Attachment 9

GAO

United States Government Accountability Office

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

March 2006

NUCLEAR POWER PLANTS

Efforts Made to Upgrade Security, but the Nuclear Regulatory Commission's Design Basis Threat Process Should Be Improved

This Report Is Temporarily Restricted Pending Official Public Release.

GAO

Accountability • Integrity • Reliability

GAO-06-388

March 2006

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-388, a report to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives

NUCLEAR POWER PLANTS

Efforts Made to Upgrade Security, but the Nuclear Regulatory Commission's Design Basis Threat Process Should Be Improved

Why GAO Did This Study

The nation's commercial nuclear power plants are potential targets for terrorists seeking to cause the release of radioactive material. The Nuclear Regulatory Commission (NRC), an independent agency headed by five commissioners, is responsible for regulating and overseeing security at the plants. In April 2003, in response to the terrorist attacks of September 11, 2001, NRC revised the design basis threat (DBT), which describes the threat that plants must be prepared to defend against in terms of the number of attackers and their training, weapons, and tactics. NRC has also restructured its program for testing security at the plants through force-on-force inspections, which consist of mock terrorist attacks. GAO was asked to review (1) the process NRC used to revise the DBT for nuclear power plants, (2) the actions nuclear power plants have taken to enhance security in response to the revised DBT, and (3) NRC's progress in strengthening the conduct of force-on-force inspections at the plants.

What GAO Recommends

GAO recommends that NRC improve its process for making changes to the DBT and evaluate and implement measures to further strengthen its force-on-force inspection program. Commenting on the draft report, NRC provided clarifications regarding the process NRC used to revise the DBT, but it neither agreed nor disagreed with GAO's recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-06-388.

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

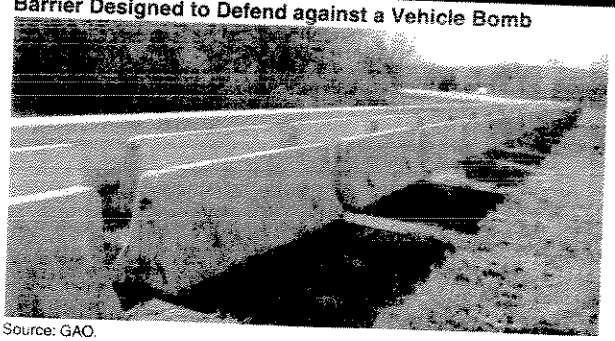
What GAO Found

NRC revised the DBT for nuclear power plants using a generally logical and well-defined process in which trained threat assessment staff made recommendations for changes based on an analysis of demonstrated terrorist capabilities. The process resulted in a DBT requiring plants to defend against a larger terrorist threat, including a larger number of attackers, a refined and expanded list of weapons, and an increase in the maximum size of a vehicle bomb. Key elements of the revised DBT, such as the number of attackers, generally correspond to the NRC threat assessment staff's original recommendations, but other important elements do not. For example, the NRC staff made changes to some recommendations after obtaining feedback from stakeholders, including the nuclear industry, which objected to certain proposed changes such as the inclusion of certain weapons. NRC officials said the changes resulted from further analysis of intelligence information. Nevertheless, GAO found that the process used to obtain stakeholder feedback created the appearance that changes were made based on what the industry considered reasonable and feasible to defend against rather than on an assessment of the terrorist threat itself.

Nuclear power plants made substantial security improvements in response to the September 11, 2001, attacks and the revised DBT, including security barriers and detection equipment, new protective strategies, and additional security officers. It is too early, however, to conclude that all sites are capable of defending against the DBT because, as of November 1, 2005, NRC had conducted force-on-force inspections at about one-third of the plants.

NRC has improved its force-on-force inspections—for example, by conducting inspections more frequently at each site. Nevertheless, in observing three inspections and discussing the program with NRC, GAO noted potential issues in the inspections that warrant NRC's continued attention. For example, a lapse in the protection of information about the planned scenario for a mock attack GAO observed may have given the plant's security officers knowledge that allowed them to perform better than they otherwise would have. A classified version of this report provides additional details about the DBT and security at nuclear power plants.

