

GAO

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

April 2004

NUCLEAR SECURITY

DOE Needs to Resolve Significant Issues Before It Fully Meets the New Design Basis Threat





Highlights of [GAO-04-623](#), a report to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, House Committee on Government Reform

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 the potential size and capabilities of terrorist forces. The terrorist attacks of September 11, 2001, rendered the then-current DBT obsolete. GAO examined DOE's response to the September 11, 2001, terrorist attacks, identified why DOE took almost 2 years to develop a new DBT, analyzed the higher threat in the new DBT, and identified the remaining issues that need to be resolved in order for DOE to meet the threat contained in the new DBT.

What GAO Recommends

GAO is making a series of recommendations to the Secretary of Energy to strengthen DOE's ability to meet the requirements of the new DBT and to strengthen the department's ability to deal with future terrorist threats. DOE did not comment on the specific recommendations, but said that it would consider them as part of its Departmental Management Challenges for 2004.

www.gao.gov/cgi-bin/getrpt?GAO-04-623.

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 Needs to Resolve Significant Issues Before It Fully Meets the New Design Basis Threat

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, DOE must press forward with additional actions to ensure that it is fully prepared to provide a timely and cost effective defense.

- DOE took immediate steps to improve physical security in the aftermath of the September 11, 2001, terrorist attacks. DOE's most visible effort involved moving to higher levels of security readiness, known as security condition (SECON) levels. While this effort has increased the visible deterrence at DOE sites, it has been expensive and has resulted in fatigue, retention problems, and less training for most sites' protective forces. In addition, the effectiveness of these increased SECON levels generally have not been assessed using the vulnerability assessment tools, such as computer modeling and full-scale force-on-force exercises, that DOE routinely uses to develop protective force strategies for its sites.
- 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 and (2) DOE's lengthy comment and review process for developing policy. In addition, during the DBT development process, there were 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 that contributed to the delay.
- 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.
- 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.

Contents

Letter		1
	Results in Brief	5
	Background	8
	DOE Took Immediate Steps to Improve Security in the Aftermath of September 11, 2001, but the Effectiveness of These Steps Is Uncertain	12
	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	15
	The May 2003 DBT Identifies a Larger Terrorist Threat, but in Most Cases is Less Than the Terrorist Threat Identified by an Important Intelligence Community Assessment	18
	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	23
	Conclusions	27
	Recommendations for Executive Action	28
	Agency Comments and Our Evaluation	29
Appendix I	Comments from the Department of Energy	30
Appendix II	GAO Contact and Staff Acknowledgments	31
	GAO Contact	31
	Staff Acknowledgments	31

Abbreviations

DBT	design basis threat
DOD	Department of Defense
DOE	Department of Energy
EM	Office of Environmental Management
NNSA	National Nuclear Security Administration
SECON	security condition

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



G A O

Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

April 27, 2004

The Honorable Christopher Shays
Chairman, Subcommittee on National Security,
Emerging Threats, and International Relations
Committee on Government Reform
House of Representatives

Dear Mr. Chairman:

The Department of Energy (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. Weapons or special nuclear material 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 the National Nuclear Security Administration (NNSA)—a separately organized agency within DOE.¹ 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).² Furthermore, NNSA's Office of Secure Transportation transports these materials among the sites and between the sites and Department of Defense (DOD) bases. Contractors operate each site for DOE.³ NNSA and

¹NNSA is responsible for the nation's nuclear weapons, nonproliferation, and naval reactors programs. We did not include Naval Reactors in our review because that office is a semiautonomous entity with a unique security structure and program.

²At 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.

³Federal employees instead of contractors operate the assets of the Office of Secure Transportation.

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. Physical security combines security equipment, personnel, and procedures to protect facilities, information, documents, or material against theft, sabotage, diversion, or other criminal acts.

All the sites listed above have facilities that contain Category I special nuclear material. Category I material includes specified quantities of plutonium and highly enriched uranium in the following forms: (1) assembled nuclear weapons and test devices; (2) pure products containing higher concentrations of plutonium or highly enriched uranium, such as major nuclear components and recastable metal; and (3) high-grade materials, such as carbides, oxides, solutions, and nitrates. 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 Category I special nuclear material poses such risks, DOE's effective management of the safeguards and security program, which includes developing safeguards and security policies and overseeing contractors' activities, is essential to preventing an unacceptable, adverse impact on national security.⁴ 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. The DBT is a key component of DOE's well-established, risk-based security practices. DOE requires the contractors operating its sites to provide sufficient protective forces and equipment to defend against the threat contained in the DBT. The effectiveness of these protective systems is periodically assessed through a process known as a vulnerability assessment. 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.

