectively and efficiently. Specifically, the original NNSA Act prescribed roles and responsibilities for DOE's Office of Counterintelligence and NNSA's Office of Defense Nuclear Counterintelligence. Under section 3204 of the NNSA Act, the director of DOE's Office of Counterintelligence was responsible for establishing policy for counterintelligence programs and activities at departmental facilities. At the same time, section 3232 of the NNSA Act specified that NNSA's Chief

of Defense Nuclear Counterintelligence was responsible for developing and implementing the Administration's counterintelligence programs.

To better define the relationship between the two counterintelligence offices, DOE issued a Secretarial Policy Memorandum in January 2001 and a DOE order in December 2004. The Secretarial memorandum, in part, directed that the DOE headquarters counterintelligence program offices would be a shared resource between the DOE Office of Counterintelligence and the NNSA Office of Defense Nuclear Counterintelligence but that the funding needed for those program offices would come from DOE's Office of Counterintelligence budget. The December 2004 DOE order contained similar provisions but specified that the headquarters inspections and polygraph programs would be directed solely by the Director of DOE's Office of Counterintelligence.

According to DOE and NNSA counterintelligence officials, the organizational relationship created by the Secretarial memorandum and the DOE order led to the following problems:

- DOE and NNSA counterintelligence officials have disagreed over the scope and direction of the counterintelligence program. NNSA counterintelligence officials would like NNSA's counterintelligence program to emphasize a multifaceted and proactive approach to prevent intelligence activity. This program would integrate all of the tools of the shared counterintelligence program offices—Analysis; Operations and Investigations; Plans, Policy, Training and Awareness; and Information and Special Technologies—as well as the DOE-directed Polygraphs and Inspections program office. However, DOE's Office of Counterintelligence emphasized a reactive approach to counterintelligence—one that primarily focused on investigating counterintelligence incidents that have already occurred. NNSA counterintelligence officials stated that they would have liked to have changed the scope and direction of the NNSA counterintelligence program. However, such changes require the concurrence of DOE's Office of Counterintelligence, according to NNSA counterintelligence officials, which did not occur.

- DOE and NNSA counterintelligence officials also disagreed over their ability to jointly direct the staff in the headquarters counterintelligence program offices. Funding for these offices was included in DOE's counterintelligence budget, and DOE's Office of Counterintelligence senior management provided the program office directors with their

performance rating, with advisory input from the NNSA counterintelligence office. Consequently, NNSA counterintelligence officials believed that NNSA had less leverage in assigning tasks to the program office staff, while DOE counterintelligence officials believed that the DOE and NNSA counterintelligence offices had equal leverage.

- DOE and NNSA counterintelligence officials disagreed over the allocation of counterintelligence resources. The NNSA Chief for Defense Nuclear Counterintelligence believed that counterintelligence resources should be allocated according to risk management and priority-setting principles. She noted that the risk associated with NNSA nuclear weapons facilities was generally higher than the risk associated with other DOE facilities because the loss of nuclear weapons information or materials to foreign intelligence would constitute a serious breach of national security. Therefore, in an August 2005 memorandum, the NNSA chief asked the Director of DOE's Office of Counterintelligence to comprehensively evaluate whether resources could be redirected to benefit higher-risk counterintelligence targets and to provide guidance for future decision making about resource allocation. As of November 2006, the DOE director had not responded to the NNSA memorandum.

- DOE and NNSA counterintelligence officials disagreed over counterintelligence policymaking. For example, from September 2004 to August 2005, the NNSA counterintelligence office unsuccessfully attempted to obtain the DOE counterintelligence office's concurrence on issuing a joint DOE/NNSA policy on personnel security file reviews and sharing of counterintelligence information. When the DOE counterintelligence office did not respond, the NNSA counterintelligence office issued a NNSA-specific policy on August 12, 2005. This issuance without DOE's concurrence sparked a series of verbal and e-mail exchanges between DOE and NNSA counterintelligence officials, according to NNSA officials. DOE counterintelligence officials stated in the e-mails we reviewed that NNSA did not have the authority to issue NNSA-specific counterintelligence policy without DOE concurrence. As such, the DOE counterintelligence office initially demanded that the NNSA office retract the policy. Subsequently, in April 2006, the DOE counterintelligence office issued a memorandum that embraced the NNSA policy.

- DOE and NNSA counterintelligence officials disagreed over, or were confused about, their roles and responsibilities in handling specific counterintelligence matters. A case in point was the department's handling of the well-publicized mid-2005 intrusion into an unclassified NNSA computer system and removal of the names and social security numbers of 1,502 individuals working for NNSA. The 1,502 NNSA individuals were not notified of this incident until June 2006, after the incident was acknowledged during a congressional hearing held earlier in the month. Subsequently, the Secretary of Energy requested that the Office of Inspector General examine the department's response to this incident. In its July 2006 report, the Inspector General identified multiple factors that contributed to the lack of a timely response to this incident, including the delay in notifying the 1,502 NNSA individuals that certain personal information had been compromised. The Inspector General recommended that the department redefine and clarify the roles and responsibilities of DOE and NNSA counterintelligence officials.

DOE and NNSA counterintelligence officials told us that they spent an enormous amount of time resolving these types of problems between the two offices and that this effort detracted from their focus on counterintelligence activities. According to NNSA counterintelligence officials, the arrangement did not meet the intent of the NNSA Act to create a separately organized counterintelligence program within NNSA. As a result, these officials added, NNSA's ability to execute a separate counterintelligence program that meets its unique needs was impeded and largely limited to what the two counterintelligence offices could agree on.