Barrier Designed to Defend against a Vehicle Bomb



Source: GAO.

Contents

Letter

Results in Brief 1
Background 5
NRC's Process for Revising Its DBT for Nuclear Power Plants Was Generally Logical and Well Defined, but Some Changes Were Not Clearly Linked to an Analysis of the Terrorist Threat 9
Nuclear Power Plants Made Substantial Changes to Their Security to Address the Revised DBT, but NRC Inspections Have Uncovered Problems 12
NRC Has Significantly Improved the Force-on-Force Inspection Program, but Challenges Remain 26
Conclusions 37
Recommendations for Executive Action 41
Agency Comments and Our Evaluation 43

Appendixes

Appendix I: Scope and Methodology 44
Appendix II: Details of Findings from NRC Reports on Baseline and Force-on-Force Inspections 47
Appendix III: Comments from the Nuclear Regulatory Commission 52
Appendix IV: GAO Contact and Staff Acknowledgments 55

Table

Table 1: Summary of Key Changes to the NRC DBT for Nuclear Power Plants 57

Figures

Figure 1: Diagram of a Sample Nuclear Power Plant Site 17
Figure 2: Example of a Bullet-Resistant Structure 27
Figure 3: Example of a Vehicle Barrier System 29
Figure 4: Example of an Active Vehicle Barrier System 32
34

Abbreviations

DBT	design basis threat
DHS	Department of Homeland Security
DOE	Department of Energy
FBI	Federal Bureau of Investigation
NEI	Nuclear Energy Institute
NRC	Nuclear Regulatory Commission

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.

GAO
Accountability * Integrity * Reliability
United States Government Accountability Office
Washington, D.C. 20548

March 14, 2006

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 nation's 103 operating commercial nuclear power plants, located at 65 sites in 31 states,[1] are potential targets for terrorists seeking to cause the release of radioactive material. Such a release, which may result from a meltdown of a plant's nuclear reactor core or damage to the spent nuclear fuel located at the site, could endanger public health and safety through exposure to radiation. The Nuclear Regulatory Commission (NRC), an independent agency headed by five commissioners, licenses commercial nuclear power plants and is responsible for regulating and overseeing their safe operation and security. According to NRC, there is a general credible threat of a terrorist attack to the nation's commercial nuclear power plants, in particular by al Qaeda and like-minded Islamic terrorist groups. For example, as discussed in *The 9/11 Commission Report*, nuclear power plants were among the targets considered in the original plan for the September 11, 2001, attacks.[2] However, NRC and intelligence agency officials we spoke with said they are not aware of current intelligence information indicating specific plans for an attack on a nuclear power plant.

NRC issues and enforces security-related regulations and orders, and nuclear power plant licensees implement security measures to meet NRC requirements. In particular, to ensure that nuclear power plants are secure against a terrorist attack, NRC formulates a design basis threat (DBT)—the threat that plants must defend against—and tests plants' ability to defend

[1]Some sites have more than one nuclear power plant.

[2]The National Commission on Terrorist Attacks Upon the United States issued *The 9/11 Commission Report* on July 22, 2004.

against the DBT.[3] The DBT characterizes the elements of a potential attack, including the number of attackers, their training, and the weapons and tactics they are capable of employing. NRC established the first DBT for nuclear power plants in the late 1970s. NRC conducts semiannual reviews of the potential terrorist threat to determine whether to make changes to the DBT and has revised it twice in response to changes in the threat. First, NRC expanded the DBT to include a vehicle laden with explosives after two incidents in 1993—the vehicle bombing of the World Trade Center and a vehicle intrusion incident at one of the nuclear power plant sites. NRC revised the DBT again in April 2003 in response to the terrorist attacks of September 11, 2001. Among other changes, this most recent DBT increased the number of attackers, refined and expanded the list of weapons and equipment that might be used in an attack, and increased the maximum size of a vehicle bomb that plants must defend against.