⁴See 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).

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. Specifically, as agreed with your office, we (1) examined DOE's response to the September 11, 2001, attacks; (2) identified the reasons DOE needed almost 2 years to develop a new DBT; (3) analyzed the higher threat contained in the new DBT; and (4) identified the remaining issues that need to be resolved in order for DOE to fully defend against the threat contained in the new DBT.⁵

To determine how DOE responded to the terrorist attacks of September 11, 2001, we reviewed relevant DOE policy and planning documents, including orders and guides, particularly DOE Order 470.1 and DOE Notice 473.6. In addition, we met with officials from DOE headquarters and site offices, as well as contractors who operate DOE sites. The primary offices we obtained information from were DOE's Office of Security, DOE's Office of Independent Oversight and Performance Assurance, DOE's Office of Environmental Management, NNSA's Office of Defense Nuclear Security, and NNSA's Nuclear Safeguards and Security Program. To review augmented security measures put into place after September 11, 2001, from March 2002 through June 2003, we visited nine DOE sites and one DOE program office that handle Category I special nuclear material. Specifically, we visited the Los Alamos National Laboratory and the NNSA Office of Los Alamos Site Operations in New Mexico, the Sandia National Laboratory and the NNSA Office of Kirtland Site Operations in New Mexico, the Lawrence Livermore National Laboratory and the NNSA Livermore Site Office in California, the Y-12 Plant and the NNSA Y-12 Site Office in Tennessee, the Pantex Plant and the NNSA Office of Amarillo Site Operations in Texas, and the NNSA's Office of Secure Transportation in New Mexico. We also visited the Savannah River Site and EM's Savannah River Operations Office in South Carolina, the Rocky Flats Environmental Technology Site and EM's Rocky Flats Field Office in Colorado, the Hanford Site and EM's Richland Operations Office in Washington, and the Idaho National Engineering and Environmental Laboratory and EM's Idaho Falls Operations Office in Idaho.

To determine why DOE needed almost 2 years to develop a new DBT, we reviewed historical documents, the four draft DBTs produced between

⁵We 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).

May 2002 and April 2003, the final May 2003 DBT, and other threat guidance provided to us by DOE's Office of Security. We also reviewed associated field and program office comments on the draft DBTs and threat guidance. We discussed the DBT development process with DOE's Office of Security, DOE's Office of Independent Oversight and Performance Assurance, EM and NNSA headquarters security offices, and federal and contractor personnel at all of the sites and field offices we visited. We also discussed postulated terrorist threats to nuclear weapon facilities with two 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. From May 2002 to May 2003, DOE denied us access to the draft DBTs it was developing; however, in May 2003, we were able to obtain access to the documents and complete our review.

To analyze the higher threat level contained in the new DBT, we examined previous DBTs and related documents provided to us by DOE's Office of Security. We traced how key parameters of the new DBT, such as the size of terrorist forces and the treatment of improvised nuclear devices, evolved during the 2002 through 2003 DBT development process and compared these parameters with previous DBTs and the Postulated Threat. We discussed the higher threat level and other key threat aspects contained in the final 2003 DBT, such as the graded threat approach; improvised nuclear device concerns; and radiological, chemical, and biological sabotage criteria; with DOE's Office of Security; DOE's Office of Independent Oversight and Performance Assurance; EM and NNSA headquarters security offices; federal and contractor personnel at all of the sites and field offices we visited; DOD's Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence; and the Defense Intelligence Agency. In order to determine what industry security standards exist to prevent terrorist acts of sabotage at industrial chemical facilities, we reviewed a report we issued in March 2003 on measures used to protect commercial chemical facilities.⁶

⁶See 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).

To identify the remaining issues that DOE must resolve before it can fully meet the threat contained in the new DBT, we met with DOE, EM, and NNSA headquarters security offices, as well as field security officials. We also reviewed relevant documents these offices provided. In particular, we reviewed recent Office of Independent Oversight and Performance Assurance inspection reports that identified some of the challenges associated with meeting the threat contained in the new DBT. DOE did not provide us with preliminary cost estimates for meeting the requirements of the DBT on the grounds that these costs had not yet been officially determined; however, DOE's Budget Office did outline for us potential mechanisms for funding DBT implementation over the next several years.

