United States General Accounting Office

GAO

Testimony

Before the Subcommittee on National Security, Emerging Threats, and International Relations, House Committee on Government Reform

For Release on Delivery
Expected at 9:00 a.m. EI
June 24,2003

NUCLEAR SECURITY

DOE Faces Security Challenges in the Post September 11,2001, Environment

Statement of Robin M. Nazzaro, Director
Natural Resources and Environment Team

GAO
Accountability • Integrity * Reliability

GAO-03-896TNI

June 24, 2003

GAO
Accountability·Integrity·Reliability

Highlights

Highlights c O- : TNI, a report to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives

Why GAO Did This Study

The attacks of September 11, 2001, intensified long-standing concerns about the adequacy of safeguards and security at DOE and NNSA that facilities store plutonium and uranium in a variety of forms. These contractor-operated facilities can become targets for such actions as sabotage or theft. The Department of Energy (DOE) and the National Nuclear Security Administration (NNSA)—a separately organized agency within DOE—are responsible for these facilities. GAO reviewed how effectively NNSA manages its safeguards and security program, including how it oversees contractor security operations. GAO also reviewed DOE and NNSA's response to the terrorist attacks of September 11, 2001. In this regard, GAO examined (1) DOE and NNSA's immediate response to September 11, (2) DOE's efforts to develop a new design basis threat, a classified document that identifies the potential size and capabilities of the terrorist forces that DOE and NNSA sites must be prepared to defend against, and (3) the challenges DOE and NNSA face in meeting the requirements of the new design basis threat.

www.gac ov cg bin/getrp C 0: 8 TNI.

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

NUCLEAR SECURITY

DOE Faces Security Challenges in the Post September 11,2001, Environment

Wha GAO Found

NNSA has not been fully effective in managing its safeguards and security program. For example, NNSA has not fully defined clear roles and responsibilities for its headquarters and site operations. Without a functional management structure and with ongoing confusion about roles and responsibilities, inconsistencies have emerged among NNSA sites on how they assess contractors' security activities. Consequently, NNSA cann be assured that all facilities are subject to the comprehensive annual assessments that DOE policy requires. To compound the problems in conducting security assessments, NNSA contractors do not consistently conduct required analyses in preparing corrective action plans. As a result, potential opportunities to improve physical security at the sites are not maximized because corrective actions are developed without fully considering the problems' root causes, risks posed, or cost versus the benefi of taking corrective action. Finally, NNSA has shortfalls at its site offices in the total number of staff and in expertise, which could make it more difficul for site offices to effectively oversee security activities. GAO made recommendations to improve the management of NNSA's safeguards and security program. NNSA has begun to respond to these recommendations.

With respect to DOE and NNSA's response to September 11, the agencies took immediate steps to improve security in the aftermath of the terrorist attacks. For example, DOE and NNSA moved to a higher level of security, which required, among other things, more vehicle inspections and security patrols. While these steps are believed to have improved DOE and NNSA's security posture, they have been expensive and, until fully evaluated, their effectiveness is uncertain.

The number and capabilities of the terrorists involved in the September 11 attacks rendered obsolete DOE's design basis threat, last issued in 1999. However, DOE's effort to develop and issue a new design basis threat took almost 2 years; it was issued in May 2003. This effort was slowed by, among other things, disagreements over the size of the potential terrorist group that might attack a DOE or NNSA facility.

Successfully addressing the increased threats will take time and resources, as well as new ways of doing business, sound management, and leadership. Currently, DOE does not have a reliable estimate of the cost to fully protect DOE and NNSA facilities. The fiscal year 2006 budget will probably be the first to show the full budgetary impact of the new design basis threat. Once funds become available, most sites estimate that it will take from 2 to 5 years to fully implement, test, validate, and refine strategies for meeting the requirements of the new design basis threat.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss our work for this Subcommittee on physical security at the Department of Energy (DOE) and the National Nuclear Security Administration (NNSA)—a separately organized agency within DOE.[1] DOE and NNSA recognize that a successful terrorist attack on a facility that contains nuclear weapons or nuclear weapons materials could have devastating consequences for the facility and its surrounding communities.

DOE and NNSA rely on their safeguards and security programs to ensure the physical security of NNSA's nuclear weapons complex. Currently, the complex has four production sites—in Missouri, South Carolina, Tennessee and Texas—and three national laboratories that design nuclear weapons in California and New Mexico. DOE's Office of Environmental Management is responsible for cleaning up former nuclear weapons sites that contain some nuclear weapons materials, including sites in Colorado and Washington State. To implement their safeguards and security programs, NNSA and the Office of Environmental Management rely on contractors that are responsible for conducting day-to-day security activities and adhering to DOE policies. The contractors' activities are subject to DOE/NNSA oversight. NNSA and the Office of Environmental Management have offices—site offices—co-located with each site.

