United States General Accounting Office

GAO

Testimony

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

For Release on Delivery
Expected at 10:00 a.m. EDT
Tuesday, April 27, 2004

NUCLEAR SECURITY

DOE Must Address Significant Issues to Meet the Requirements of the New Design Basis Threat

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

April 27, 2004

NUCLEAR SECURITY

DOE Must Address Significant Issues to Meet the Requirements of the New Design Basis Threat

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-701T, a testimony to the Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives

Why GAO Did This Study

A successful terrorist attack on Department of Energy (DOE) sites containing nuclear weapons or the material used in nuclear weapons could have devastating consequences for the site and its surrounding communities. Because of these risks, DOE needs an effective safeguards and security program. A key component of an effective program is the design basis threat (DBT), a classified document that identifies, among other things, the potential size and capabilities of terrorist forces. The terrorist attacks of September 11, 2001, rendered the then-current DBT obsolete, resulting in DOE issuing a new version in May 2003.

GAO (1) identified why DOE took almost 2 years to develop a new DBT, (2) analyzed the higher threat in the new DBT, and (3) identified remaining issues that need to be resolved in order for DOE to meet the threat contained in the new DBT.

What GAO Found

DOE took a series of actions in response to the terrorist attacks of September 11, 2001. While each of these has been important, in and of themselves, they are not sufficient to ensure that all of DOE's sites are adequately prepared to defend themselves against the higher terrorist threat present in the post September 11, 2001 world. Specifically, GAO found:

- DOE took almost 2 years to develop a new DBT because of (1) delays in developing an intelligence community assessment—known as the Postulated Threat—of the terrorist threat to nuclear weapon facilities, (2) DOE's lengthy comment and review process for developing policy, and (3) sharp debates within DOE and other government organizations over the size and capabilities of future terrorist threats and the availability of resources to meet these threats.

- While the May 2003 DBT identifies a larger terrorist threat than did the previous DBT, the threat identified in the new DBT, in most cases, is less than the threat identified in the intelligence community's Postulated Threat, on which the DBT has been traditionally based. The new DBT identifies new possible terrorist acts such as radiological, chemical, or biological sabotage. However, the criteria that DOE has selected for determining when facilities may need to be protected against these forms of sabotage may not be sufficient. For example, for chemical sabotage, the 2003 DBT requires sites to protect to "industry standards;" however, such standards currently do not exist.

- DOE has been slow to resolve a number of significant issues, such as issuing additional DBT implementation guidance, developing DBT implementation plans, and developing budgets to support these plans, that may affect the ability of its sites to fully meet the threat contained in the new DBT in a timely fashion. Consequently, DOE's deadline to meet the requirements of the new DBT by the end of fiscal year 2006 is probably not realistic for some sites.

www.gao.gov/cgi-bin/getrpt?GAO-04-701T.

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.

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. Specifically, today we are issuing our report, *Nuclear Security*: *DOE Needs to Resolve Significant Issues Before It Fully Meets the New Design Basis Threat* (GAO-04-623).

DOE has long recognized that a successful terrorist attack on a site containing nuclear weapons or the material used in nuclear weapons—called special nuclear material—could have devastating consequences for the site and its surrounding communities. Because terrorist attacks against sites that contain special nuclear material could have such devastating consequences, DOE's effective management of the safeguards and security program, which includes developing safeguards and security policies, is essential to preventing an unacceptable, adverse impact on national security.[1] For many years, DOE has employed risk-based security practices. To manage potential risks, DOE has developed a design basis threat (DBT), a classified document that identifies the potential size and capabilities of terrorist forces. DOE's DBT is based on an intelligence community assessment known as the Postulated Threat. DOE requires the contractors operating its sites to provide sufficient protective forces and equipment to defend against the threat contained in the DBT. The DBT in effect on September 11, 2001, had been DOE policy since June 1999. DOE replaced the 1999 DBT in May 2003 to better reflect the current and projected terrorist threats that resulted from the September 11, 2001, attacks.

Following the September 11, 2001, terrorist attacks, you asked us to review physical security at DOE sites that have facilities with Category I special nuclear material. Category I special nuclear material includes specified quantities of plutonium and highly enriched uranium in forms of assembled nuclear weapons and test devices, major nuclear components, and other high-grade materials such as solutions and oxides. Specifically, we examined, among other things, (1) the reasons DOE needed almost 2 years to develop a new DBT; (2) the higher threat contained in the new

[1]See 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).