Subsequently, the Congress amended the NNSA Act to address the problems with the NNSA's and DOE's counterintelligence programs. Specifically, section 3117 of the John Warner National Defense Authorization Act for Fiscal Year 2007 contained provisions to consolidate the counterintelligence programs of DOE and NNSA under the Department of Energy.[41] Section 3117 also established the Intelligence Executive Committee within the Department of Energy, consisting of the Deputy Secretary of Energy, who would chair the committee, and each Under Secretary of Energy. The section requires the Secretary of Energy to use the committee to assist in developing and promulgating the counterintelligence and intelligence policies, requirements, and priorities

[41]Pub. L. No. 109-364, § 3117 (2006).

of the entire Department. The section also established within the staff of the Administrator, NNSA, a position of NNSA Intelligence and Counterintelligence Liaison who would be responsible for liaison between the NNSA and the Department's Office of Intelligence and Counterintelligence. The amendment sunsets on September 30, 2010, and the NNSA functions, personnel, funds, assets, and other resources transferred to the Secretary of Energy will be returned to the control of the Administrator, NNSA.

The conference report stated that the Congress reluctantly provided this authority to consolidate the program despite the ongoing skepticism of many in the Congress over the Department's ability to implement a strong security program for the Department and its laboratories.[42] The conference report noted that with the recent Departmental initiative to combine the Offices of Intelligence and Counterintelligence and with the authority provided in this provision, the intelligence and counterintelligence functions would be organized as they were when the Department experienced significant counterintelligence problems. The conference report stated that the conferees believed that the Department could have addressed many of the perceived issues associated with having separate counterintelligence offices for the Department and NNSA by demonstrating greater management resourcefulness. The report also stated that the conferees were unpersuaded that the Department fully and faithfully implemented the counterintelligence program structure called for in the NNSA Act.

Nevertheless, the conference report noted that the Department had continued--under the leadership of two different Secretaries of Energy and two different Deputy Secretaries--to identify the counterintelligence structure of the NNSA Act as an impediment to the smooth functioning of security operations within DOE. Therefore, the conferees agreed to include a provision that would provide temporary authority for the disestablishment of the Office of Defense Nuclear Counterintelligence within NNSA and the transfer of NNSA counterintelligence personnel to the Department's Office of Counterintelligence. DOE officials told us that they are in the process of developing plans to implement the consolidation of the counterintelligence programs and expect full implementation in early 2007. According to these officials, the consolidation should be a seamless

[42]H.R. Conf. Rep. No. 109-702 at 969-971 (Sep. 29, 2006).

process and will provide the leadership necessary to effectively implement DOE's counterintelligence activities.

External Entities Continue to Express Concern about NNSA's Organizational Relationship

Almost 7 years after NNSA was created, concerns persist about the organization and management of the nuclear weapons complex that led to NNSA's establishment. For example, in January 2006, DOD's Defense Science Board Task Force on Nuclear Capabilities reviewed alternative institutional arrangements that it believed could provide for more efficient management of the nuclear enterprise. The task force expressed concern that other elements of DOE were continuing to micromanage NNSA. To correct this situation, the task force proposed the following three options:

- *Reform the existing structure*. The task force would accomplish this reform by having the Secretary of Energy enforce the requirement that the Administrator be autonomous and accountable only to the Secretary. The task force believed that this approach would require a significant change in DOE culture, but it had little confidence in the prospect for effective, lasting change within DOE.

- *Move NNSA to DOD*. The task force believed that there was more confluence between DOD's core missions and the nuclear weapons complex. However, the task force noted that, historically, the Congress has been reluctant to concentrate nuclear weapons authority in a single department and that, on balance, DOD was not a good fit for the development and production of nuclear weapons.

- *Create a National Nuclear Weapons Agency.* The task force supported this option, believing that the nuclear weapons enterprise was unique in its missions and the demands placed upon managers and that a unique organizational approach was therefore warranted. The National Nuclear Weapons Agency would report through a Board of Directors, comprising the Secretaries of several cabinet offices, including Energy and Defense, to the President.

However, former senior DOE and NNSA officials, as well as, one Defense official with whom we spoke, generally did not favor removing NNSA from DOE. These officials included the first and second Administrators of NNSA, the former Deputy Secretary of DOE, and a senior member of the Defense Science Board Task Force responsible for the January 2006 report. These officials offered the following comments on NNSA's organization:

- According to the second NNSA Administrator, it would not be a good idea to make NNSA a totally independent agency. The Administrator indicated that NNSA is very much entangled in the operations of DOE and the costs associated with making NNSA totally independent from DOE would outweigh the benefits.

- One former senior official told us he never knew what it meant to have NNSA as a separately organized agency. In this official's view, because DOE and NNSA had not clearly defined the concept, there was some uncertainty in the relationship between the DOE Secretary and the Administrator of NNSA. While this official would not be in favor of establishing NNSA as a totally separate agency, he believes that NNSA needs to take a half-step away from DOE to gain more independence.

- According to another former senior official, the DOE/NNSA organizational relationship might have benefited from a more formal definition. Regarding organizational changes, in this official's view, the Congress should either make NNSA a totally independent agency or fold it back into DOE.

- NNSA is not a separately organized agency, a Defense Science Board Task Force official told us. In this official's view, DOE ensured that fate by deciding, in its 2000 implementation plan, that certain functions would not be transferred to NNSA. When NNSA was created, this official said, the Congress was clear in the enabling legislation about the type of entity it wanted NNSA to be. However, the Congress has allowed the problems associated with DOE's implementation to languish.

NNSA Needs to Fully Resolve Its Human Capital Issues

Under GAO's internal control standards, agencies should ensure that they have a sufficient number of staff, particularly in managerial positions, and that staff have the skills required to carry out the agency's organizational objectives. While NNSA has engaged in a variety of human capital activities since its creation, DOE and NNSA have yet to fully determine the appropriate size of their respective workforces.

In its January 2000 NNSA Implementation Plan, DOE outlined a series of steps it would take to staff NNSA. In order to be prepared when the NNSA Act took effect on March 1, 2000, DOE indicated that current employees assigned to those program offices that would become part of NNSA would be transferred to NNSA. For other employees, such as those in

departmental support offices, DOE stated that a more detailed analysis would be necessary to determine those employees subject to transfer.