Over the past decade, we and others have raised concerns about the adequacy of security at nuclear weapons facilities within the department and NNSA. For example, we reported to you last month that NNSA needs to better manage its safeguards and security program.[2] Concern over security within the nuclear weapons complex was brought into sharper focus by the September 11, 2001, terrorist attacks. These attacks highlighted the importance of effective physical security in response to a challenging and well-organized terrorist threat.

Following the September 11 terrorist attacks, you asked us to review physical security at DOE and NNSA's most sensitive facilities—those

[1] Physical security is the combination of operational and security equipment, personnel, and procedures used to protect facilities, information, documents, or material against theft, sabotage, diversion, or other criminal acts.

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

facilities that contain specified quantities of plutonium and highly enriched uranium, which require the Category I level of protection—the highest protection requirement? As agreed with your office, we examined two issues. First, we reviewed how NNSA manages its safeguards and security program. Second, we examined DOE's response to the terrorist attacks of September 11,2001. In this regard, we examined (1) DOE's and NNSA's immediate response to the attacks; (2) DOE's efforts to develop the design basis threat (DBT), a classified document that identifies the potential size and capabilities of the terrorist forces that DOE and NNSA sites must be prepared to defend against; and (3) the challenges DOE and NNSA face in meeting the requirements of the new DBT.

To carry out our objectives, we reviewed DOE policy and planning documents, including orders, implementation guidance, and reports. We met with officials from DOE and NNSA headquarters and NNSA site offices. We obtained information primarily from DOE's Office of Security, Office of Independent Oversight and Performance Assurance, and Office of Environmental Management; and NNSA's Office of Defense Nuclear Security and NNSA's Nuclear Safeguards and Security Program.[4] We visited NNSA's four production plants and the three design laboratories as well as NNSA's Office of Transportation Safeguards. We also visited four Office of Environmental Management sites that contain Category I special nuclear materials. At each location we met with both federal and contractor officials, observed their physical security operations and obtained and reviewed pertinent supporting documentation, including corrective action plans.

We performed our review from December 2001 through May 2003 in accordance with generally accepted government auditing standards.

[3]Category I special nuclear material that requires Category I level of protection includes plutonium and highly enriched uranium in the form of (1) assembled nuclear weapons and test devices; (2) specified quantities of products containing higher concentrations of plutonium or uranium, such as major nuclear components, and recastable metal, and (3) specified quantities of high-grade materials, such as carbides, oxides, solutions, and nitrates.

[4]We did not include naval reactors in our review because that office is a semiautonomous entity within NNSA with a unique security structure and program.

In summary, we found NNSA has not been fully effective in managing safeguards and security program in four key areas. As a result, NNSA cannot be assured that its contractors are working to maximum adva to protect critical facilities and materials from adversaries seeking to inflict damage. Specifically, we found the following:

- NNSA has not fully defined clear roles and responsibilities for its headquarters and site operations.

- Without a stable and effective management structure and with ongoi confusion about roles and responsibilities, inconsistencies have emer among NNSA site offices on how they assess contractors' security activities. Consequently, NNSA cannot be assured that all facilities ar subject to the comprehensive annual assessments that DOE policy requires.

- To compound the problems in conducting security assessments, NNS contractors do not consistently conduct required analyses in preparir corrective action plans. As a result, potential opportunities to improv physical security at the sites are not maximized because corrective a are developed without fully considering the problems' root causes, ri posed, or the cost versus benefit of taking corrective action.

- NNSA has shortfalls at its site offices in the total number of staff and expertise, which could make it more difficult for site offices to effect oversee security activities.

We made four recommendations designed to improve NNSA's securit management and oversight. NNSA concurred with two of our four recommendations and has made progress in addressing the issues WE identified, including publishing a *Safeguards and Security Functions Responsibilities, and Authorities Manual* and developing and issuin guidance for corrective action plans. Beyond these changes, sustaine attention and commitment to sound safeguards and security manage1 will be needed as DOE and NNSA adjust to the post-September 11 se environment.

With respect to DOE's and NNSA's response to the September 11 terr attacks, we found that the department has taken a number of importa steps to respond to the terrorist threat; however, DOE's response has slow in some vital respects, and DOE and NNSA will need at least sev years and an as yet undetermined amount of resources before their si

are fully prepared to meet the projected threat. Specifically, we found the following:

- DOE and NNSA took immediate steps to improve security in the aftermath of the September 11 terrorist attacks. For example, DOE and NNSA moved to a higher level of security that required, among other things, more vehicle inspections and security patrols. While these steps are believed to have improved DOE and NNSA's security posture, they have been expensive and, until fully evaluated, their effectiveness is uncertain.

- The number and capabilities of the terrorists involved in September 11 attacks rendered obsolete DOE's DBT, last issued in 1999. However, DOE's effort to develop and issue a new DBT took almost 2 years; it issued the new DBT in May 2003. The effort to develop a new DBT was slowed by, among other things, disagreements over the size of the potential terrorist group that might attack a DOE or NNSA facility.