The DBT does not represent the maximum size and capability of a terrorist attack that is possible, but rather NRC's assessment of the threat that the nuclear power plants must be prepared to defend against "to ensure adequate protection of public health and safety." Furthermore, NRC regulations do not require nuclear power plants to protect against attacks directed against the sites by an "enemy of the United States," whether a foreign government or other person.[4] NRC originally included this provision in its regulations in 1967 (prior to issuing the first DBT for nuclear power plants). According to NRC officials, the provision was intended to address the possibility that Cuba might launch an attack on a nuclear power plant in Florida. In revising the DBT in April 2003, NRC did not use this provision to exempt plants from defending against terrorist groups such as al Qaeda but rather stated that a private security force (such as at a nuclear power plant) cannot reasonably be expected to defend against all threats—for example, airborne attacks.

Importantly, NRC also works with the Department of Homeland Security (DHS), the Federal Aviation Administration, the Federal Bureau of Investigation (FBI), and other federal, state, and local authorities to

[3]The DBT applied to nuclear power plants is intended to address the threat of radiological sabotage, a deliberate act against a plant that could directly or indirectly endanger public health and safety through exposure to radiation. NRC has a separate DBT (not the subject of this report) for NRC-licensed facilities storing material that could be used in a nuclear weapon.

[4]10 C.F.R. § 50.13.

coordinate an integrated response to a terrorist threat or attack on a nuclear power plant.[5] Furthermore, NRC does not directly gather intelligence information but rather receives intelligence from other agencies that it uses to formulate the DBT for nuclear power plants. NRC has access to intelligence information on terrorist activities and the domestic terrorist threat, including information from secure databases and intelligence reports from intelligence and other agencies.

Before receiving a license to operate a nuclear power plant, owners must develop and implement an NRC-approved security plan describing how they will defend the site against the threat presented in the DBT. As set forth in the security plan, the licensees employ private security forces (either hired directly or through a contractor) and provide them with the weapons, training, and equipment to defend the site. When NRC revised the DBT in 2003, it required licensees to develop new security plans describing their strategy for defending the sites against the revised DBT and to implement any security enhancements outlined in the plans by October 29, 2004. These security enhancements were in addition to other measures licensees implemented—such as stricter requirements for obtaining physical access to nuclear power plants, minimum training requirements for security officers, and limits on the work hours of the security force to address the potential for fatigue—in response to a series of security orders NRC issued after September 11, 2001. According to the Nuclear Energy Institute (NEI), which represents the nuclear power industry, the cost of security enhancements made since September 11, 2001, for all sites amounts to over $1.2 billion.[6]

NRC reviews and approves the security plans, conducts regular "baseline" inspections to verify compliance with the plans and other security requirements, and conducts force-on-force inspections involving multiple mock terrorist attacks to ensure sites are capable of defending against an

[5]The process of assessing threats to critical infrastructure, such as nuclear power plants, and identifying actions to reduce risks is often referred to as "risk management." Risk management acknowledges that while risk generally cannot be eliminated, enhancing protection from known or potential threats can reduce it. Furthermore, because security systems cannot protect against all threats, plans for actions to be taken if an event occurs that exceeds the capability of a security system are also important to reducing risk.

[6]NEI representatives told us this figure is current as of June 2004 based on a survey of nuclear power plants.

attack.[7] NRC considers the DBT, the security plans, and the results of its inspections and force-on-force exercises to contain "safeguards information" and other sensitive information, including details about security that could potentially aid terrorists plotting to attack a nuclear power plant.[8] Consequently, NRC does not make this information available to the general public, which has made it difficult for the agency to alleviate concerns about the level of security at nuclear power plants. The concerns center on whether the revised DBT adequately reflects the post-September 11 threat to nuclear power plants, and whether sites have done enough to respond to the threat.

You asked us to (1) examine the process NRC used to develop the April 2003 DBT for nuclear power plants, and (2) determine what actions nuclear power plants have taken to enhance security in response to the revised DBT. In addition, you asked us to review NRC's progress in strengthening the conduct of force-on-force inspections. In response, we have prepared this unclassified public report, which does not include certain details about the DBT and security at nuclear power plants that NRC considers to be safeguards information. We have prepared a classified version of this report in which we include such details.