In February 2002 testimony before the Special Oversight Panel on Department of Energy Reorganization of the House Armed Services Committee, the then Administrator stated that NNSA was taking a "phased approach" to assess the status of each NNSA function and the costs and benefits of continued reliance on DOE for service. For example, in the area of human resources, the former Administrator stated that NNSA had decided to develop an independent capability to select, promote, and develop its own executive workforce. In other areas, such as the investigation of serious accidents, NNSA would continue to rely on DOE personnel. However, DOE and NNSA have never conducted a systematic, detailed analysis of NNSA's staffing needs in relation to DOE's.

During this review, we identified areas where potential staff imbalances have affected NNSA's ability to operate as a separately organized agency within DOE. These imbalances occur even though NNSA's federal staff deals with about 40 percent of DOE's budget and programs, according to a June 2006 DOE analysis. The imbalance is most notable in NNSA's Office of General Counsel. Section 3217 of the NNSA Act established the position of the NNSA General Counsel to serve as NNSA's chief legal officer. Initially, DOE assigned the DOE General Counsel to also serve as the NNSA General Counsel. This dual-hatting was subsequently prohibited by an amendment to the NNSA Act.[43] NNSA has since hired a General Counsel and 34 other attorneys to provide NNSA with legal advice and analysis. In contrast, the rest of DOE has 277 attorneys. According to NNSA's General Counsel, who has been at NNSA since September 2001, no formal analysis of his office's staffing needs has ever been done. However, he believes that such an analysis would show that his office needs about 15 to 20 additional attorneys to fully handle NNSA's legal workload with minimal assistance from DOE. Absent additional attorneys, NNSA must rely on DOE's Office of General Counsel to perform a significant portion of its legal work.

The June 2006 DOE analysis also showed a large difference between the size of the NNSA federal staff compared with the rest of DOE federal staff in other areas. NNSA concurred with this analysis. (See table 7.)

[43]Pub. L. 106-398, § 3157, 114 Stat. 1654, 1654A-468 (2000) (codified as amended at 50 U.S.C. § 2410).

Table 7: Staffing Levels within NNSA and DOE Offices

Function	NNSA staffing	DOE staffing
Public Affairs	16	74
Congressional Affairs	5	23
Security	131	181
Planning, Programming, Budgeting, and Evaluation	124	555
Information Technology	50	522

Source: DOE Office of Human Capital Management.

According to the first Administrator, because of the difference in staff size, DOE can control NNSA's agenda by deciding which issues will get reviewed and when. In his view, this problem began when NNSA was created and has only gotten worse. He also stated that because NNSA did not have a plan for how it would fully staff its headquarters organization, he tried to hire the people he needed one at a time. An April 2005 NNSA report on its security program raised similar concerns,[44] noting that the disparity in size between NNSA and DOE headquarters staffs greatly impaired NNSA's effectiveness within the headquarters bureaucracy. For example, the report said, DOE dominated the development of security policy because its staff was significantly larger. In addition, a May 2005 NNSA staffing analysis noted that the far larger DOE staff are able to devote considerable effort to "second-guessing" NNSA actions or to excessive requests for data and that other DOE staff sometimes seek to interfere with NNSA.

[44]*NNSA Security: An Independent Review*, April 2005.

Reconciling any disparity between the size of the NNSA and DOE staffs, and determining the staff NNSA needs to carry out its overall mission, should take place within the context of a broader, data-driven workforce plan. In December 2001, we reported that NNSA did not have the coherent human capital and workforce planning strategies it needed to develop and maintain a well-managed workforce over the long run. We therefore recommended that, before NNSA allocated any additional excepted service positions, it develop a thorough human capital and workforce planning strategy.[45] In June 2004, we reported that while the workforce plan NNSA developed in December 2003 attempted to establish a framework for long-term workforce planning, the plan was of limited use because it did not have current statistics on workforce, positions, and organizational structures.[46] Furthermore, the downsizing NNSA was completing at the time was taking place in an unstructured environment. Under these conditions, agencies can experience significant challenges in deploying people with the right skills, in the right places, and at the right time, and in ensuring that they perform their missions economically, efficiently, and effectively. In NNSA's case, we noted at the time that there were early indications that the lack of planning was contributing to skill imbalances such as those imbalances in security staff already discussed. We further stated that without a functional long-term workforce plan, NNSA ran the risk of facing more serious staff shortages or skill imbalances in the future, which would affect its ability to adequately oversee its contractors and ensure the safety and security of its various facilities.

To its credit, NNSA has recognized that it needs to improve its human capital management, and in a November 28, 2005, memorandum to NNSA senior managers, the Administrator announced a workforce planning initiative. The Administrator acknowledged that NNSA had no systematic way to assess current, or forecast future, human capital needs. Consequently, he asked the NNSA Office of Human Resources to develop and refine a workload analysis and planning approach. While the Administrator expected that this approach would be usable by the middle of fiscal year 2006, according to the Director for NNSA's Office of Human Resources, he made certain changes to the workload analysis to ensure that more appropriate data could be collected. As a result of those changes,

[45]GAO-02-93R.

[46]GAO-04-545.

the Director said, the workload analysis and planning approach would take longer to complete.

NNSA Can Take Additional Action to Improve Project Management

Project management remains a significant concern for NNSA and DOE and, over the last several years, both have initiated improvement efforts. For example, NNSA has implemented earned value management systems to improve project reporting, conducted independent project reviews to diagnose problem areas before the projects are executed, and, in April 2006, completed training and certifying its project managers. In July 2006, DOE issued a new program and project management order. Nevertheless, DOE's fiscal year 2006 performance and accountability report still identified project management as a significant issue. Furthermore, according to NNSA's November 2006 report on project management performance, 5 of 31 NNSA projects, or about 16 percent, are in jeopardy of breaching their cost baseline, schedule baseline or both. To further improve NNSA's project management performance, we identified seven areas for additional action.

- *Develop a project management policy.* Any improvement requires a policy that clearly articulates management's vision. While NNSA has been involved in drafting a revised DOE order on project management, and creating and promulgating DOE project management guides, in an April 2003 memorandum, the NNSA Administrator committed to issuing an NNSA-specific project management policy to (1) further assist in the implementation of the DOE project management manual issued in March 2003 and (2) assure consistent application with the NNSA Act. However, according to an official in NNSA's Office of Project Management and Systems Support—which would be responsible for developing a project management policy—no NNSA project management policy has been issued.