DBT; and (3) the remaining issues that need to be resolved in order for DOE to fully defend against the threat contained in the new DBT.[2]

To carry out our objectives, we reviewed draft DBTs, the final May 2003 DBT, and DOE policy and planning documents, including orders, implementation guidance, and reports. We met with officials from DOE and NNSA headquarters and field offices. We obtained information primarily from DOE's Office of Security, Office of Independent Oversight and Performance Assurance, and Office of Environmental Management; NNSA's Office of Defense Nuclear Security; and NNSA's Nuclear Safeguards and Security Program. We visited all three of NNSA's three design laboratories and its two production plants that possess Category I special nuclear material, as well as NNSA's Office of Secure Transportation. We also visited the four EM sites that, at the time, contained Category I special nuclear materials. At each site we met with both federal and contractor officials and reviewed pertinent supporting documentation. We also discussed postulated terrorist threats to nuclear weapon facilities with two Department of Defense (DOD) organizations: the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence; and the Defense Intelligence Agency. We also reviewed *The Postulated Threat to U.S. Nuclear Weapon Facilities and Other Selected Strategic Facilities*, henceforth referred to as the Postulated Threat, which is the intelligence community's January 2003 official assessment of potential terrorist threats to nuclear weapon facilities.

We performed our work from December 2001 through April 2004 in accordance with generally accepted government auditing standards.

In summary, we found that while DOE has taken some important actions in its response to the terrorist attacks of September 11, 2001, DOE struggled to develop its new DBT. The DBT that DOE ultimately developed, however, is substantially more demanding than the previous one. Because the new DBT is more demanding and because DOE wants to implement new protective strategies within 2 years, DOE must press forward with additional actions to ensure that it is fully prepared to

[2]We testified on these issues before the Subcommittee on National Security, Emerging Threats, and International Relations, House Committee on Government Reform, on June 24, 2003. See U.S. General Accounting Office, *Nuclear Security: DOE's Response to the September 11, 2001 Terrorist Attacks*, GAO-03-898TC (Washington, D.C.: June 24, 2003).

provide a timely and cost effective defense of its most sensitive facilities. Specifically, we found the following:

- Development of the new DBT took almost 2 years because of (1) delays in developing an intelligence community assessment—known as the Postulated Threat—of the terrorist threat to nuclear weapon facilities, (2) DOE's lengthy comment and review process for developing policy, and (3) sharp debates within DOE and other government organizations over the size and capabilities of future terrorist threats and the availability of resources to meet these threats.

- While the May 2003 DBT identifies a larger terrorist threat than did the previous DBT, the threat identified in the new DBT, in most cases, is less than the threat identified in the intelligence community's Postulated Threat, on which the DBT has been traditionally based. The new DBT identifies new possible terrorist acts such as radiological, chemical, or biological sabotage. However, the criteria that DOE has selected for determining when facilities may need to be protected against these forms of sabotage may not be sufficient. For example, for chemical sabotage, the 2003 DBT requires sites to protect to "industry standards;" however, such standards currently do not exist.

- DOE has been slow to resolve a number of significant issues, such as issuing additional DBT implementation guidance, developing DBT implementation plans, and developing budgets to support these plans, that may affect the ability of its sites to fully meet the threat contained in the new DBT in a timely fashion. Consequently, DOE's deadline to meet the requirements of the new DBT by the end of fiscal year 2006 is probably not realistic for some sites.

In our report to you, we made seven recommendations to the Secretary of Energy that are intended to strengthen DOE's ability to meet the requirements of the new DBT, improve the department's ability to deal with future terrorist threats, and better inform Congress on departmental progress in meeting the threat contained in the new DBT and reducing risks to critical facilities at DOE sites. DOE did not comment specifically on our recommendations other than to say that the department would consider them as part of its Departmental Management Challenges for 2004. DOE has identified the DBT as a major departmental initiative within the National Security Management Challenge.