- Successfully addressing the increased threats contained in the new DBT will take time and resources, as well as new ways of doing business, sound management, and leadership. Currently, DOE does not have a reliable estimate of the cost to fully protect DOE and NNSA facilities against the new DBT. DOE and NNSA are developing preliminary cost estimates that could be included in the fiscal year 2005 budget, which is now being formulated. However, the fiscal year 2006 budget will probably be the first to show the full budgetary impact of the new DBT. Once funds become available, most sites estimate that it will take from 2 to 5 years to fully implement, test, validate, and refine strategies for meeting the new DBT requirements. Finally, DOE and NNSA will have to change how they perform physical security through such actions as employing new technologies, consolidating special nuclear materials, and closing unneeded facilities.

Background

From the beginning of the Manhattan Project in the 1940s, a primary mission of DOE and its predecessor organizations has been to design, test, and build the nation's nuclear weapons. To accomplish this mission, DOE constructed a vast nuclear weapons complex throughout the United States. Much of this complex was devoted to the production and fabrication of weapons components made from two special nuclear materials—plutonium and highly enriched uranium.

The end of the Cold War changed the department's focus from building new weapons to extending the lives of existing weapons, disposing of surplus nuclear material, and cleaning up no longer needed weapons sites.

NNSA is responsible for extending the lives of existing weapons in the stockpile and for ultimately disposing of surplus nuclear material, while the Office of Environmental Management is responsible for cleaning up former nuclear weapons sites. Contractors, who are responsible for protecting classified information, nuclear materials, nuclear weapons, and nuclear weapons components, operate both NNSA and Office of Environmental Management sites."[5]

Besides NNSA and the Office of Environmental Management, DOE has two other important security organizations. DOE's Office of Security develops and promulgates orders and policies, such as the DBT, to guide DOE and NNSA's safeguards and security programs. DOE's Office of Independent Oversight and Performance Assurance supports DOE and NNSA by, among other things, independently evaluating the effectiveness of contractors' performance in safeguards and security. It also performs follow-up reviews to ensure that contractors have taken effective corrective actions and appropriately addressed weaknesses in safeguards and security.

A key component of DOE's protective strategy is the DBT, a classified document that identifies the characteristics of the potential threats to DOE assets. The DBT considers a variety of threats in addition to terrorists: criminals, psychotics, disgruntled employees, violent activists, insiders, and spies. The terrorist threat is generally the most demanding threat contained in the DBT. The DBT has traditionally been informed and shaped by classified multiagency intelligence assessments of potential terrorists threats. The basis for DOE's 2003 DBT is an intelligence community assessment entitled the ***Postulated Threat*** to *U.S.* ***Nuclear Weapons Facilities and other Selected Strategic Facilities*** (henceforth referred to as the Postulated Threat).

DOE counters the terrorist threat specified in the DBT with a multifacete protective system. While specific measures vary from site to site, all protective systems at DOE's and NNSA's most sensitive sites employ a defense-indepth concept that includes

[5]Responsibility for the Idaho National Environmental Engineering Laboratory has been transferred to DOE's Nuclear Energy Program.

[6]An exception is the Office of Transportation Safeguards, whose protective forces are Special Federal Agents.

- a variety of integrated alarms and sensors capable of detecting intruders;
- physical barriers, such as fences and anti-vehicle obstacles;
- numerous access control points, such as turnstiles, badge readers, vehicle inspection stations, special nuclear material detectors, and metal detectors;
- operational security procedures, such as a "two person" rule that prevents only one person from having access to special nuclear material,
- hardened facilities and/or vaults; and
- a heavily armed paramilitary protective force equipped with such items as automatic weapons, night vision equipment, body armor, and chemical protective gear.

Depending on the material, protective systems at DOE and NNSA Category I sites are designed to accomplish the following objectives in response to the terrorist threat.

- **Denial of access.** For some potential terrorist scenarios, DOE employs a protection strategy that requires the engagement and neutralization of an adversary before the adversary can acquire hands-on access to the assets.
- **Denial of task.** For assets that might present terrorists with opportunities to steal a nuclear weapon or nuclear test device, DOE requires the prevention and/or neutralization of the adversary before the adversary can complete a specific task.
- **Containment with recapture.** In scenarios where the theft of nuclear material (instead of a nuclear weapon) is the likely terrorist objective, DOE requires that adversaries not be allowed to escape the facility and that DOE protective forces recapture the material as soon as possible. This objective requires the use of specially trained and well-equipped special response teams.