To address the first objective, we reviewed the process NRC uses to analyze terrorist and criminal activities to assess the threat to nuclear power plants. We interviewed NRC officials responsible for analyzing information received from the intelligence and law enforcement communities and three of the four NRC commissioners serving at the time the DBT was revised to determine what factors they took into account in deciding on changes to the DBT. We compared the April 2003 DBT with NRC documents summarizing the threat to nuclear power plants and with the Department of Energy (DOE) DBT for its nuclear weapons facilities. We also interviewed officials from other federal agencies, including DHS and FBI, to obtain their assessments of the terrorist threat to nuclear

[7]For more information on these efforts, see GAO, *Nuclear Regulatory Commission: Preliminary Observations on Efforts to Improve Security at Nuclear Power Plants*, GAO-04-1064T (Washington, D.C.: Sept. 14, 2004); and *Nuclear Regulatory Commission: Oversight of Security at Commercial Nuclear Power Plants Needs to Be Strengthened*, GAO-03-752 (Washington, D.C.: Sept. 4, 2003).

[8]Safeguards information includes information that is not classified as National Security Information or Restricted Data but is considered sensitive because it identifies a licensee's security measures. Requirements for the protection of safeguards information are detailed in 10 C.F.R. § 73.21.

power plants, and we interviewed DOE officials regarding the DOE DBT. To address the second objective, we visited four nuclear power plant sites (one in each of the four NRC regions) to observe the security enhancements that sites made to address the revised DBT. We selected the four sites using a number of criteria, including size and type of reactor. GAO staff with a professional background in security accompanied us on our visits in order to provide the expertise needed to fully comprehend the sites' security strategies. At each site, we interviewed senior plant management, security managers, and security officers. Before visiting the four sites, we visited two other nuclear power plants to familiarize ourselves with NRC security requirements and the sites' security equipment and strategies; at one site, we observed an NRC baseline security inspection, and at the other, we observed a force-on-force inspection. We did not test the effectiveness of the security strategies at the four sites, and we cannot project the results of our work to all nuclear power plants. In addition to visiting four sites, we reviewed a sample of NRC's baseline and force-on-force inspection reports. To review NRC's progress in improving the force-on-force inspection program, we observed a total of three force-on-force inspections at two sites, reviewed NRC reports on force-on-force inspections, and interviewed NRC officials responsible for implementing the program. For other views on security at nuclear power plants, we interviewed officials from the nuclear industry group NEI and from the Project on Government Oversight, an independent nonprofit organization. (App. I presents a detailed discussion of our scope and methodology.) We conducted our work from November 2004 through January 2006 in accordance with generally accepted government auditing standards.

Results in Brief

The process NRC used to revise the DBT for nuclear power plants in April 2003 was generally logical and well defined. NRC made the revisions as part of a process that it had been using since formulating the first DBT in the late 1970s. NRC staff trained in threat assessment used reports and secure databases provided by intelligence agencies to monitor information on terrorist activities worldwide. To enhance the predictability and consistency of its assessments of this information and its recommendations to the NRC commissioners for changes to the DBT, the NRC threat assessment staff developed and used a comprehensive screening tool to analyze intelligence information and evaluate particular terrorist capabilities, or "adversary characteristics," for inclusion in the DBT. NRC's process also included consultation with DOE, which has a DBT for its facilities that process or store radiological materials and therefore

are also potential targets for radiological sabotage, and with stakeholders such as the nuclear power industry and state governments.

Using this process, NRC produced a revised DBT that generally, but not always, corresponded to the original recommendations of the threat assessment staff. For example, the maximum number of attackers in the revised DBT is based in part on the staff's analysis of the size of terrorist cells worldwide, as well as NRC's interpretation that multiple cells along the lines of the September 11, 2001, attacks would not necessarily target a single nuclear power plant. However, for other important elements of the DBT, such as the weapons that attackers could use against a plant, the final version of the revised DBT does not correspond to the staff's original recommendations. We identified two principal reasons for these differences:

- First, the threat assessment staff made changes to its initial recommendations after obtaining feedback from stakeholders, including the nuclear industry, on a draft of the DBT. A number of the changes reflected industry objections to the draft. For example, following meetings with industry, the staff decided not to recommend including certain weapons in the list of adversary characteristics that nuclear power plants should be prepared to defend against. In its comments, the industry had pressed for NRC to remove such adversary characteristics from the draft DBT. The industry considered these adversary characteristics prohibitively expensive to defend against or to be representative of an enemy of the United States, which is the responsibility of the government, rather than the industry, to defend against. When we asked about the changes to the staff's original recommendations, NRC officials told us the changes resulted from further analysis of the intelligence data and the reasonableness of required defensive measures rather than the industry objections. Nevertheless, in our view, the process by which NRC used the threat assessment staff to obtain stakeholder feedback created the appearance that changes were made based on what industry considered reasonable and feasible to defend against rather than an assessment of the terrorist threat, especially given the high degree of judgment involved in assessing threat information. NRC officials said they have altered their process in order to better separate the analysis of threat information from interaction with stakeholders.

- Second, in deciding on the revised DBT, the NRC commissioners largely supported the staff's recommendations but also made some significant

changes to those recommendations. These changes reflected the commissioners' policy judgments on what is reasonable for a private security force to defend against. For example, the commissioners decided against including two weapons that the threat assessment staff had concluded could plausibly be used against a U.S. nuclear power plant. Consideration of issues such as what is reasonable for a private security force to defend against can certainly be considered by the commissioners in approving changes to the DBT. However, the commissioners did not identify explicit criteria for what is and is not reasonable for a private security force to defend against, such as the cost of defending against particular adversary characteristics. NRC officials said detailed criteria on what is reasonable for a private security force would reduce the commissioners' discretion in approving changes to the DBT. Nevertheless, we believe the absence of reviewable criteria reduced the transparency of the commissioners' decisions to make changes to the threat assessment staff's recommendations. The absence of criteria also potentially reduced the rigor of the decision-making process.

Licensees of nuclear power plants have made substantial changes to their security in response to the September 11, 2001, attacks and the 2003 revisions to the DBT. At the sites we visited, these actions included, for example, adding security barriers and detection equipment, implementing new protective strategies, enhancing access control, and hiring additional security officers. According to NRC, other sites implemented similar security enhancements to defend against the 2003 DBT. The sites' efforts have been substantial and, in some cases, have gone beyond what was required. For example, one site added electronic intrusion detection equipment to its outer perimeter, which was not required. Despite these considerable efforts, it is too early to conclude that all sites are capable of defending against the DBT because, as of November 1, 2005, NRC had conducted force-on-force inspections at 20 of the 65 sites. According to NRC, sites have generally performed well during force-on-force inspections, and the results of baseline inspections show that sites have generally complied with their security plans. However, a number of sites have experienced problems and have not always met security requirements. For example, a baseline inspection at one site found that detection equipment malfunctioned and had to be fixed. Similarly, we observed a force-on-force inspection at another site in which the licensee's performance at the time was at best questionable in its ability to defend the site against the DBT. According to NRC, it will complete the first cycle of

triennial force-on-force inspections at all nuclear power plant sites on schedule, by 2007.

NRC has made a number of improvements to its force-on-force inspection program, several of which address recommendations we made in our September 2003 report on the agency's oversight of security at commercial nuclear power plants. For example, NRC is implementing a schedule to conduct the inspections more frequently at each site—every 3 years rather than every 8 years—and has instituted measures to make the inspections more realistic, such as using laser equipment to better simulate the weapons that attackers and security officers would likely employ during an actual attack on a nuclear power plant. These improvements are important because, as we noted from our observation of three force-on-force inspections and our review of NRC reports on others, the inspections have the ability to detect weaknesses in sites' protective strategies, which can then be corrected. Nevertheless, in observing three inspections and discussing the program with NRC officials, we noted issues in the force-on-force program that warrant continued NRC attention. For example, a lapse in protection of information about the planned scenario for a mock attack that we observed may have given the plant's security officers knowledge that allowed them to perform better than they otherwise would have. According to NRC officials, NRC inspectors have been instructed to be vigilant regarding any indications that a site's security force may have received advance knowledge of an attack scenario.