Background

Category I special nuclear materials are present at the three design laboratories—the Los Alamos National Laboratory in Los Alamos, New

Mexico; the Lawrence Livermore National Laboratory in Livermore, California; and the Sandia National Laboratory in Albuquerque, New Mexico—and two production sites—the Pantex Plant in Amarillo, Texas, and the Y-12 Plant in Oak Ridge, Tennessee, operated by NNSA. Special nuclear material is also present at former production sites, including the Savannah River Site in Savannah River, South Carolina, and the Hanford Site in Richland, Washington. These former sites are now being cleaned up by DOE's Office of Environmental Management (EM).[3] Furthermore, NNSA's Office of Secure Transportation transports these materials among the sites and between the sites and DOD bases. Contractors operate each site for DOE.[4] NNSA and EM have field offices collocated with each site. In fiscal year 2004, NNSA and EM expect to spend nearly $900 million on physical security at their sites.[5] Physical security combines security equipment, personnel, and procedures to protect facilities, information, documents, or material against theft, sabotage, diversion, or other criminal acts.

In addition to NNSA and EM, DOE has other important security organizations. DOE's Office of Security develops and promulgates orders and policies, such as the DBT, to guide the department's safeguards and security programs. DOE's Office of Independent Oversight and Performance Assurance supports the department 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. Under a recent reorganization, these two offices were incorporated into the new Office of Security and Safety Performance Assurance. Each office, however, retains its individual missions, functions, structure, and relationship to the other.

[3]At the time of our review, the Rocky Flats Environmental Technology Site in Rocky Flats, Colorado, was in the process of shipping its remaining Category I special nuclear material primarily to the Savannah River Site. This has now been completed. In addition, responsibility for the Idaho National Engineering and Environmental Laboratory, in Idaho Falls, Idaho, which is also a Category I special nuclear material site, was transferred from DOE's EM to DOE's Office of Nuclear Energy in May 2003.

[4]Federal employees instead of contractors operate the assets of the Office of Secure Transportation.

[5]Other DOE program offices, such as the Office of Science and Office of Nuclear Energy operate sites that may contain Category I special nuclear material. In fiscal year 2004, these program offices expect to spend $118 million on security.

The risks associated with Category I special nuclear materials vary but include the nuclear detonation of a weapon or test device at or near design yield, the creation of improvised nuclear devices capable of producing a nuclear yield, theft for use in an illegal nuclear weapon, and the potential for sabotage in the form of radioactive dispersal. Because of these risks, DOE has long employed risk-based security practices.

The key component of DOE's well-established, risk-based security practices is the DBT, a classified document that identifies the characteristics of the potential threats to DOE assets. The DBT has been traditionally based on a classified, multiagency intelligence community assessment of potential terrorist threats, known as the Postulated Threat. The DBT considers a variety of threats in addition to the terrorist threat. Other adversaries considered in the DBT include criminals, psychotics, disgruntled employees, violent activists, and spies. The DBT also considers the threat posed by insiders, those individuals who have authorized, unescorted access to any part of DOE facilities and programs. Insiders may operate alone or may assist an adversary group. Insiders are routinely considered to provide assistance to the terrorist groups found in the DBT. The threat from terrorist groups is generally the most demanding threat contained in the DBT.

DOE counters the terrorist threat specified in the DBT with a multifaceted protective system. While specific measures vary from site to site, all protective systems at DOE's most sensitive sites employ a defense-in-depth concept that includes sensors, physical barriers, hardened facilities and vaults, and heavily armed paramilitary protective forces equipped with such items as automatic weapons, night vision equipment, body armor, and chemical protective gear.

Depending on the material, protective systems at DOE Category I special nuclear material sites are designed to accomplish the following objectives in response to the terrorist threat:

- *Denial of access*. For some potential terrorist objectives, such as the creation of an improvised nuclear device, DOE may employ a protection strategy that requires the engagement and neutralization of adversaries before they can acquire hands-on access to the assets.

- *Denial of task*. For nuclear weapons or nuclear test devices that terrorists might seek to steal, DOE requires the prevention and/or neutralization of

the adversaries before they can complete a specific task, such as stealing such devices.

- *Containment with recapture.* 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 vulnerability assessments. 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 assets, such as special nuclear material. To conduct such assessments, 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 a group of mock terrorists.

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, 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 Category I special nuclear material—and mitigate the risks to these assets to an acceptable level. Levels of risk—high, medium, and low—are assigned classified numerical values and are derived from a mathematical equation that compares a terrorist group's capabilities with the overall effectiveness of the crucial elements of the site's protective forces and systems.