The effectiveness of the protective system is formally and regularly examined through a vulnerability assessment. A vulnerability assessment is a systematic evaluation process in which qualitative and quantitative techniques are applied to detect vulnerabilities and arrive at effective protection of specific targets, such as special nuclear material. To conduct this assessment, DOE uses, among other things, subject matter experts, such as U.S. Special Forces; computer modeling to simulate attacks; and

force-on-force performance testing, in which the site's protective forces undergo simulated attacks by an adversary team.

The results of these assessments are documented at each site in a classified document known as the Site Safeguards and Security Plan. In addition to identifying known vulnerabilities and risks and protection strategies for the site, the Site Safeguards and Security Plan formally acknowledges how much risk the contractor and DOE are willing to accept. Specifically, for more than a decade, DOE has employed a risk management approach that seeks to direct resources to its most critical assets—in this case specified quantities of Category I special nuclear material—and mitigate the risks to these assets to an acceptable level. DOE strives to keep its most critical assets at a low risk level and may insist on immediate compensatory measures should a significant vulnerability develop. Compensatory measures could include such things as deploying additional protective forces.

Through a variety of complementary measures, DOE ensures that its safeguards and security policies are being complied with and are performing as intended. Contractors perform regular self-assessments and are encouraged to uncover any problems themselves. In addition to routine oversight, DOE and NNSA site offices are required by DOE Order to conduct comprehensive annual surveys of contractors' operations for safeguards and security. These surveys, which can draw upon subject matter experts throughout the complex, generally take about 2 weeks to conduct and cover such areas as program management, protection program operations, information security, nuclear materials control and accountability, and personnel security. The survey team assigns ratings of satisfactory, marginal, or unsatisfactory. Currently, most of the DOE and NNSA facilities that we examined have been rated satisfactory in most areas. All deficiencies (findings) identified during a survey require the contractors to take corrective action. DOE's Office of Independent Oversight and Performance Assurance provides yet another check through its comprehensive inspection program. This office performs such inspections roughly every 18 months at each DOE and NNSA site that has Category I special nuclear material.

NNSA Needs to Better Manage Its Safeguards and Security Program

As we reported to you on May 30,2003, NNSA has not been fully effective in managing its safeguards and security program in four key areas, and therefore it cannot be assured that its contractors are working to maximum advantage to protect critical facilities and materials from individuals seeking to inflict damage. The four key areas are the following:

- **Defining clear roles and responsibilities.** Since its creation in March 2000, NNSA's management structure has been in a state of flux. In December 2002, NNSA issued what it considers final directives for reorganizing headquarters and site offices; however, NNSA expects it will take until at least September 2004 to fully implement its new management structure. This still-developing management structure has led to confusion about the safeguards and security roles and responsibilities of headquarters and site offices. For example, at the time of our review, NNSA headquarters could not provide details on how it intends to (1) monitor the NNSA site offices' performance with respect to safeguards and security or (2) address deficiencies. At the end of May 2003, however, NNSA released a ***Safeguards and Security Functions, Responsibilities and Authorities Manual.*** This manual, which NNSA itself recognizes as crucial, is intended to set out roles and responsibilities clearly.

- **Assessing sites' security activities.** Without a functional management structure and with ongoing confusion about roles and responsibilities, inconsistencies have emerged among the NNSA sites on how to conduct key aspects of safeguards and security assessment activities. In particular, three out of the seven NNSA site offices use the traditional survey approach, as required by DOE policy, to oversee security activities, while four have discontinued surveys and instead rely on surveillance activities. The distinction between these two activities is important: A survey provides a comprehensive annual review, by a team of experts from throughout NNSA, of contractor safeguards and security and generally takes about 2 weeks. In contrast, surveillance relies on a single or small number of NNSA site officials to oversee one or more aspects of a contractor's safeguards and security activities throughout *the* year. However, officials from DOE's Office of Security—which developed the policy for conducting surveys—believe the surveillance model does not comply with the DOE order because it does not provide a comprehensive overview. Furthermore, officials from DOE's Office of Independent Oversight and Performance Assurance and NNSA headquarters have expressed concern about the site offices' ability to conduct surveillance because of shortfalls in available expertise. The four site offices have been able to operate using only surveillance activities because, during the reorganization of the management structure, NNSA has not issued guidance on complying with DOE policy for conducting surveys.

- **Overseeing contractors' corrective actions.** NNSA contractors do not consistently conduct the analyses DOE policy requires in preparing corrective action plans, which compounds the problems of ensuring physical security. Inconsistency occurs because the NNSA site officials do not have implementation guidance from headquarters on how to address corrective actions. Of the 43 corrective action plans we reviewed for 1999 through 2002, less than half showed that the contractor had performed the required root cause analysis. Furthermore, less than 25 percent demonstrated that the contractor had performed a required risk assessment or cost-benefit analysis. As a result, potential opportunities to improve physical security at the sites were not maximized because corrective actions were developed without fully considering the problems' root causes, risks posed, or cost versus benefit of taking corrective action. However, at the seven sites we visited in 2002, the site offices and contractors are making some progress in establishing formal processes for root cause and other analyses. Nevertheless, inconsistencies remain regarding the approaches used to complete these analyses. For example, some site processes specify that root cause analyses will be conducted for all corrective action plans, while other sites consider the completion of these analyses optional. NNSA did, however, recently issue guidance to its sites regarding compliance with DOE Orders on corrective actions.