- *Prepare a project management improvement plan.* Short- and long-range plans are critical to implementing a project management policy. However, NNSA developed its last project management improvement plan in December 2000. According to information presented at NNSA's 2005 Project Management Training Workshop, the Administration successfully accomplished many of the eight goals in this plan, including using qualified, experienced project managers to oversee NNSA projects and establishing formal procedures for obtaining senior manager review and approval of projects. However, the NNSA staff presenter at the workshop also noted that NNSA was not completely successful in

creating a cultural shift in NNSA that emphasizes the importance of project management or creating incentives to improve project managers' performance. As a result, NNSA has not significantly reduced project delivery times or costs. The NNSA staff presenter, therefore, proposed the development of new short- and long-range improvement plans, which officials from NNSA's Office of Project Management and Systems Support acknowledged the Administration currently does not have. While these officials acknowledged the need for such plans, NNSA management indicated that it was not aware of the staff proposal.

- *Prepare project management annual reports.* After its creation, NNSA began preparing an annual status report to the Congress on its construction project accomplishments. However, it submitted only two reports—for fiscal years 2000 and 2001. In fiscal year 2000, NNSA reported, among other things, that about 70 percent of its Defense Programs' 46 projects were progressing satisfactorily and that Defense Programs had many success stories during the year, including (1) reestablishing the quarterly project review process, (2) developing and implementing a project management improvement plan, and (3) sponsoring a project management workshop. However, NNSA also reported that the root causes of project management problems were deeply entrenched and could not be eliminated without a basic cultural change, which would require at least 3 years. In fiscal year 2001, NNSA reported that 30, or about 73 percent, of its 41 projects were progressing satisfactorily and noted accomplishments in project management. However, NNSA also reported that (1) management costs for projects were nearly double those of other organizations and (2) projects took approximately 3 years longer to accomplish than similar projects performed elsewhere. The Director of NNSA's Office of Project Management and Systems Support—who assumed his position in 2004—did not know why the reports were discontinued. Other NNSA officials in the Office of Project Management and Systems Support told us that the reports were discontinued because statements, such as those contained in the fiscal year 2001 report, cast NNSA in too unfavorable a light.

- *Include major projects in the Project Assessment and Reporting System (PARS).* In 2001, DOE implemented PARS—a Web-based system for keeping DOE senior managers apprised about the performance of projects costing more than $5 million. In response to a February 2004 memorandum from the Deputy Secretary of Energy citing inadequate management of critical activities within DOE and NNSA, NNSA

indicated that it intended to treat more of its activities as projects so that the cost and schedule performance associated with those activities could be improved. While NNSA has applied project management principles to more of its activities, we identified four major NNSA projects—estimated to cost over $100 million each—that are not enrolled in the PARS system and do not receive senior management oversight through that system (See table 8.) NNSA indicated that these projects are not in PARS because they are information technology projects or programmatic efforts. However, we believe each listing in table 8 meets DOE's definition of a project because it has a defined start and end date. In addition, information technology projects are not prohibited from inclusion in PARS.

Table 8: Major Projects Not Included in PARS

Project name	Description
B-61 Life Extension	NNSA expects this project, designed to extend the service life of the B-61 bomb, to cost about $287 million between fiscal years 2005 and 2009.[a]
W-76 Life Extension	NNSA expects this project, designed to extend the service life of the W-76 nuclear warhead by replacing components, to cost about $1.05 billion between fiscal years 2005 and 2011.
Enterprise Project	NNSA increased the total cost of this project, which will replace the accounting and management systems at Los Alamos National Laboratory, from about $70 million when it was initiated in 2001 to nearly $160 million.
Purple and BlueGene/L Supercomputers under the Advanced Simulation and Computing Program	NNSA expects this project to cost about $290 million.

Source: GAO analysis of DOE information.

Note: The W-80 Life Extension was also not included as a project in PARS; however, NNSA recently announced that this effort was being terminated.

[a]The cost for the B-61 and W-76 life extension projects is contained in NNSA's fiscal year 2007 budget.

We are particularly concerned that the life extension projects were not included in the PARS database. In our July 2003 report on NNSA's life extension program, we recommended that NNSA establish the individual life extensions as projects and manage them according to DOE's project management requirements.[47] As we reported, the then NNSA Deputy Assistant Administrator for Military Application and Stockpile Operations acknowledged that the three life extensions were projects, and NNSA concurred with our recommendations. During our current review, however, we could not find any evidence that NNSA had taken any action to establish the life extensions as projects.

- *Complete a lessons learned report database*. DOE's project management manual states that a lessons learned report should be completed, distributed, and included in a project's permanent file; however, the manual does not require the establishment of a comprehensive lessons learned project management database. To its credit, the Administration has attempted to create such a database on one of its internal Web pages, but we found that certain key NNSA lessons learned reports were not included, including, for example, reports for NNSA's Accelerated Strategic Computing Initiative and W-87 Life Extension. We believe that these reports provided information worthy of dissemination across the NNSA complex. For example, the W-87 lessons learned report noted that the project plan was prepared too late in the development cycle and was not used as a tool to identify problems and take corrective actions. In addition, the Accelerated Strategic Computing Initiative report noted that the Lawrence Livermore and Los Alamos National Laboratories had mixed success, in part, because they did not look at the lessons learned from other communities. While officials in the Office of Project Management and Systems Support acknowledged that the Web page was incomplete, they said the forthcoming DOE project management order would reinforce the importance of lessons learned information. However, the final order, issued in July 2006, did not discuss a lessons learned database; instead, it required that a lessons learned report be prepared and submitted to DOE's Office of Engineering and Construction Management for broader sharing among the DOE project management community. According to that office, it has yet to develop internal procedures for sharing this information.