Historically, DOE has striven to keep its most critical assets at a low risk level and may insist on immediate compensatory measures should a significant vulnerability develop that increases risk above the low risk level. Compensatory measures could include such things as deploying additional protective forces or curtailing operations until the asset can be better protected. In response to a September 2000 DOE Inspector General's report recommending that DOE establish a policy on what actions are required once high or moderate risk is identified, in September 2003, DOE's Office of Security issued a policy clarification stating that identified high risks at facilities must be formally reported to the Secretary

of Energy or Deputy Secretary within 24 hours. In addition, under this policy clarification, identified high and moderate risks require corrective actions and regular reporting.

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. DOE Orders also require field offices to comprehensively survey contractors' operations for safeguards and security every year. DOE's Office of Independent Oversight and Performance Assurance provides yet another check through its comprehensive inspection program. All deficiencies identified during surveys and inspections require the contractors to take corrective action.

Development of the New DBT Took Almost 2 Years Because of Delays in Developing the Postulated Threat and DOE's Lengthy Review and Comment Process

In the immediate aftermath of September 11, 2001, DOE officials realized that the then current DBT, issued in April 1999 and based on a 1998 intelligence community assessment, was obsolete. The September 11, 2001, terrorist attacks suggested larger groups of terrorists, 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 was difficult and took 21 months because of delays in issuing the Postulated Threat, debates over the size of the future threat and the cost to meet it, and the DOE policy process.

As mentioned previously, DOE's new DBT is based on a study known as the Postulated Threat, which was developed by the U.S. intelligence community. The intelligence community originally planned to complete the Postulated Threat by April 2002; however, the document was not completed and officially released until January 2003, about 9 months behind the original schedule. According to DOE and DOD officials, this delay resulted from other demands placed on the intelligence community after September 11, 2001, as well as from sharp debates among the organizations developing the Postulated Threat over the size and capabilities of future terrorist threats and the resources needed to meet these threats.

While waiting for the new Postulated Threat, DOE developed several drafts of its new DBT. During this process, debates, similar to those that occurred during the development of the Postulated Threat, emerged in DOE. Like the participants responsible for developing the Postulated Threat, during the development of the DBT, DOE officials debated the size

of the future terrorist threat and the costs to meet it. DOE officials at all levels told us that concern over resources played a large role in developing the 2003 DBT, with some officials calling the DBT the "funding basis 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 the requirements for the size of protective forces appear to have played a significant role in determining the terrorist group numbers contained in prior DBTs.

Finally, DOE developed the DBT using DOE's policy process, which emphasizes developing consensus through a review and comment process by program offices, such as EM and NNSA. However, many DOE and contractor officials found that the policy process for developing the new DBT was laborious and not timely, especially given the more dangerous threat environment that has existed since September 11, 2001. As a result, during the time it took DOE to develop the new DBT, its sites were only required to defend against the terrorist group defined in the 1999 DBT, which, in the aftermath of September 11, 2001, DOE officials realized was obsolete.

The May 2003 DBT Identifies a Larger Terrorist Threat, but in Most Cases is Less Than the Terrorist Threat Identified by the Postulated Threat

While the May 2003 DBT identifies a larger terrorist group than did the previous DBT, the threat identified in the new DBT, in most cases, is less than the terrorist threat identified in the intelligence community's Postulated Threat. The Postulated Threat estimated that the force attacking a nuclear weapons site would probably be a relatively small group of terrorists, although it was possible that an adversary might use a greater number of terrorists if that was the only way to attain an important strategic goal. In contrast to the Postulated Threat, DOE is preparing to defend against a significantly smaller group of terrorists attacking many of its facilities. Specifically, only for its sites and operations that handle nuclear weapons is DOE currently preparing to defend against an attacking force that approximates the lower range of the threat identified in the Postulated Threat. For its other Category I special nuclear material sites, all of which fall under the Postulated Threat's definition of a nuclear weapons site, DOE is requiring preparations to defend against a terrorist force significantly smaller than was identified in the Postulated Threat. DOE calls this a graded threat approach.

Some of these other sites, however, may have improvised nuclear device concerns that, if successfully exploited by terrorists, could result in a nuclear detonation. Nevertheless, under the graded threat approach, DOE

requires these sites only to be prepared to defend against a smaller force of terrorists than was identified by the Postulated Threat. Officials in DOE's Office of Independent Oversight and Performance Assurance disagreed with this approach and noted that sites with improvised nuclear device concerns should be held to the same requirements as facilities that possess nuclear weapons and test devices since the potential worst-case consequence at both types of facilities would be the same—a nuclear detonation. Other DOE officials and an official in DOD's Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence disagreed with the overall graded threat approach, believing that the threat should not be embedded in the DBT by adjusting the number of terrorists that might attack a particular target.