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

Results in Brief

DOE took immediate steps to improve physical security in the aftermath of the September 11, 2001, terrorist attacks. DOE's most visible effort involved moving to higher levels of security readiness, known as security condition (SECON) levels. On September 11, 2001, within a matter of hours, DOE 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 increase, among other things, the number of vehicle inspections and badge checks, the distance between public and sensitive areas to protect against large truck bombs, and the number of protective forces on duty, and to more heavily arm these forces. While sites are now at SECON level 3, most of these requirements still exist. Increased SECON levels have been expensive in both their financial cost and their toll on the readiness of the protective forces. Specifically, operating at the increased SECON levels has resulted in between \$18,000 to \$200,000 in unplanned costs per week at each site—primarily the result of overtime costs for the protective forces. More importantly, according to a June 2003 DOE Inspector General's report, the large amounts of overtime needed to meet these SECON requirements have resulted in fatigue, retention problems, and less training for protective forces.⁷ While the SECON levels have increased the visible deterrence at DOE sites, the effectiveness of the SECON levels in place at most sites has not been assessed using the vulnerability assessment tools, such as computer modeling and full-scale

⁷*Audit Report: Management of the Department's Protective Forces*, DOE/IG-0602, Department of Energy, Office of the Inspector General, June 2003.

force-on-force exercises, that DOE uses to develop protective force strategies for its sites. Consequently, DOE cannot assure itself that these enhanced requirements are providing effective increases in security. In its comments on our report, DOE has agreed to explore procedures to incorporate the evaluation of increased SECON levels into its vulnerability assessments.

Development of the DBT took almost 2 years because of delays in developing the Postulated Threat and DOE's lengthy review and comment process for developing policy. 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 over the size of the future threat and the availability of resources to meet it. 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.

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 these sites to be prepared to defend against a terrorist force significantly smaller than was identified in the Postulated Threat. DOE based its departure from the Postulated Threat on the conclusions of its own subject matter experts on what they judged likely to be the most credible, near-term terrorist threats to its facilities. The new DBT also 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, in March 2003, we reported that such standards currently do not exist. Consequently, without appropriate standards, DOE cannot ensure that its sites and facilities are adequately protected against the full range of consequences that might result from terrorist acts.

While DOE issued the final DBT in May 2003, it 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 DOE sites to fully meet the threat contained in the new DBT. For example, DOE has only recently issued additional DBT implementation guidance—several months behind DOE's original schedule—and developed initial DBT implementation plans. DOE officials currently do not have any official estimates of the overall costs of DBT implementation. In addition, DOE officials believed that budget information provided by sites for inclusion in the fiscal year 2005 budget was of generally poor quality because most sites had not yet completed the necessary vulnerability assessments to determine their resource requirements. Moreover, other important DBT-related issues remain unresolved. For example, the Secretary of Energy has not yet designated, as called for in the new DBT, which, if any, of DOE's sites have improvised nuclear device concerns. If a site is designated to have such a concern, it may be required to shift to a more demanding and costly protection strategy. As a result of these issues, DOE is unlikely to meet its own fiscal year 2006 deadline for full implementation of the requirements of the new DBT. Specifically, some sites estimate that it could take as long as 5 years, given adequate funding, to fully meet the requirements of the new DBT. 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 probably are at higher risk under the new DBT than they were under the old DBT.

We are making recommendations to the Secretary of Energy that are intended to strengthen DOE's ability to meet the requirements of the new DBT, as well as to strengthen the department's ability to deal with future terrorist threats. We are also recommending that the Secretary report to the Congress on departmental progress in meeting the threat contained in the new DBT and reducing risks to critical facilities at its sites.

We provided DOE with a draft of this report for review and comment. In its written comments, DOE said it was committed to the development and promulgation of an accurate and comprehensive DBT policy. 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

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 EM 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 EM sites.

In addition to NNSA and EM, DOE has two 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.