[47]GAO, *Nuclear Weapons: Opportunities Exist to Improve the Budgeting, Cost Accounting, and Management Associated with the Stockpile Life Extension Program*, GAO-03-583 (Washington, D.C.: July 28, 2003).

- *Develop contractor performance benchmarks*. Benchmarking is an integral part of project management.[48] It is used to analyze the gap between actual and preferred performance in order to identify opportunities for improvement. We found that while NNSA tracks cost and schedule performance on individual projects through various reporting systems, including information contained in the PARS system, neither the PARS system nor any other departmental system ranks the collective project management performance of NNSA's contractors. On its own initiative, however, the Los Alamos National Laboratory contracted in 2004 to have its project management performance benchmarked against comparable organizations. The August 2004 report found that, on a scale of 1 to 5, with 1 as the lowest, Los Alamos' project management rated a 2. Los Alamos had project management processes, although such processes were not considered an organizational standard on all projects. According to NNSA site office managers we contacted, it would be helpful to know how their contractor ranked in project management performance against other NNSA contractors. The Sandia Site Office Manager added that this ranking, as well as an NNSA national average, would help determine if project management at her laboratory was doing well or not. Overall, the managers added, if their contractor's project management performance was not at a comparable level to other contractors, they could identify problems and develop solutions.

[48]*Measuring Performance and Benchmarking Project Management at the Department of Energy*, National Research Council of the National Academies, 2005.

- *Require contractors to receive project manager training.* DOE and NNSA have initiated a program to train and certify all departmental project managers on projects costing $5 million or more. However, because departmental projects are usually undertaken by an outside contractor, the training of the contractor's project manager is equally important. Several studies conducted at the request of either DOE, NNSA or their contractors have recommended training and certifying contractors' project managers. For example, in 1999, the National Research Council found that the lack of project management skills was a fundamental cause of poor project performance and recommended that DOE require all contractors' project managers to be experienced, trained, and qualified in project management appropriate to the project.[49] Similarly, in 2004, the Civil Engineering Research Foundation reported that project management competence was a critical factor in project success and recommended that formal project management training of contractor project managers be made a contract requirement.[50] Despite this support for contractor project manager training and certification, neither DOE nor NNSA has a policy on contractor project manager training. According to an NNSA official, the Administration has taken the position that it will stipulate in its contracts what it wants accomplished and then leave it up to the contractor to determine how best to achieve NNSA's requirements.

NNSA Can Also Improve Program Management Through Additional Action

Program managers are responsible for accomplishing an organized set of activities directed toward a common purpose or goal. To fulfill that responsibility, NNSA program managers are expected to have a working knowledge of such diverse areas as contracting, budgeting, and engineering. Recognizing the importance of program managers, NNSA has taken several actions, such as initiating a project and program management improvement team and developing a program management policy. However, DOE's performance and accountability reports indicate that additional improvements in program management are possible. For example, according to DOE's fiscal year 2006 performance and accountability report, NNSA fully met only about 52 percent of its program

[49]*Improving Project Management in the Department of Energy,* National Research Council of the National Academies, 1999.

[50]*Independent Research Assessment of Project Management Factors Affecting Department of Energy Project Success*, Civil Engineering Research Foundation, July 12, 2004.

goals, compared with about 79 percent for the rest of DOE. Similarly, according to departmental information, NNSA met about 74 percent of its performance targets from fiscal years 2002 through 2006, compared with 87 percent for the rest of DOE. To further improve its program management performance, NNSA will need to take the following actions:

- *Prepare status reports on program management improvement.* In any performance-based management system, once a problem has been identified, a corrective action plan is prepared and reports are generated to periodically evaluate the status of the corrective action. In a July 2004 memorandum to the DOE Under Secretary, NNSA indicated that each NNSA office would prepare a corrective action plan, known as a program management implementation plan. While all NNSA offices completed at least a portion of these implementation plans, only the offices of Defense Programs, Nuclear Nonproliferation, and Defense Nuclear Security outlined specific tasks, or deliverables, in their plans that needed to be completed. More importantly, of these offices, only Defense Programs and Nuclear Nonproliferation identified a due date for each task. Plans prepared by the offices of Emergency Operations, and Infrastructure and Environment did not include any specific tasks or due dates. Moreover, none of the NNSA offices have prepared periodic reports on the status of their efforts to improve program management. Therefore, it is unclear how much progress each NNSA office has made.

- *Complete a best practices guide on program management.* In response to the Government Performance and Results Act, agencies have learned that they can improve performance by emulating the best practices of leading organizations. In October 2003, an internal review of NNSA's program management found that, among other things, NNSA needed to have (1) a common language and terminology about program management, (2) consistency in program manager functions and qualifications, and (3) a clear channel of direction and consistent and timely flow of information from NNSA programs to contractors.[51] It recommended that NNSA develop and issue a best practices guide by December 1, 2003. The draft guide was never issued in final form and

[51]Formally termed the NNSA Program Management Workload Reduction Team, the team's charter was to arrive at a realistic, uniform, and timely approach for optimizing and implementing Federal management processes across NNSA.

disseminated within NNSA.[52] According to a NNSA official and a NNSA contractor official who served on the program management team, the best practices guide floundered after NNSA made certain organizational and employee changes and the guide no longer had a person serving as a champion of program management improvement.

- *Identify and train program managers*. NNSA's August 2004 program management policy largely superseded earlier NNSA team recommendations on program manager training.[53] According to the August 2004 policy, NNSA's Office of Management and Administration was responsible for developing and maintaining a database of NNSA program managers to identify (1) the manager for each program, (2) the training and certification requirements for each program manager position, (3) the dates the program manager initially completed various training and certifications, and (4) when, if applicable, the training and certification must be renewed. The policy did not stipulate any deadline for the database's completion. Consequently, according to an official in NNSA's Office of Management and Administration, this program manager database has not been created. In contrast, according to an official in DOE's Office of Engineering and Construction Management, the department has developed a training curriculum for DOE program managers with approval of that curriculum by the DOE Deputy Secretary expected in the next few months. Unlike the NNSA program management policy, DOE will not initially require that program managers be certified on the amount of training received.