- **Allocating staff.** NNSA has shortfalls at its site offices in the total number of staff and in areas of expertise, which could make it more difficult for the site offices to oversee safeguards and security effectively and to ensure that the agency fully knows security conditions at its sites. According to officials at five of the seven site offices we visited, they have, or expect to have, an average of 2 to 6 vacancies per site for overseeing contractors' safeguards and security; typically, each site expects to have 10 to 14 security-related positions within the next 2 years. The vacancies occur, in part, because staff are reluctant to move to locations they view as less desirable and because NNSA has frozen hiring in response to budget constraints. Some of these vacancies are for specialists in particular subject areas, such as Industrial Security Systems—a key specialty needed for conducting physical security inspections. The lack of expertise and staff could be further complicated for some sites by NNSA's realignment plan. Under this plan, NNSA expects to streamline federal oversight of contractors and reduce headquarters and field staff by 20 percent by the end of fiscal year 2004. Site officials said that they will fill some vacancies through a virtual organization in which experts at other locations will assist with certain components of the surveillance activities. However, it will take time to work through some of the difficulties associated with making the transition to this approach.

DOE and NNSA's Response to the Terrorist Attacks of September 11, 2001

I would like now to discuss DOE and NNSA's response to the terrorist attacks of September 11,2001. I will cover DOE's and NNSA's immediate response to the attacks; DOE's efforts to develop a new DBT that DOE and NNSA sites must be prepared to defend against; and the challenges DOE and NNSA face in meeting the requirements of the new DBT.

DOE and NNSA Improved Security after September 11, 2001, but Have Not Fully Tested These Improvements

DOE and NNSA took immediate steps *to* improve physical security in the aftermath of the September 11,2001, terrorist attacks. These steps included the following:

- **Raised the Level of Security Readiness.** DOE's most visible effort involved moving to higher levels of security readiness, as outlined by DOE Notice 473.6. This notice specifies DOE Security Condition, or SECON, levels and the corresponding security measures that have to be implemented.[7] On September 11,2001, within a matter of hours, DOE and NNSA sites went from their then-normal SECON level 4—terrorist threat level low—to SECON level 2—terrorist threat level high. Sites were required to implement nearly 30 additional measures, such as increasing vehicle inspections and badge checks; increasing stand-off distances between public and sensitive areas; activating and manning emergency operations centers on a continuous basis; and more heavily arming and increasing the number of protective forces on duty. Sites maintained SECON level 2 through October 2001 before dropping to an enhanced SECON level 3. The sites have returned to SECON level 2 several times since September 11 2001, most recently in May 2003, when the national threat warning systems was elevated to Orange Alert. The new baseline for security at DOE and NNSA facilities is generally assumed to be at an enhanced SECON level 3. This level is still substantially greater than DOE's pre-September 11,2001 security posture.

- **Enhanced Protective Force Responses.** On October 3,2001, the Secretary of Energy issued a classified directive that ordered more robust protective force responses and increased levels of performance testing for the protection of certain special nuclear material at DOE's and NNSA's most critical facilities.

[7] SECON levels are pegged to the national threat level issued by the Department of Homeland Security. For example, a national level of ORANGE equates to SECON level 2 for DOE facilities.

- **Conducted Security Reviews, Studies and Analyses.** DOE and NNSA also conducted a number of security-related reviews, studies, and analyses. For example, within days after the terrorist attacks, DOE and NNSA officials conducted a classified assessment of their facilities' vulnerabilities to an attack such as the one on September 11. This assessment came to be known as the *72 Hour Review*. In addition, NNSA organized a 90-day Combating Terrorism Task Force, composed of 12 federal and contractor employee teams that looked at a number of security areas. One team, the site-by-site security review and vulnerability assessment group, identified over 80 prioritized security improvement projects, totaling more than $2 billion, that could be completed within 5 to 6 years. These projects ranged from hiring additional protective forces to consolidating special nuclear material.

- **Increased Liaison with Federal, State, and Local Authorities:** Before the September 11 terrorist attacks, DOE and NNSA headquarters offices and sites maintained a variety of relationships, memoranda of understanding, and other formal and informal communications with organizations such as the Federal Aviation Administration, Federal Bureau of Investigation, and state and local law enforcement and emergency management agencies. After the terrorist attacks, DOE and NNSA officials increased their communication with these organizations and established direct links through sites' emergency operations centers. Because of the potential threat of aircraft attacks created by the September 11 attacks, sites worked closely with the Federal Aviation Administration and the U.S. *military*.