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 terrorists. Other adversaries considered in the DBT include criminals, psychotics, disgruntled employees, violent activists, and spies. The DBT also considers the threat posed by insiders, 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

- a variety of integrated alarms and sensors capable of detecting intruders;
- physical barriers, such as fences and antivehicle 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 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. In addition to routine oversight, DOE Orders require field offices to comprehensively survey contractors' operations for safeguards and security every year. 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. 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 site that has specified quantities of Category I special nuclear material. All deficiencies (findings) identified during a survey require the contractors to take corrective action.

DOE Took Immediate Steps to Improve Security in the Aftermath of September 11, 2001, but the Effectiveness of These Steps Is Uncertain

DOE 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.* Presidential Decision Directive 39, issued in June 1995, states that the United States shall give the highest priority to developing effective capabilities to detect, prevent, and defeat terrorists seeking nuclear weapons or materials. In response, DOE Notice 473.6 specifies SECONs that have to be implemented at its Category I special nuclear material sites in response to a terrorist threat. On September 11, 2001, within a matter of hours, DOE 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 to protect against large vehicle bombs; 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 December 2003, when the national threat warning system was elevated to Orange Alert. The new baseline for security at DOE sites is generally assumed to be the measures currently associated with SECON level 3.
- *Denial protection strategies.* On October 3, 2001, the Secretary of Energy issued a classified directive ordering all sites to develop and implement plans to move to a denial protection strategy. DOE Manual 5632.1C-1 states that a denial protection strategy should be used where unauthorized access presents an unacceptable risk. In this regard, denial programs are designed to prevent an unauthorized opportunity to credibly initiate a nuclear dispersal or detonation or to use available materials for on-site assembly of an improvised nuclear device. Denial has typically been understood to mean that terrorists would never gain access to certain types of special nuclear material. The October 2001 directive also increased levels of performance testing for the protection of special nuclear material at DOE's most critical facilities to ensure that these denial strategies were effective.
- *Conducted security reviews, studies, and analyses.* DOE 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 by aircraft, such as the attacks that occurred on September 11, 2001, or large

vehicle bombs. NNSA also 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 and set priorities for over 80 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 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 officials increased their communications 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 and because of such attacks' potentially devastating consequences, sites worked closely with the Federal Aviation Administration and the U.S. military.

Several benefits have resulted from these immediate measures. With respect to improved security, DOE security officials believe that the implementation of SECON levels 2 and 3 has, for example, increased the visible deterrence at DOE sites by placing more protective forces around the sites. Studies and analyses have also resulted in different and less vulnerable storage strategies for some special nuclear material. For example, one NNSA site purchased special fire and blast-resistant safes to store special nuclear material. Finally, some long-recognized security enhancement projects have received more funding, such as the construction of a new storage facility at an NNSA site, and efforts to control access to public areas and roads adjacent to several NNSA sites.

While these measures have produced several positive outcomes, they have also had the following negative impacts:

- First, the role of the implemented SECON measures in improving DOE physical security is uncertain. While DOE Notice 473.6, which established the department's SECON levels, does not explicitly require SECON measures to be performance tested, DOE Manual 473.2-2 states that performance tests must be used to realistically evaluate and verify the effectiveness of protective force programs. While some of the SECON measures, such as vehicle inspection checkpoints, have undergone some limited performance testing of their effectiveness, most DOE sites

generally have not assessed the SECON level measures in place using the vulnerability assessment tools, such as computer modeling and full-scale force-on-force performance tests, that play such a key role in developing and verifying protective strategies at their sites. Consequently, the effectiveness of SECON measures against other aspects of the 2003 DBT, such as a larger group of well-armed terrorists, is largely unknown. In its comments on our report, DOE agreed to explore procedures to incorporate the evaluation of increased SECON levels into its vulnerability assessments.

- Second, increased SECON measures have been expensive. DOE sites estimate that it costs each site from \$18,000 to nearly \$200,000 per 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. The costs of the higher SECON levels, however, can be measured in more than just budget dollars. Specifically, a June 2003 DOE Inspector General's 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. Additional protective forces have been hired and trained in an effort to provide some relief; however, the DOE Inspector General has found that the deployment of additional protective forces has been delayed by slow processing of the necessary security clearances.
- Third, 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, according to a NNSA security official, because of the high costs of maintaining SECON measures, one site had to delay purchasing weaponry and ammunition for its protective forces to use to defeat commercially available armored vehicles that could be used by terrorists.
- Fourth, the sites did not complete the implementation of the Secretary's October 3, 2001, denial directive because of confusion over its meaning and because of the projected high costs of implementation. Over the years, DOE has issued varying guidance on denial protection strategies and, as a result, the sites have approached denial protection from different perspectives. For example, some NNSA sites and operations have implemented the most stringent form of denial, which is now defined as denial of access. In contrast, other NNSA sites have plans in place to interrupt terrorists who have gained access to materials, now called a denial of task protection strategy. Most EM sites have practiced containment protection strategies augmented by recapture and recovery