DOE Office of Security officials cited three reasons for why the department departed from the Postulated Threat's assessment of the potential size of terrorist forces. First, these officials stated that they believed that the Postulated Threat only applied to sites that handled completed nuclear weapons and test devices. However, both the 2003 Postulated Threat, as well as the preceding 1998 Postulated Threat, state that the threat applies to nuclear weapons and special nuclear material without making any distinction between them. Second, DOE Office of Security officials believed that the higher threat levels contained in the 2003 Postulated Threat represented the worst potential worldwide terrorist case over a 10-year period. These officials noted that while some U.S. assets, such as military bases, are located in parts of the world where terrorist groups receive some support from local governments and societies thereby allowing for an expanded range of capabilities, DOE facilities are located within the United States, where terrorists would have a more difficult time operating. Furthermore, DOE Office of Security officials stated that the DBT focuses on a nearer-term threat of 5 years. As such, DOE Office of Security officials said that they chose to focus on what their subject matter experts believed was the maximum, credible, near-term threat to their facilities. However, while the 1998 Postulated Threat made a distinction between the size of terrorist threats abroad and those within the United States, the 2003 Postulated Threat, reflecting the potential implications of the September 2001 terrorist attacks, did not make this distinction. Finally, DOE Office of Security officials stated that the Postulated Threat document represented a reference guide instead of a policy document that had to be rigidly followed. The Postulated Threat does acknowledge that it should not be used as the sole consideration to dictate specific security requirements and that decisions regarding security risks should be made and managed by decision makers in policy offices. However, DOE has traditionally based its DBT on the Postulated

Threat. For example, the prior DBT, issued in 1999, adopted exactly the same terrorist threat size as was identified by the 1998 Postulated Threat.

Finally, the department's criteria for determining the severity of radiological, chemical, and biological sabotage may be insufficient. For example, the criterion used for protection against radiological sabotage is based on acute radiation dosages received by individuals. However, this criterion may not fully capture or characterize the damage that a major radiological dispersal at a DOE site might cause. For example, according to a March 2002 DOE response to a January 23, 2002, letter from Representative Edward J. Markey, a worst-case analysis at one DOE site showed that while a radiological dispersal would not pose immediate, acute health problems for the general public, the public could experience measurable increases in cancer mortality over a period of decades after such an event. Moreover, releases at the site could also have environmental consequences requiring hundreds of millions to billions of dollars to clean up. Contamination could also affect habitability for tens of miles from the site, possibly affecting hundreds of thousands of residents for many years. Likewise, the same response showed that a similar event at a NNSA site could result in a dispersal of plutonium that could contaminate several hundred square miles and ultimately cause thousands of cancer deaths. For chemical sabotage standards, the 2003 DBT requires sites to protect to industry standards. However, we reported March 2003 year that such standards currently do not exist.[6] Specifically, we found that no federal laws explicitly require chemical facilities to assess vulnerabilities or take security actions to safeguard their facilities against a terrorist attack. Finally, the protection criteria for biological sabotage are based on laboratory safety standards developed by the U.S. Centers for Disease Control and not physical security standards.

[6]See U.S. General Accounting Office, *Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness is Unknown*, GAO-03-439 (Washington, D.C.: Mar. 14, 2003).

DOE Has Been Slow to Resolve a Number of Significant Issues That May Affect the Ability of its Sites to Fully Meet the Threat Contained in the New DBT

While DOE issued the final DBT in May 2003, it has only recently resolved a number of significant issues that may affect the ability of its sites to fully meet the threat contained in the new DBT in a timely fashion and is still addressing other issues. Fully resolving all of these issues may take several years, and the total cost of meeting the new threats is currently unknown. Because some sites will be unable to effectively counter the higher threat contained in the new DBT for up to several years, these sites should be considered to be at higher risk under the new DBT than they were under the old DBT.

In order to undertake the necessary range of vulnerability assessments to accurately evaluate their level of risk under the new DBT and implement necessary protective measures, DOE recognized that it had to complete a number of key activities. DOE only recently completed three of these key activities. First, in February 2004, DOE issued its revised Adversary Capabilities List, which is a classified companion document to the DBT, that lists the potential weaponry, tactics, and capabilities of the terrorist group described in the DBT. This document has been amended to include, among other things, heavier weaponry and other capabilities that are potentially available to terrorists who might attack DOE facilities. DOE is continuing to review relevant intelligence information for possible incorporation into future revisions of the Adversary Capabilities List.