While these steps are believed to have generally improved security, they have been expensive and, until fully tested using DOE's vulnerability analysis approach, their effectiveness is uncertain. With respect to improved security, implementation of SECON levels 2 and 3 has, for example, increased the visible deterrence at DOE and NNSA sites by placing more guards around the sites. Studies and analyses, such as the *72 Hour Review*, have also resulted in different and less vulnerable storage strategies for some special nuclear material. DOE and NNSA have hired additional protective forces and are training them. Finally, some long-recognized security enhancement projects have received more funding, such as the construction of a new highly enriched uranium materials facility at the Y-12 Plant, and the removal of some of the Los Alamos National Laboratory's most sensitive materials and equipment to a more modern facility at the Nevada Test Site have been accelerated.

At the same time, it has been expensive to implement the increased SECON measures. DOE and NNSA sites estimate that it costs each site

from $18,000 to nearly $200,000per week in unplanned expenditures to implement the required SECON level 2 and 3 measures. Most of these expenses result from overtime pay to protective forces.

However, the costs of the higher SECON levels can be measured in more than just budget dollars. For example, a recent DOE Inspector's General report found that the large amounts of overtime needed to meet the higher SECON requirements have resulted in fatigue, reduced readiness, retention problems, reduced training, and fewer force-on-force performance tests for the protective forces.' In addition, the increased operational costs associated with the higher SECON levels can hinder or preclude sites from making investments that could improve their security over the long term. For example, one site delayed purchasing equipment for its protective force that would address a known vulnerability because of the high costs of SECON implementation. F'inally, implementation of the protective force response plans outlined in the Secretary's October 3,2001, directive was sharply limited by the lack of available funding, with some sites estimating it would take from about $30 million to over $200 million to implement the directive completely. Moreover, the performance testing requirements of this directive were generally not conducted because of the already large amounts of protective force overtime required by the higher SECON levels. The new DBT, however, has replaced this directive.

Other than deterrence, the role of the higher SECON levels in improving DOE and NNSA physical security is uncertain. Some aspects of the SECON measures, such as vehicle inspection checkpoints have undergone some limited testing of their effectiveness. However, the higher SECON level measures in place at most sites have not been assessed using the vulnerability assessment tools, such as computer modeling and full-scale force-on-force exercises, that play such a key role in developing protective strategies for DOE and NNSA sites.

Finally, while liaison with other agencies is important, DOE and NNSA site officials anticipate that terrorist attacks on their facilities will be short and violent affairs and will be over before any external responders can arrive on site. In addition, because some DOE and NNSA sites are close to airports and/or major flight routes, they may receive little warning of

[8] *Audit Report: Management of the Department's Protective Forces,* DOE/IG-0602, **Department of Energy Office of the Inspector General, June 2003.**

aircraft attacks and U.S. military aircraft may have little opportunity to intercept these attacks.

Development of a New DBT Was Difficult, but Resulted in a Higher Threat Level

In the immediate aftermath of September 11, 2001, DOE and NNSA officials realized that the then current DBT, issued in 1999 and based on a 1998 intelligence community assessment, was largely obsolete. The terrorist attacks suggested larger groups of adversaries, larger vehicle bombs, and broader terrorist aspirations to cause mass casualties and panic than were envisioned in the 1999 DOE DBT. However, formally recognizing these new threats by updating the DBT has proven difficult.

The traditional basis for the DBT has been a study, known as the Postulated Threat, conducted by the U.S. intelligence community and agency security organizations, principally the Department of Defense's (DOD) Defense Intelligence Agency. However, the new Postulated Threat was completed about 9 months behind its original schedule and not finally released until January 2003. According to DOE and DOD officials, this delay was the result of other post-September 11, 2001, demands placed on the intelligence community as well as sharp debates among the organizations involved with developing the Postulated Threat over the size and capabilities of future terrorist threats and the resources needed to meet these projected threats.

Given the delay associated with the development of the Postulated Threat, DOE, on its own, developed a number of draft threat statements that culminated in the final May 20, 2003, DBT. These included the following:

- **December 2001—Interim Joint Threat Policy Statement.** DOE and DOD worked on this joint draft document but abandoned this effort later in 2002.
- **January 2002—Interim Implementing Guidance.** DOE's Security Office issued this guidance so that DOE and NNSA programs could begin to plan for eventual increases in the DBT.
- **May 2002—Draft DBT.** DOE produced its official draft DBT. This was labeled an interim product pending the release of the Postulated Threat.
- **August 2002—2nd Draft DBT.**
- **December 2002—3rd Draft DBT.**

- **April 2003—4th Draft DBT.**
- **May 2003—Final DBT.**

DOE's Security Office distributed the drafts to DOE and NNSA program and site offices and invited them to provide comments. DOE's Security Office considered these comments and often incorporated them into the next version of the DBT. DOE's Security Office also continued to coordinate with the other federal organizations that have similar assets, chiefly DOD and the Nuclear Regulatory Commission.