capabilities. For sites that did not already have a denial strategy in place, moving to a full denial of access strategy appears to be enormously expensive, with some sites estimating it would cost from about \$30 million to \$200 million to implement the directive completely. Moreover, the performance testing requirements of this directive have generally not been conducted because of the already large amounts of protective force overtime required by the higher SECON levels. For example, a NNSA security official at one site estimated it would have to conduct as many as 30 full-scale force-on-force performance tests each year to comply with the Secretary's Directive. The 2003 DBT, however, has now replaced this directive by explicitly defining denial of access and denial of task protection strategies and when these strategies should be employed.

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

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

Under DOE Order 470.1, the DBT is intended to provide the foundation for all of DOE's protective strategies. For example, DOE Order 473.2 states that protective forces must be trained and equipped to defeat the terrorist groups contained in the DBT. 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 because of debates over the size of the future threat, the cost to meet it, and the DOE policy process.

The traditional basis for the DBT has been the Postulated Threat, which is conducted by the U.S. intelligence community, principally DOD's Defense Intelligence Agency, and the security organizations of a number of different agencies, including DOE. For example, DOE closely based its 1999 DBT on the 1998 Postulated Threat assessment and adopted the same number of terrorists as identified by the 1998 Postulated Threat as its highest threat to its facilities. Efforts to revise the Postulated Threat began soon after the terrorist attacks of September 11, 2001. 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 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.

While waiting for the new Postulated Threat, DOE developed a number of draft documents that culminated in the final May 20, 2003, DBT. These documents 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 because neither agency wanted to act without the benefit of the Postulated Threat.
- *January 2002—Interim Implementing Guidance.* DOE’s Office of Security issued this guidance so that DOE programs could begin to plan and budget for eventual increases in the DBT. This interim guidance suggested that sites begin planning for an increased number of adversaries over the 1999 DBT.
- *May 2002—Draft DBT.* DOE produced its first official draft DBT and labeled it an interim product pending the release of the Postulated Threat.
- *August 2002—Second Draft DBT.* This draft introduced the graded threat approach, which is an important feature in the final DBT.
- *December 2002—Third Draft DBT.*
- *April 2003—Fourth Draft DBT.* This draft was the first to consider the final January 2003 Postulated Threat.
- *May 2003—Final DBT.*

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 through the standard DOE review and comment process for developing policy as outlined in DOE Order 251.1A and DOE Manual 251.1-1A. This process emphasizes developing consensus and resolving conflicts and involving a wide number of DOE organizations and affected contractors. Once DOE formulates a proposed policy, it typically allows 60 days for review and comment and 60 days for issue resolution. While developing the 2003 DBT, DOE's Office of Security distributed the draft DBTs to DOE program and field offices and invited them to provide comments. Field offices distributed the drafts to contractors, who were also invited to provide comments. DOE's Office of Security considered these comments and often incorporated them into the next version of the DBT. DOE's Office of Security also continued to coordinate with the other federal organizations that have similar assets, chiefly DOD and the Nuclear Regulatory Commission. Having followed this process for 21 months, the Deputy Secretary of Energy signed the revised DBT in May 2003. According to the Director of Policy in DOE's Office of Security, the DBT was developed as fast as possible, given delays in completing the Postulated Threat and the constraints of the DOE policy system. He added that using the DOE policy process was difficult and time-consuming and inevitably added to delays in issuing the new DBT. Many officials in DOE's program offices and sites, as well as contractor officials, also found the process to be laborious and not timely, especially given the more dangerous threat environment that existed after the September 11, 2001, terrorist attacks.