[52]NNSA's Office of Defense Programs has issued a best practices document to assist its program managers in the preparation of program plans.

[53]Two NNSA program management improvement teams, one established in 2002 and the other in 2003, recommended training program managers. For example, the 2003 team noted that there was a finite set of officially designated NNSA program managers who needed to be trained and certified to a minimum set of qualification standards and recommended an implementation schedule to have all NNSA program managers named by January 1, 2004, and a policy setting out program management qualification standards implemented across NNSA by October 1, 2004.

Certain Financial Management Weaknesses Remain Despite NNSA Improvements

Under section 3252 of the NNSA Act, NNSA had to develop a planning, programming, and budgeting process that comported with sound financial and fiscal management principles.[54] The NNSA Act also requires NNSA to annually submit to the Congress a Future Years Nuclear Security Program plan that details NNSA's planned expenditures for the next 5 years.[55] Very early in his tenure, the first NNSA Administrator indicated that he intended to comply with the NNSA Act by instituting a planning, programming and budgeting process similar to DOD's. While DOD's approach has not been without its problems over the past 40 years, it is generally recognized as a system that, when properly led and staffed, can provide cost-effectiveness comparisons and develop the detailed program and budget plans called for in the NNSA Act. Although NNSA has made significant progress in implementing its PPBE process over the last 4 years, it still needs to (1) complete its PPBE policy guidance, (2) establish an independent analysis unit to assist the Administrator in making budget allocation decisions, (3) develop criteria for compiling an NNSA-wide priorities list, (4) develop an up-to-date schedule of those programs requiring budget validation, and (5) establish a DOE-compliant budget validation process.

- *Complete NNSA's PPBE policy.* As recognized in Office of Management and Budget (OMB) Circular A-123, an important part of internal controls over financial reporting is having policies and procedures in place to ensure that management directives are carried out and that management's assertions in its financial reporting are valid. To this end, NNSA has issued 10 policy letters providing guidance to NNSA staff on various aspects of the PPBE process: 6 of these 10 letters are final, 3 have been in draft for more than 1 year, and 1 has been in draft for more than 2 years. According to the director of NNSA's Office of Planning, Programming, Budgeting, and Evaluation, the four draft policy letters have not been made final, in part, because NNSA has been waiting to see DOE's position on issues in the draft letters. However, we believe that waiting 2 years for DOE's views is inconsistent with NNSA's operation as a separately organized agency with its own PPBE budgeting process. NNSA indicated that it is continuing to evaluate aspects of the PPBE budgeting process and expects to finalize at least three of the draft policy letters during fiscal year 2007.

[54]50 U.S.C. § 2452.

[55]50 U.S.C. § 2453.

- *Establish an independent analysis unit.* PPBE provides a mechanism for centralized resource allocation decisions. In NNSA, that mechanism consists of having senior NNSA managers develop a budget for their program and then collegially review, through a management council, the budgets from the other programs, including the programs' justification for additional resources to meet requirements they cannot fund within their target allocation. The council can either decide to shift funding between programs to meet such requirements or determine whether the issue should be presented to the Administrator for resolution. The Administrator reviews the council's decisions, resolves issues identified by the council, and makes final resource allocation decisions. Such a mechanism places considerable pressure on the Administrator alone to make difficult funding decisions.

  While the NNSA PPBE process was modeled after the process DOD uses, it differs markedly in one aspect. Unlike DOD, NNSA has not established an independent group responsible for reviewing program proposals, verifying cost estimates, and analyzing alternatives. In August 2003, DOE's Office of Inspector General reported that most NNSA senior managers interviewed believed such an analytical group could be of value.[56] For example, the then NNSA Acting Associate Administrator for Management and Administration said that he supported the formation of such a group to provide objective analyses to the Administrator when he had to move resources between programs. Several senior managers also stated that resource allocation decisions among program offices were likely to become more frequent in future years and, therefore, NNSA's need for independent analytical services was likely to grow. Although NNSA agreed with the Inspector General's recommendation regarding the need for an independent analytical support group, it did not believe that such a group could be created before the end of calendar year 2005, after downsizing and reorganization had been completed.

  NNSA indicated that its management is fully supportive of the importance of independent analysis at both the NNSA and DOE level, but mindful that the resources needed to create this capability must be balanced with all of the competing needs within NNSA in a highly constrained funding and staffing environment. However, in our view, in

[56]Audit Report: National Nuclear Security Administration's Planning, Programming, Budgeting, and Evaluation Process, DOE/IG-0614, Aug. 5, 2003.

such an environment, the need for an independent budget analysis unit to ensure that appropriate budgetary decisions are made becomes even more important.

- *Develop criteria for compiling an NNSA-wide priorities list.* In order to make trade-off decisions among organizations and programs within an organization, DOE formally requires each of its organizations to annually submit a report to its Office of Budget that ranks its programs for the budget year and provides a rationale for the ranking. As we noted in July 2003, NNSA did not submit these ranking reports for fiscal years 2002 through 2004.[57] It submitted a list for the first time for the fiscal year 2007 budget, after the Secretary of Energy specifically requested it. According to an NNSA budget official, each NNSA program, such as Defense Programs and Nuclear Nonproliferation, prepared its list individually. Afterwards, this official stated, the NNSA Administrator compiled an overall priority list without using any formal criteria.

  According to an official in DOE's Office of Budget, his office had some questions about the ranking of activities on the NNSA list. For example, the impact associated with not funding a particular activity was not always sufficiently clear to explain NNSA's ranking rationale. While NNSA subsequently answered all of the Office of Budget's questions satisfactorily, he noted that NNSA might have benefited from preparing and following some formal criteria for developing its priority ranking list, as do other DOE organizations, such as the Office of Environmental Management. Formal criteria, in this official's view, would consider the impact of not funding an activity plus the probability of success if additional funding occurred.