Second, DOE also only recently provided additional DBT implementation guidance. In a July 2003 report, DOE's Office of Independent Oversight and Performance Assurance noted that DOE sites had found initial DBT implementation guidance confusing. For example, when the Deputy Secretary of Energy issued the new DBT in May 2003, the cover memo said the new DBT was effective immediately but that much of the DBT would be implemented in fiscal years 2005 and 2006. According to a 2003 report by the Office of Independent Oversight and Performance Assurance, many DOE sites interpreted this implementation period to mean that they should, through fiscal year 2006, only be measured against the previous, less demanding 1999 DBT.

In response to this confusion, the Deputy Secretary issued further guidance in September 2003 that called for the following, among other things:

- DOE's Office of Security to issue more specific guidance by October 22, 2003, regarding DBT implementation expectations, schedules, and requirements. DOE issued this guidance January 30, 2004.

- Quarterly reports showing sites' incremental progress in meeting the new DBT for ongoing activities. The first series of quarterly progress reports may be issued in July 2004.

- Immediate compliance with the new DBT for new and reactivated operations.

A third important DBT-related issue was just completed in early April 2004. A special team created in the 2003 DBT, composed of weapons designers and security specialists, finalized its report on each site's improvised nuclear device vulnerabilities. The results of this report were briefed to senior DOE officials in March 2004 and the Deputy Secretary of Energy issued guidance, based on this report, to DOE sites in early April 2004. As a result, some sites may be required under the 2003 DBT to shift to enhanced protection strategies, which could be very costly. This special team's report may most affect EM sites because their improvised nuclear device potential had not previously been explored.

Finally, DOE's Office of Security has not completed all of the activities associated with the new vulnerability assessment methodology it has been developing for over a year. DOE's Office of Security believes this methodology, which uses a new mathematical equation for determining levels of risk, will result in a more sensitive and accurate portrayal of each site's defenses-in-depth and the effectiveness of sites' protective systems (i.e., physical security systems and protective forces) when compared with the new DBT. DOE's Office of Security decided to develop this new equation because its old mathematical equation had been challenged on technical grounds and did not give sites credit for the full range of their defenses-in-depth. While DOE's Office of Security completed this equation in December 2002, officials from this office believe it will probably not be completely implemented at the sites for at least another year for two reasons. First, site personnel who implement this methodology will require additional training to ensure they are employing it properly. DOE's Office of Security conducted initial training in December 2003, as well as a prototype course in February 2004, and has developed a nine-course vulnerability assessment certification program. Second, sites will have to collect additional data to support the broader evaluation of their protective systems against the new DBT. Collecting these data will require additional computer modeling and force-on-force performance testing.

Because of the slow resolution of some of these issues, DOE has not developed any official long-range cost estimates or developed any integrated, long-range implementation plans for the May 2003 DBT.

Specifically, neither the fiscal year 2003 nor 2004 budgets contained any provisions for DBT implementation costs. However, during this period, DOE did receive additional safeguards and security funding through budget reprogramming and supplemental appropriations. DOE is using most of these additional funds to cover the higher operational costs associated with the increased security condition (SECON) measures. DOE has gathered initial DBT implementation budget data and has requested additional DBT implementation funding in the fiscal year 2005 budget: $90 million for NNSA, $18 million for the Secure Transportation Asset within the Office of Secure Transportation, and $26 million for EM. However, DOE officials believe the budget data collected so far has been of generally poor quality because most sites have not yet completed the necessary vulnerability assessments to determine their resource requirements. Consequently, the fiscal year 2006 budget may be the first budget to begin to accurately reflect the safeguards and security costs of meeting the requirements of the new DBT.

Reflecting these various delays and uncertainties, in September 2003, the Deputy Secretary changed the deadline for DOE program offices, such as EM and NNSA, to submit DBT implementation plans from the original target of October 2003 to the end of January 2004. NNSA and EM approved these plans in February 2004. DOE's Office of Security has reviewed these plans and is planning to provide implementation assistance to sites that request it. DOE officials have described these plans as being ambitious in terms of the amount of work that has to be done within a relatively short time frame and dependent on continued increases in safeguards and security funding, primarily for additional protective force personnel. However, some plans may be based on assumptions that are no longer valid. Revising these plans could require additional resources, as well as add time to the DBT implementation process.