During the 21 months it took to develop the DBT, DOE sites still officially followed the 1999 DBT, although their protective posture was augmented by implementing SECON level 2 and 3 measures. EM sites continued to conduct vulnerability assessments and develop Site Safeguards and Security Plans based on the 1999 DBT. In contrast, NNSA largely suspended the development of Site Safeguards and Security Plans pending the issuance of the new DBT, although NNSA did embark on a new vulnerability assessment process, called Iterative Site Analysis. NNSA performed Iterative Site Analysis exercises at a number of its sites. EM also conducted an Iterative Site Analysis at one site. Also during this period, 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 higher than the 1999 DBT, but it had done so only once before the 2003 DBT was issued.

The May 2003 DBT Identifies a Larger Terrorist Threat, but in Most Cases is Less Than the Terrorist Threat Identified by an Important Intelligence Community Assessment

Reflecting the post-September 11, 2001, environment, the May 2003 DBT, among other things, identifies a larger terrorist threat than did the previous DBT. It also mandates specific protection strategies and expands the range of terrorist objectives to include radiological, biological, and chemical sabotage. However, the threat identified in the new DBT, in most cases, is less than the terrorist threat identified in the intelligence community's Postulated Threat. Key features of the 2003 DBT include the following:

- *Expanded terrorist characteristics and goals.* The 2003 DBT assumes that terrorist groups are the following: well armed and equipped; trained in paramilitary and guerrilla warfare skills and small unit tactics; highly motivated; willing to kill, risk death, or commit suicide; and capable of attacking without warning. Furthermore, according to the 2003 DBT, terrorists might attack a DOE or NNSA facility for a variety of goals, including the theft of a nuclear weapon, nuclear test device, or special nuclear material; radiological, chemical, or biological sabotage; and the on-site detonation of a nuclear weapon, nuclear test device, or special nuclear material that results in a significant nuclear yield. DOE refers to such a detonation as an improvised nuclear device.
- *Increased size of the terrorist group threat.* The 2003 DBT increases the terrorist threat levels for the theft of the department's highest value assets—Category I special nuclear materials—although not in a uniform way. Previously, under the 1999 DBT, all DOE sites that possessed any type of Category I special nuclear material were required to defend against a uniform terrorist group composed of a relatively small number of individuals. Under the 2003 DBT, however, the department judges the theft of a nuclear weapon or test device to be more attractive to terrorists, and sites that have these assets are required to defend against a substantially higher number of terrorists than are other sites. For example, an NNSA site that, among other things, assembles and disassembles nuclear weapons, is required to defend against a larger terrorist group. Other NNSA sites, some of which fabricate nuclear weapons components, or EM sites that store excess plutonium, only have to defend against a smaller group of terrorists. However, the number of terrorists in the 2003 DBT is larger than the 1999 DBT number. DOE calls this a graded threat approach.

-
- *Mandated 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 must now implement specific protection strategies, such as denial of access, denial of task, or containment with recapture for their most sensitive facilities and assets. For example, one NNSA site is required under the new DBT to implement a denial of task strategy to prevent terrorists from stealing a nuclear weapon or test device. In contrast, other DOE sites are required to implement a containment with recapture strategy to prevent the theft of special nuclear material. However, if these sites have an improvised nuclear device concern, they will have to implement denial of access or denial of task strategies. Finally, sites will have to develop, for the first time, specific protection strategies for facilities, such as radioactive waste storage areas, wastewater treatment, and science laboratories, against the threat of radiological, chemical, or biological sabotage. Previously, in an April 1998 policy clarification, DOE's Office of Security had stated that, assuming that baseline security requirements were met, radiological dispersal sabotage events were not considered attractive to terrorists.
 - *Addressed the potential for improvised nuclear device concerns.* The new DBT establishes a team to report to the Secretary of Energy on each site's potential for improvised nuclear devices. Based on the teams' advice, the Secretary of Energy will have to designate whether a site has such a concern. This official designation should help address the general dissatisfaction with previous DOE policies for improvised nuclear devices, knowledge of which is carefully controlled and not shared widely with security officials. For example, some EM sites have had no information at all on their potential for this risk, and at least one NNSA site official believed that scenarios for such risks have not been fully characterized.
 - *Introduced aircraft threats and mitigation measures.* In the 1999 DBT, DOE only acknowledged the risk for unspecified air attacks but did not lay out any protective measures to mitigate this risk. In the 2003 DBT, DOE considers aircraft as airborne improvised explosive devices. DOE's new policy is to rely on other federal government agencies, such as the Departments of Homeland Security and Defense, to defeat such a threat. DOE sites are expected, however, to consider measures, such as how they handle and store their materials, to mitigate the consequences of an aircraft attack on existing facilities, and new DOE facility designs are expected to include features to mitigate the consequences of an attack. While DOE's 2003 DBT makes some important advances, aspects of the DBT raise several important issues.