We are recommending that NRC improve its DBT development process in two ways. First, we recommend that NRC assign responsibility for obtaining feedback from the nuclear industry and other stakeholders on proposed changes to the DBT to an office within NRC other than the Threat Assessment Section, thereby insulating the staff and mitigating the appearance of industry influence on the threat assessment itself. Second, we recommend that NRC develop explicit criteria to guide the commissioners in their deliberations to approve changes to the DBT. These criteria should include setting out the specific factors and how they will be weighed in deciding what is unreasonable for a private security force to defend against. In addition, we are recommending that NRC continue to evaluate and implement measures to further strengthen its force-on-force inspection program. In commenting on a draft of this report, NRC provided additional clarifying comments pertaining to the process NRC used to revise the DBT for nuclear power plants, and we revised the report accordingly. NRC's written comments are included in appendix III.

Background

NRC is an independent agency established by the Energy Reorganization Act of 1974 to regulate the civilian use of nuclear materials. NRC is headed by a five-member commission, with one commission member designated by the President to serve as chairman and official spokesperson. The commission as a whole formulates policies and regulations governing nuclear reactor and materials safety and security, issues orders to licensees, and adjudicates legal matters brought before it. Security for commercial nuclear power plants is addressed by NRC's Office of Nuclear Security and Incident Response. This office develops policy on security at nuclear facilities and is the agency's security interface with DHS, the intelligence and law enforcement communities, DOE, and other agencies. Within this office, the Threat Assessment Section assesses security threats involving NRC-licensed activities and develops recommendations regarding the DBT for the commission's consideration.

The DBT for radiological sabotage applied to nuclear power plants identifies the terrorist capabilities (or "adversary characteristics") that sites are required to defend against. The adversary characteristics generally describe the components of a ground assault and include the number of attackers; the size of a vehicle bomb; and the weapons, equipment, and tactics that could be used in an attack. Other threats in the DBT include a waterborne assault and the threat of an insider. The DBT does not include the threat of an airborne attack. However, according to NRC officials, NRC regulations do require nuclear power plants to implement readily available measures to mitigate against the potential consequences of such an attack. In its publicly available regulations governing the licensing of nuclear power plants, NRC has issued a general description of the DBT—for example, requiring sites to defend against an attack by several well-trained and dedicated individuals armed with hand-carried weapons and equipment and assisted by a knowledgeable insider who participates in a passive or active role.[9] In April 2003, NRC issued orders to nuclear power plant licensees containing a more detailed description of the revised DBT, which NRC considers safeguards information.

NRC requires nuclear power plants to have and implement a security plan that describes their strategy for defending against an attack having the characteristics of the DBT. Nuclear power plant sites are responsible for installing barriers and intrusion detection equipment, hiring security

[9] 10 C.F.R. § 73.1.

officers, and implementing other measures in accordance with their security plans. NRC then inspects the sites' compliance with the plans and ability to defend against the DBT. After revising the DBT, NRC required sites to submit new plans by April 29, 2004, for NRC's review and approval and to implement the security described in their new plans by October 29, 2004. The plans contain information about the sites, including

- a description of sites' physical layout, such as barriers and buildings, and a description of any environmental features important to the effective coordination of response operations;
- the minimum number of security officers defending the vital areas (the areas containing equipment needed to ensure the safe shutdown of the reactor and protection of spent fuel pools); and
- a description of the protective strategy that sites will enact in response to an attack or threat defined in the DBT, such as an external land-based assault, a vehicle bomb, a waterborne assault, or an insider threat.

NRC's performance-based means for testing the effectiveness of nuclear power plant security programs is through force-on-force inspections. These inspections, which consist of 350 hours of on-site inspection activity, are intended to demonstrate how well a nuclear power plant might defend against a real-life threat. In a force-on-force inspection, a professional team of adversaries attempts to reach specific "target sets" within a nuclear power plant that would allow them to commit radiological sabotage. These target sets represent the minimum pieces of equipment or infrastructure an attacker would need to destroy or disable to commit radiological sabotage resulting in an elevated release of radioactive material to the environment. Force-on-force exercises do not directly test the response of outside agencies, such as local law enforcement. However, sites simulate actions they would take to notify local law enforcement and other outside agencies. In addition, according to NRC officials, sites routinely conduct liaison activity with local law enforcement and emergency response agencies.