  NNSA indicated that it annually issues strategic planning guidance and program and fiscal guidance, holds internal NNSA office programming sessions, and convenes a senior NNSA leadership meeting to discuss the various NNSA office proposals. NNSA added that, considering all these actions and balancing competing priorities, the Administrator makes his decisions which are documented in the Administrator's Final Recommendations report. In our view, having formalized criteria to follow would assist the Administrator in making his decisions and render those decisions more transparent and defensible to outside review.

[57]GAO-03-583.

- *Develop an up-to-date schedule of those programs requiring budget validation.* Under the PPBE process, once NNSA establishes the relative priority of its programs, the budget associated with those programs must be developed and validated. During validation, NNSA evaluates the need for the program's proposed activities and the cost estimates in support of those activities. In a May 2004 memorandum, NNSA's Office of Management and Administration announced the Administration's 5-year schedule for conducting budget validations for fiscal years 2005 through 2009. NNSA indicated that it would select programs for validation on the basis of several factors, including programs receiving OMB Performance Assessment Rating Tool reviews, program manager requests, Administrator direction, significant external interest, and high program visibility. Using those factors, for fiscal year 2006, NNSA planned to validate the budgets for the Office of the Administrator, Science Campaign, Readiness Campaign, Safeguards and Security, International Nuclear Materials Protection and Cooperation, Elimination of Weapons-Grade Plutonium Production, and Naval Reactors Operations and Maintenance, and for the fiscal year 2007 budget, it would validate Directed Stockpile Work/Stockpile Services, Nuclear Weapons Incident Response, Nonproliferation and Verification research and development, and Highly-Enriched Uranium Transparency Implementation.[58]

  While NNSA followed the May 2004 schedule for fiscal years 2006 and 2007, it had not updated this schedule as of November 2006 to reflect program changes. For example, new major program initiatives—such as the Reliable Replacement Warhead and the efforts to transform the nuclear weapons complex, called Responsive Infrastructure—are not listed on the May 2004 validation schedule for fiscal years 2005 through 2009. While the amounts requested in the fiscal year 2007 budget for these two initiatives are low compared with other program efforts, both initiatives are considered centerpieces in the NNSA budget, will require significant additional funding in succeeding fiscal years, and meet NNSA's selection criteria for program validation on the basis of

[58]The Nonproliferation and Verification Research and Development Program's mission is to conduct needs-driven research, development, testing, and evaluation of new technologies that are intended to strengthen the United States' ability to prevent and respond to nuclear, chemical, and biological attacks. The Highly-Enriched Uranium Transparency Implementation Program's mission is to ensure that the nonproliferation goals of the February 1993 agreement on the U.S. purchase of uranium from the Russian Federation are met.

significant external interest and high program visibility. Because the May 2004 schedule has not been updated, NNSA does not know when certain programs like the Reliable Replacement Warhead and Responsive Infrastructure would be validated, according to an official in NNSA's Office of Planning, Programming, Budgeting, and Evaluation. This official added that NNSA is contemplating updating the program validation schedule later in 2006.

NNSA indicated that it would not be beneficial to add the Reliable Replacement Warhead and Responsive Infrastructure programs to its budget validation schedule until DOE and the Office of Management and Budget have made decisions to proceed with these activities. However, both of these programs are ongoing and are expected to grow; therefore, in our view, they should be considered when NNSA updates its budget validation schedule.

- *Establish a DOE-compliant budget validation process*. NNSA's May 2004 draft budget validation policy also outlined the Administration's approach to budget validation. Specifically, the Administration will follow a two-phased validation approach. During phase one, NNSA will assess selected programs' conformance with strategic guidance, program plans, and performance data and seek insight into how each organization formulates its budget. During phase two, NNSA will choose a few of the programs from the phase one review and conduct a detailed review that examines the reasonableness of the cost estimates supporting the program's budget. Following this two-phased approach, NNSA performed a detailed validation review on only approximately 12 percent of the Administration's budget submitted for fiscal years 2006 and 2007. However, in our view, this approach does not adhere to DOE's guidance on that subject. According to the director of DOE's Budget Operations Division, commencing in fiscal year 2001 as a performance measure, DOE has required that at least 20 percent of the budget undergo a detailed review, so that 100 percent of the budget would be evaluated every 5 years. In our 2003 report on NNSA's Stockpile Life Extension Program, we also found that NNSA was not conducting proper budget validation reviews and, consequently, recommended that NNSA validate its stockpile life extension budget request in accordance with DOE directives.[59] NNSA indicated that its budget validation review focuses on the process used in developing budget requests and is not an

[59]GAO-03-583.

audit of the resulting budget estimates. NNSA further indicated that it does not have the capabilities to audit and instead relies on DOE's Office of Inspector General and GAO for those reviews. While such reviews are helpful in evaluating budget estimates, we believe these reviews do not abrogate NNSA's responsibility to adhere to DOE requirements.[60]

NNSA also noted that the results of its progress in implementing PPBE are reflected in (1) the average scores received through the Office of Management and Budget's Program Assessment Rating Tool scores which are among the highest in DOE and the U.S. Government, (2) NNSA management and operating contractors working without serious interruption through multiple continuing resolutions in the past four years, and (3) NNSA transitioning smoothly to the DOE budget formulation process in the summer of 2006.

Conclusions

Prior to the creation of NNSA, DOE's management of the nuclear weapons complex was widely considered, in the words of the President's Foreign Intelligence Advisory Board as "science at its best" and "security at its worst." Underpinning this characterization was a long departmental history of organizational disarray and poor security, project and program management. Consequently, producing a well-organized and effective agency out of what was widely considered a dysfunctional enterprise has been a considerable challenge. In some areas, NNSA should be viewed as a success. Most notably, through its internal reorganization efforts, NNSA has addressed many major organizational issues and has made important progress in establishing critical management systems, especially PPBE.