First, 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 applies to nuclear weapons sites, which the Postulated Threat defines as research and development facilities with nuclear weapons, components, or special nuclear material; weapons production facilities; sites for long-term storage of nuclear weapons; and nuclear weapons in transport. With respect to these sites, the Postulated Threat specified the following:

- There is a credible threat to U.S. facilities with nuclear or chemical weapons or biological agents.
- A well-organized terrorist group presents the greatest and most likely threat in most circumstances.
- Terrorists may use aircraft as weapons.
- Terrorists may use multiple vehicle bombs loaded with explosives.
- Terrorist groups would probably consist of a small to medium sized group of well-armed and trained members. A larger force is possible if the group thought this was necessary to attain an important strategic goal.
- Terrorist objectives include the theft of a weapon, detonation of a nuclear weapon in place, radiological sabotage, mass casualties, and/or public panic.

In contrast to the Postulated Threat, DOE is preparing to defend against a significantly smaller group of terrorists attacking most 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 the other DOE sites that have Category I special nuclear material—all of which fall under the Postulated Threat's definition of a nuclear weapons site—DOE is currently only preparing to defend against a smaller number terrorists—or approximately the same number contained in its DBT in the early 1980s.

Second, and more critically, some of these sites 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. DOE's Office of Security cited subject matter expert opinion as support for this distinction. However, according to officials in DOE's Office of Independent Oversight and Performance Assurance, 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. Some 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 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 last year that such standards currently do not exist. Specifically, we found that no federal laws explicitly require chemical facilities to assess vulnerabilities or take security actions to safeguard their facilities against terrorist attack. Finally, the protection criteria for biological sabotage are based on laboratory safety standards developed by the U.S. Centers for Disease Control, not physical security standards.

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 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 in a timely fashion. Fully resolving 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 two of these key activities. First, in February 2004, DOE issued its 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 particular, the 2003 report found that one NNSA site was planning to conduct certain operations starting in 2003 that involved special nuclear material using security plans that did not comply with even the 1999 DBT. Consequently, the Office of Independent Oversight and Performance Assurance recommended that the site suspend these planned operations until it had adequate security plans that reflected the new DBT. NNSA security officials concurred with this recommendation and postponed the site's proposed operations.

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

Other important DBT-related issues remain unresolved. First, as noted earlier, 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. Based on this team's report, the Secretary may officially designate some sites as having an improvised nuclear device concern. If this designation is made, some sites may be required under the 2003 DBT to shift to a denial of access or denial of task protection strategy, which could be very costly. This special team's report may most affect EM sites because their improvised nuclear device potential had not been explored until this review, and their formal protection strategy remains at the less demanding containment with recapture and recovery level. DOE officials have not identified when the Secretary will make these designations.

Second, 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 used most of these additional funds to cover the higher operational costs associated with the increased 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.

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. For example, one NNSA site already has developed detailed plans and budgets to meet the new DBT requirements.

While this site may be already close to meeting the new DBT requirements, other DOE sites are at higher risk to the threats specified under the 2003 DBT than they were under the old 1999 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. 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.

Conclusions

DOE took a series of immediate actions in response to the terrorist attacks of September 11, 2001. While each of these actions have been important, in and of themselves, we believe 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 a post September 11, 2001 world. Rather, DOE must press forward with a series of actions to ensure that it is fully prepared to provide a timely and cost effective defense.

First, DOE needs to know the effectiveness of its most immediate response to September 11, 2001—the move to higher SECON levels. The higher SECON levels, while increasing the level of visible deterrence, have come at a significant cost in budget dollars and protective force readiness. We believe that DOE needs to follow its own policies and use its well-established vulnerability assessment methodology to evaluate the effectiveness of these additional security measures.

Second, because the September 11, 2001, terrorist attacks suggested larger groups of terrorists with broader aspirations of 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.

Third, 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. Consequently, 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 resolve a number of DBT and DBT-related issues and 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 inform the Congress about what sites are at high risk and what progress is being made to reduce these risks to acceptable levels.