During the development of DOE's DBT, debates, similar to those that occurred during the development of the Postulated Threat, emerged in DOE and NNSA over the size of the future threat and how much it would cost to meet the new threat. DOE and NNSA officials from all levels told us that concern over resources played a large role in developing the 2003 DBT, with some officials calling the DBT the "fundingbasis threat," or the maximum threat the department could afford. This tension between threat size and resources is not a new development. According to a DOE analysis of the development of prior DBTs, political and budgetary pressures and the apparent desire to reduce protective force manpower requirements appear to have played a significant role in determining the adversary numbers contained in prior DBTs.

Reflecting the post-September 11,2001,environment, the 2003 DBT is a substantially different and more demanding document than previous DBTs. Key differences from the 1999 DBT include the following:

- **Increased adversary threat levels.** The 2003 DBT increases the terrorist threat levels for the theft of the department's highest value assets—special nuclear material—although not in a uniform way. The 1999 DBT required DOE and NNSA sites to protect against only one terrorist threat level. Under the 2003 DBT, however, the theft of a nuclear weapon or test assembly is judged to be more attractive to terrorists, and sites that have these assets are required to defend against a substantially higher number of adversaries than are other DOE and NNSA sites that possess other forms of Category I quantities of special nuclear material. For example, the Pantex Plant, which, among other things, assembles and disassembles nuclear weapons, is required to defend to a higher level than sites such Los Alamos or Y-12, both of which fabricate nuclear weapons components. DOE calls this a graded threat approach.

- Specific protection strategies. In line with the graded threat approach and depending on the type of materials they possess and the likely mission of the terrorist group, sites are now required to implement specific protection strategies, such as denial of access, denial of task, or containment with recapture for their most sensitive facilities and assets.

- Wider range of terrorist objectives. The 2003 DBT recognizes a wider range of terrorist objectives, particularly in the area of radiological, chemical, and biological sabotage. The 2003 DBT requires the development of protection strategies for a range of facilities, such as some radioactive waste storage areas, that were not covered under the previous DBT.

- Increased Complexity. With a graded approach and broader coverage, the new DBT is a more complex document than its predecessor. For example, the 1999 DBT was 9 pages long, while the 2003 DBT is 48 pages long.

During the 21 months it took to develop the DBT policy, DOE and NNSA sites still officially followed the 1999 DBT, although their protective posture was augmented by implementing SECON level 2 and 3 measures. While DOE sites under the Office of Environmental Management continued to conduct vulnerability assessments and develop Site Safeguards and Security Plans based on the 1999 DBT, NNSA largely suspended the development of Site Safeguards and Security Plans pending the issuance of the new DBT. During this period, however, NNSA did embark on a new vulnerability assessment process, called Iterative Site Analysis, at four sites and its Office of Transportation Safeguards. The Iterative Site Analyses were analytical, tabletop exercises that addressed a spectrum of potential threats, both within and beyond the threat contained in the 1999 DBT. Iterative Site Analyses were conducted by independent and highly skilled security professionals from across the government and private sector. Most NNSA sites agreed that the Iterative Site Analysis exercises were valuable, and some sites believe that it gave them a head start in meeting the requirements of the new DBT. The Office of Environmental Management is testing this methodology at one of its sites this summer. DOE's Office of Independent Oversight and Performance Assurance continued its inspections; however, it initially reduced the amount of force-on-force performance testing it conducted because of the high levels of protective force overtime caused by implementation of SECON level 2 and 3 measures. This Office also planned to begin performance testing at levels beyond the 1999 DBT, but had done so at only one site before the 2003 DBT was issued.

Implementation of the 2003 DBT Will Be Challenging

Successfully addressing the increased threats contained in the 2003 DBT will take time and resources, as well as new ways of doing business, sound management, and leadership. Currently, the department does not have a reliable estimate for the total cost of fully protecting DOE and NNSA facilities against the 2003 DBT. While DOE and NNSA officials expect new resource requirements to vary widely among the sites, neither the current fiscal year 2003 nor the planned fiscal year 2004 budget includes funds for implementing the 2003 DBT. DOE and NNSA are currently developing preliminary cost estimates that could be included in the fiscal year 2005 budget, which is now being formulated; however, the fiscal year 2006 budget will probably be the first to show the full budgetary impact of the new DBT. DOE and NNSA officials suggest that in order to take earlier action, they may pursue additional security funding through reprogramming and/or supplemental appropriations.

Once funds become available, most sites estimate that it will take from 2 to 5 years to fully implement, test, validate, and refine strategies for meeting the new DBT requirements. Some sites, particularly those that benefited from the Iterative Site Analysis, may be able to move more quickly, and all sites will continue to place priority on improving the protection of special nuclear material.