A DOE Office of Budget official told us that current DBT implementation cost estimates do not include items such as closing unneeded facilities, transporting and consolidating materials, completing line item construction projects, and other important activities that are outside of the responsibility of the safeguards and security program. For example, EM's Security Director told us that for EM to fully comply with the DBT requirements in fiscal year 2006 at one of its sites, it will have to

- close and de-inventory two facilities,
- consolidate excess materials into remaining special nuclear materials facilities, and

- move consolidated Category I special nuclear material, which NNSA's Office of Secure Transportation will transport, to another site.

Likewise, the EM Security Director told us that to meet the DBT requirements at another site, EM will have to accelerate the closure of one facility and transfer special nuclear material to another facility on the site. The costs to close these facilities and to move materials within a site are borne by the EM program budget and not by the EM safeguards and security budget. Similarly, the costs to transport the material between sites are borne by NNSA's Office of Secure Transportation budget and not by EM's safeguards and security budget. A DOE Office of Budget official told us that a comprehensive, department-wide approach to budgeting for DBT implementation that includes such important program activities as described above is needed; however, such an approach does not currently exist.

The department plans to complete DBT implementation by the end of fiscal year 2006. However, most sites estimate that it will take 2 to 5 years, if they receive adequate funding, to fully meet the requirements of the new DBT. During this time, sites will have to conduct vulnerability assessments, undertake performance testing, and develop Site Safeguards and Security Plans. Consequently, full DBT implementation could occur anywhere from fiscal year 2005 to fiscal year 2008. Some sites may be able to move more quickly and meet the department's deadline of the end of fiscal year 2006.

Because some sites will be unable to effectively counter the threat contained in the new DBT for a period of up to several years, these sites should be considered to be at higher risk under the new DBT than they were under the old DBT. For example, the Office of Independent Oversight and Performance Assurance has concluded in recent inspections that at least two DOE sites face fundamental and not easily resolved security problems that will make meeting the requirements of the new DBT difficult. For other DOE sites, their level of risk under the new DBT remains largely unknown until they can conduct the necessary vulnerability assessments.

In closing, while DOE struggled to develop its new DBT, the DBT that DOE ultimately developed is substantially more demanding than the previous one. Because the new DBT is more demanding and because DOE wants to implement it by end of fiscal year 2006—a period of about 29 months—DOE must press forward with a series of additional actions to

ensure that it is fully prepared to provide a timely and cost effective defense of its most sensitive facilities.

First, because the September 11, 2001, terrorist attacks suggested larger groups of terrorists with broader aspirations for causing mass casualties and panic, we believe that the DBT development process that was used requires reexamination. While DOE may point to delays in the development of the Postulated Threat as the primary reason for the almost 2 years it took to develop a new DBT, DOE was also working on the DBT itself for most of that time. We believe the difficulty associated with developing a consensus using DOE's traditional policy-making process was a key factor in the time it took to develop a new DBT. During this extended period, DOE's sites were only being defended against what was widely recognized as an obsolete terrorist threat level.

Second, we are concerned about two aspects of the resulting DBT. We are not persuaded that there is sufficient difference, in its ability to achieve the objective of causing mass casualties or creating public panic, between the detonation of an improvised nuclear device and the detonation of a nuclear weapon or test device at or near design yield that warrants setting the threat level at a lower number of terrorists. Furthermore, while we applaud DOE for adding additional requirements to the DBT such as protection strategies to guard against radiological, chemical, and biological sabotage, we believe that DOE needs to reevaluate its criteria for terrorist acts of sabotage, especially in the chemical area, to make it more defensible from a physical security perspective.

Finally, because some sites will be unable to effectively counter the threat contained in the new DBT for a period of up to several years, these sites should be considered to be at higher risk under the new DBT than they were under the old DBT. As a result, DOE needs to take a series of actions to mitigate these risks to an acceptable level as quickly as possible. To accomplish this, it is important for DOE to go about the hard business of a comprehensive department-wide approach to implementing needed changes in its protective strategy. Because the consequences of a successful terrorist attack on a DOE site could be so devastating, we believe it is important for DOE to better inform Congress about what sites are at high risk and what progress is being made to reduce these risks to acceptable levels.

Mr. Chairman, this concludes our prepared statement. We would be happy to respond to any questions that 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 and Jonathan Gill also made key contributions to this testimony.

GAO's Mission

The General Accounting 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 the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

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. General Accounting 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

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548