However, without a workable model on how a separately organized agency should function, NNSA and DOE officials have had to develop their working relationships largely on a case-by-case basis, often with limited success. The fact that the Congress felt it necessary to step in and modify the NNSA Act to address continuing organizational conflict within the counterintelligence program demonstrates, in our view, that DOE and NNSA need to take a more active approach to clearly defining DOE and NNSA's working relationships and determining how conflict will be resolved. While there have been continuing calls for removing NNSA from DOE and establishing it as a separate agency, we do not believe that such

[60]According to NNSA Policy Letter NAP-1 dated May 21, 2002, DOE orders are applicable to NNSA unless or until a NNSA policy letter is provided.

drastic change is necessary to produce an organization that can provide effective oversight of the nation's nuclear weapons complex.

Beyond addressing organizational issues, if NNSA is ultimately to provide comprehensive oversight of the operation and security of the nation's nuclear weapons programs, it must address a variety of lingering, often unrelated, but important management issues. These issues include providing sufficient, qualified staff to conduct program and operational oversight, especially in the security area, and developing and implementing improvements needed to support effective project, program, and financial management.

Recommendations for Executive Action

To improve NNSA's efficiency and effectiveness, we are making 21 recommendations in five areas—organization, security, project management, program management, and financial management.

To ensure that NNSA functions as a separately organized agency, we recommend that the Secretary of Energy and the Administrator, NNSA, take the following two actions:

- clearly define NNSA's status as a separately organized agency within the department; and
- develop and implement standard operating procedures for conducting business and resolving conflicts between DOE and NNSA sister offices.

To improve security oversight, we recommend that the Administrator, NNSA, take the following four actions:

- develop a human capital strategy that includes standards for determining long-term staffing needs;
- implement a professional development program for security staff to ensure the completion of training needed to effectively perform oversight responsibilities;
- develop a framework to evaluate results from security reviews and guide security improvements; and
- establish formal mechanisms for sharing and implementing lessons learned across the weapons complex.

To fully implement NNSA's management reforms, we recommend that the Administrator, NNSA, institute a series of initiatives to improve project management, program management, and financial management.

With respect to project management, we recommend that NNSA take the following seven actions:

- establish an NNSA-specific project management policy to ensure application of the DOE project management manual;
- prepare a project management improvement plan;
- reinstitute annual reporting to the Congress on project management accomplishments;
- include major projects, such as the Stockpile Life Extension refurbishments, in DOE's Project Assessment and Reporting System;
- complete a comprehensive database of all projects' reports on management lessons learned to improve project management throughout NNSA;
- develop benchmark data on individual contractors' project management performance to assist managers in improving contractor performance; and
- require that contractors' project managers receive project manager training and attain project manager certification.

With respect to program management, we recommend that NNSA take the following three actions:

- prepare periodic reports that show the status of its program management improvement efforts to determine how much progress is being made;
- complete a best practices guide for program management; and
- identify, train, and certify all program managers in accordance with NNSA's program management policy.

With respect to financial management, we recommend that NNSA take the following five actions:

- complete all NNSA PPBE policy guidance;
- establish an independent budget analysis unit;
- develop criteria for compiling a NNSA-wide priorities list to assist NNSA in supporting its budget request;
- update the schedule of those NNSA programs requiring budget validation to insure that recent program initiatives like the Reliable Replacement Warhead are included; and
- establish a DOE-compliant budget validation process.

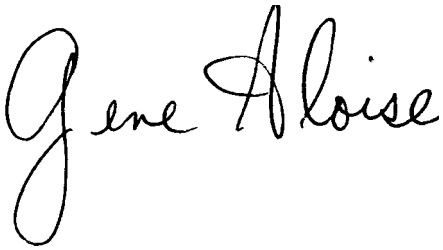
Agency Comments and Our Evaluation

We provided NNSA with a copy of this report for their review and comment. NNSA generally agreed with the report and its corresponding recommendations. NNSA noted that it considers the agency to be a success but acknowledged that there was considerable work yet to be accomplished. NNSA and DOE also provided technical comments, which we have incorporated in this report as appropriate. NNSA's comments on our draft report are presented in appendix I.

As arranged with your office, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after the date of this report. We are sending copies of this report to appropriate congressional committees, the Secretary of Energy; the Administrator, NNSA; and the Director of the Office of Management and Budget. We will also make copies available to others upon request. In addition, the report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions about this report or need additional information, please contact me at (202) 512-3481 or aloiseg@gao.gov. Contact points for our Offices of Congressional Relations and Public

Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix II.



Gene Aloise
Director, Natural Resources
and Environment

Comments from the National Nuclear Security Administration

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

December 21, 2006

Mr. Gene Aloise
Director, Natural Resources
And Environment
U.S. Government Accountability Office
Washington, DC 20548

Dear Mr. Aloise:

The National Nuclear Security Administration (NNSA) appreciates the opportunity to review the Government Accountability Office's (GAO) draft report: GAO-07-36, "NATIONAL NUCLEAR SECURITY ADMINISTRATION: Additional Actions Needed to Improve Management of the Nation's Nuclear Programs." We understand that the House's Chairman and Ranking Minority Member, Strategic Forces Subcommittee, Committee on Armed Services asked GAO to review the steps NNSA has taken to improve security at its laboratories and plants and to improve its management practices and revise its organizational structure.

NNSA generally agrees with the report and its corresponding recommendations. We note that we consider NNSA a success but we acknowledge that there is considerable work yet to be accomplished. NNSA will provide detailed responses to the recommendations during the Management Decision phase after the Final Report has been issued. In the interim, I have attached a copy of the draft report with annotated comments for edification and clarification. Should you have any questions about this response, please contact Richard Speidel, Director, Policy and Internal Controls Management.

Sincerely,

Michael C. Kane
Associate Administrator
for Management and Administration

Attachment

cc: Chief Operating Officer
Director, Service Center
Senior Procurement Executive

Printed with soy ink on recycled paper

GAO Contact and Staff Acknowledgments

GAO Contact

Gene Aloise (202) 512-3841

Staff Acknowledgments

In addition to the individual named above, James Noel, Assistant Director; Robert Baney; Preston Heard; Jonathan Ban; Rebecca Shea; Cynthia Daffron; Greg Marchand; and Carol Herrnstadt Shulman made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548