DOE and NNSA officials also recognize that they will have to change how they perform the physical security mission. A DOE 1999 report and a 2002 NNSA report, this time reinforced by the September 11 attacks, called for changes in the way the department approaches physical security.[9] These changes will be even more important now that the 2003 DBT has been issued. DOE and NNSA are seeking to

- develop and employ new technologies;
- accelerate the design and construction of new facilities;
- better utilize existing facilities;
- purchase adjacent public lands, close public roads and/or build bypass roads around key facilities to restrict public access; and

[9] *A Context and Strategy for Action: A Synthesis of the Special Security Review for DOE Executive Management*, December 1998; *A Security Architecture for NNSA: A Proposed Framework for Planning and Managing Security*, May 23, 2002.

- consolidate special nuclear material and close unneeded facilities.

DOE and NNSA have taken some steps in these directions, but will have to accomplish more to meet the post-September 11,2001,security challenges. For example:

- **Developing and Employing New Technologies.** Security at many DOE and NNSA sites is a manpower-intensive activity. Adding additional protective forces to facilities is a flexible, effective, but ultimately expensive way of providing additional security. DOE's Security Office has funded a technology development and assessment program and NNSA is initiating its own program in fiscal year 2004; however, the amount of funds devoted to these activities has been limited. The use of technology in areas such as communications, weaponry, intrusion detection, and better computer modeling offers the promise of more effective security at ultimately, lower costs.

- **Accelerating the Design and Construction of New and Better Protected Facilities.** It is difficult, expensive, and sometimes impossible to retrofit existing facilities to meet more demanding physical security requirements, such as those identified in the 2003 DBT. It is far better to make security an integral part of the design of a new facility. For example, DOE estimated that a new facility built to centrally store special nuclear material would have very steep up-front costs of $2.5 to $4 billion, but would pay for itself in 4 years because of savings from reducing the number protective forces and reducing costs for safeguards and security maintenance. While DOE is not currently planning for such a facility, it is now designing or constructing a number of new facilities at several sites that will be better protected than existing facilities, although their level of protection against the 2003 DBT is uncertain. One of these new facilities, the highly enriched uranium materials facility at the Y-12 plant, may be completed as early as fiscal year 2008.

- **Better Utilization of Existing Facilities.** DOE and NNSA had made some progress in this area, even before September 11,2001. For example, the old K Area Reactor at the Savannah River Site, a massively constructe building already outfitted with physical security systems, was converted t an interim plutonium storage facility and is currently accepting shipments of plutonium from Rocky Flats. In addition, planning is underway to move sensitive equipment and materials from Technical Area –18 at Los Alamos to the more modern Device Assembly Facility at the Nevada Test Site. However, this move is expected to cost $130 million and not be complete until fiscal year 2009.

- **Purchasing Adjacent Public Lands, Closing Public Roads and/or Building Bypass Roads Around Key Facilities to Restrict Public Access.** A number of sites are bisected or adjacent to public roads and areas. Public access to these roads and areas has been restricted since September 11, 2001, and more permanent measures are being implemented or studied at sites such as Pantex, Lawrence Livermore, Los Alamos, and Y-12.

- **Closing Unneeded Facilities and Consolidating Special Nuclear Material.** DOE's Office of Environmental Management has long had the goal of closing unneeded facilities and consolidating special nuclear material. The Office of Environmental Management has recently proposed accelerating the deadline from 2016 to 2006 for moving Category I special nuclear material from Hanford and Rocky Flats to its Savannah River Site. At Savannah River, materials will ultimately be disposed of or transferred to other program offices, such as NNSA and DOE's Nuclear Energy Program. The Office of Environmental Management expects that all Category I special nuclear material will be removed from Rocky Flats by the end of the summer, 2003.

In closing, it will be a challenge for DOE and NNSA to deal with the post-September 11 security threats. DOE and NNSA have been providing physical security for over 50 years; however, given the materials and assets they possess, physical security at DOE and NNSA facilities cannot afford to fail, even once.

Meeting these challenges will require DOE and NNSA to provide sustained, sound management for their safeguards and security programs. This is particularly true for NNSA because it is the enduring steward for the nation's special nuclear material and is responsible for ensuring that the nation's nuclear weapons are safe and reliable.

Equally important DOE and NNSA must exercise strong, sustained, and high-level leadership in providing for safeguards and security. Security officials often told us that the department has a history of alternating periods of inattention and attention to security. In the post September 11, 2001, environment, the stakes are too high to allow such lapses in the future.

Mr. Chairman, this concludes my testimony. I would be happy to respond to any questions you or Members of the Subcommittee may have.

GAO Contact and staff Acknowledgments

For further information on this testimony, please contact Robin M. Nazzaro at (202) 512-3841. James Noel, Jonathan Gill, Chris Pacheco, Andrea Miller, Chris Abraham, and Jill Berman also made key contributions to this testimony.