Recommendations for Executive Action

In order to strengthen DOE's ability to meet the requirements of the new DBT, as well as to strengthen the department's ability to deal with future terrorist threats, we are making the following seven recommendations to the Secretary of Energy:

- Evaluate the cost and effectiveness of existing SECONs and how they are implemented using DOE's vulnerability assessment methodology.
- Review how the DBT is developed to determine if using the current policy-making approach is appropriate given the dynamic post-September 11, 2001, security environment.
- Reexamine the current application of the graded threat approach to sites that may have improvised nuclear device concerns.
- Reexamine the criteria established in the May 2003 DBT to determine levels of risk from radiological, biological, and chemical sabotage to ensure that they are appropriate from a security standpoint.
- Ensure that all remaining DBT and DBT related-issues, such as the designation of improvised nuclear device concerns and the new vulnerability assessment methodology, are completed on an expedited schedule.
- Develop and implement a department-wide, multiyear, fully resourced implementation plan for meeting the new DBT requirements that includes important programmatic activities such as the closure of facilities and the transportation of special nuclear materials.

-
- Report regularly to relevant congressional oversight committees on: (1) the status of DBT implementation as reflected by the required quarterly DBT implementation progress reports and (2) which sites and facilities are currently considered to be at high risk under the new DBT and what steps are being taken to mitigate these risks to acceptable levels.

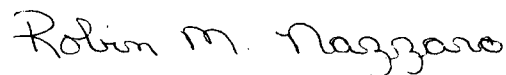
Agency Comments and Our Evaluation

We provided DOE with a draft of the classified version of this report for review and comment. In its written comments, DOE said it was committed to the development and promulgation of an accurate and comprehensive DBT policy. 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. In an enclosure attached to its comments, DOE also provided some additional technical information that we incorporated where appropriate. DOE's letter commenting on our draft report is presented in appendix I.

We are sending copies of this report to the Secretary of Energy, the Director of the Office of Management and Budget, and appropriate congressional committees. We also will make copies available to others upon request. In addition, the report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or your staff have any questions about this report, please call me at (202) 512-3841. Major contributors to this report are listed in appendix II.

Sincerely yours,



Robin M. Nazzaro
Director, Natural Resources
and Environment

Appendix I: Comments from the Department of Energy



Department of Energy
Washington, DC 20585

February 9, 2004

Ms. Robin Nazzaro
Director, Natural Resources and Environment
United States General Accounting Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Nazzaro:

The Department of Energy (DOE) appreciates the opportunity to review and comment on the General Accounting Office (GAO) draft report, "DOE Needs to Resolve Significant Issues Before it Fully Meets the New Design Basis Threat (U)," transmitted by your letter dated January 23, 2004, GAO-04-273C.

DOE is committed to the development and promulgation of an accurate and comprehensive Design Basis Threat (DBT) policy. The DBT is developed by the Office of Security and Safety Performance Assurance based on information from the intelligence organizations, both internal and external to DOE, national security information, and technical exchanges with the Department of Defense (DoD) and the Nuclear Regulatory Commission (NRC). The DBT is developed to consider all Departmental nuclear assets and the potential consequences of the loss or compromise of those assets.

With respect to the recommendations in the draft report, we will consider each of them as part of the Departmental Management Challenges for 2004. For the National Security Management Challenge, the DBT has already been identified as a major Departmental initiative.

Our specific comments are included in Enclosure 1. The comments provide additional information for consideration in the report and a suggested correction to one minor inaccuracy. Please contact Marshall Combs, Director, Office of Security, at 202-586-3345 if you have any additional questions.

Sincerely,

A handwritten signature in black ink, appearing to read "Glenn S. Podolsky".

Glenn S. Podolsky, Director
Office of Security and Safety
Performance Assurance

Enclosure (as stated)

cc:
K. McSillarow, DS
L. Brooks, NA-1
R. Card, US
T. Johnson, NA-1
B. Desmond, NA-55
M. Combs, SO-1
M. Kilpatrick, OA-1



Printed with soy ink on recycled paper

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

James Noel (202) 512-3591

Staff Acknowledgments

In addition to the individuals named above, Jonathan Gill, Chris Pacheco, Andrea Miller, Chris Abraham, Jill Berman, Carol Hernstadt Shulman, Joyce Evans, and Gail Traynham also made key contributions to this report.

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