While the adversary characteristics terrorists might use in an actual attack are uncertain, the DBT provides parameters for the conduct of force-on-force inspections. For example, the mock adversary force is constrained to using the specific number of attackers, amount of explosives, and weapons and tactics included in the DBT. According to NRC officials, the commission recently approved an option to conduct force-on-force

inspections using adversary characteristics that go beyond those in the DBT. This option would be available on a voluntary basis to nuclear power plant licensees that are clearly successful in defending against the first two mock attacks of the force-on-force inspection, which typically includes three mock exercises over 3 days.

NRC also conducts baseline inspections at nuclear power plants to determine that licensees have established measures to deter, detect, and protect against the DBT for radiological sabotage. Security inspectors in NRC's four regional offices conduct the inspections. NRC's policy is to conduct a baseline inspection at each site every year, with the complete range of baseline inspection activities conducted over a 3-year cycle. One element of a baseline inspection is evaluating the site's protective strategy—for example, by conducting tabletop drills (simulated attacks using a model of the site) to gain a better understanding of the strategy. Inspectors also examine areas such as officer training, fitness for duty, positioning and operational readiness of multiple physical and technical security components, and the controls the licensee has in place to ensure that unauthorized personnel do not gain access to the protected area. According to NRC officials, agency inspectors spend a total of 136 hours annually at a site for a baseline inspection, and the 3-year baseline inspection cycle involves more than 400 hours of inspection activity.

For both force-on-force and baseline inspections, licensees are responsible for immediately correcting or compensating for any deficiency in which NRC concludes that security is not in accordance with the approved security plans or other security orders. According to its inspection manual, NRC has 45 days to send a licensee a report on the results of an inspection, including any findings and the licensee's corrective actions.

DHS has overall responsibility among federal agencies for assessing the vulnerability of the nation's critical infrastructure to terrorist attacks and coordinating efforts to enhance security. Nuclear power plants represent one sector of the critical infrastructure. Other sectors include such things as agriculture, chemical facilities, and transportation systems. In 2005, DHS began a series of visits to nuclear power plant sites to conduct comprehensive security reviews in order to assess the risks and consequences of various types of events and to provide better information on the most effective allocation of federal resources to improve security at

critical infrastructure sites.[10] DHS conducts the comprehensive reviews with relevant agencies such as the FBI and, in the case of nuclear power plants, NRC. According to DHS, the comprehensive reviews for nuclear power plants focus primarily on the security of the sites "outside the fence"—the aspects of security outside the responsibility and control of the nuclear power plant licensees. DHS relies on NRC to regulate the security of nuclear power plants "inside the fence." DHS officials told us that the nuclear power sector is one of the few critical infrastructure sectors in which the federal government has the authority to regulate the security of sites. According to DHS, as of December 2005, the agency had completed 14 comprehensive reviews at nuclear power plant sites.

NRC's Process for Revising Its DBT for Nuclear Power Plants Was Generally Logical and Well Defined, but Some Changes Were Not Clearly Linked to an Analysis of the Terrorist Threat

The process that NRC used to revise its DBT for nuclear power plants was generally logical and well defined. In particular, the process included an analysis of intelligence and law enforcement information on terrorist capabilities and consultation with DOE, which also has a DBT for its facilities that are potential targets for terrorists seeking to cause radiological sabotage. Using this process, NRC produced a revised DBT that usually corresponded to the original recommendations of NRC's threat assessment staff. However, certain elements of the revised DBT, such as the weapons that attackers could use against a plant, do not correspond to the staff's original recommendations for two reasons. First, the NRC threat assessment staff charged with reviewing intelligence information made changes to its recommendations after receiving feedback from stakeholders, including the nuclear industry. Given the high degree of judgment involved in assessing threat information, the process NRC used to obtain stakeholder feedback created the appearance that changes were made based on industry views rather than an assessment of the terrorist threat. Second, the NRC commissioners made changes to the staff's recommendations on the basis of what is reasonable for a private security force to defend against but did not identify explicit criteria for such policy judgments.

[10]DHS conducts these activities in accordance with a Homeland Security Presidential Directive issued by the President on December 17, 2003 (HSPD-7). For further information on DHS efforts to assess risks to critical infrastructure, see GAO, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, GAO-06-91 (Washington, D.C.: Dec. 15, 2005).

NRC Has Been Assessing Threats to Nuclear Power Plants for Many Years

NRC made its 2003 revisions to the DBT for nuclear power plants as part of a process that the agency has used since first issuing the DBT in the late 1970s. In this process, NRC staff trained in threat assessment use reports and secure databases provided by the intelligence community to monitor information on terrorist activities worldwide. The staff analyze this information both to identify specific references to nuclear power plants and to determine the capabilities that terrorists have acquired and how they might use those capabilities to attack nuclear power plants in the United States. The staff normally summarize applicable intelligence information and any recommendations for changes to the DBT in semiannual reports to the NRC commissioners on the threat environment.[11] In addition, the threat assessment staff promptly report changes in the threat to the commissioners and coordinate with the intelligence agencies to help ensure that the staff are aware of all pertinent intelligence information.

In 1999, the NRC staff began developing a set of criteria—the adversary characteristics screening process—to decide whether to recommend particular adversary characteristics for inclusion in the DBT and to enhance the predictability and consistency of their recommendations. According to the NRC staff, the adversary characteristics screening process, which they used to develop the April 2003 revised DBT, begins with a thorough review of intelligence reports and application of initial screening criteria to evaluate adversary characteristics. The staff use the initial screening criteria to exclude from further consideration certain adversary characteristics, such as those that are already in the DBT or those that would more likely be used by a foreign military than by a terrorist group.

For adversary characteristics that pass the initial round of screening, the threat assessment staff apply additional screening factors. Examples of such factors include the following:

- *The type of terrorist group that demonstrated the characteristic.* For example, the staff consider whether an adversary characteristic has been demonstrated by transnational or terrorist groups operating in the

[11]These semiannual reports were suspended after the terrorist attacks of September 11, 2001, while the threat assessment staff worked to update the DBT. The threat assessment staff resumed its semiannual reports to the commissioners in October 2003.

United States, or by terrorist groups that operate only in foreign countries.

- *The location and level of social stability where the characteristic was demonstrated.* For example, the staff consider whether the adversary characteristic has been demonstrated in North America and other countries with a high level of social stability or in countries with an active insurgency or civil war. NRC considers that terrorists planning to attack a nuclear power plant in the United States would face greater operational security and logistical challenges than terrorists operating in countries where there is an internal insurgency.

- *The frequency with which the characteristic has been demonstrated and its availability.* For example, the staff consider the availability of an adversary characteristic on the open or the black market.

- *The type of target the characteristic has been used against, the tactical use of the characteristic, and the motive behind its use.* For example, the staff consider whether the adversary characteristic has been used against a target with a level of security similar to that at nuclear power plants or against targets with less security, such as the October 2002 attack on a Moscow theater by Chechen rebels.

Depending on the results of this analysis, the threat assessment staff may interact with intelligence and other agencies to obtain additional information and insights about the adversary characteristics. Finally, on the basis of their analysis and interaction with other agencies, the staff decide whether to recommend that the commission include the adversary characteristics in the DBT for nuclear power plants. NRC's Office of Nuclear Security and Incident Response, which includes the Threat Assessment Section, reviews and endorses the threat assessment staff's analysis and recommendations.

Since issuing the revised DBT in April 2003, NRC has continued to use the adversary characteristics screening process to consider additional changes—for example, to consider new intelligence information on weapons not included in the revised DBT. In addition, the Energy Policy Act of 2005 directed NRC to undertake a rulemaking to revise the DBT for nuclear power plants.[12] While the detailed description of the April 2003

[12]Pub. L. No. 109-58, § 651(a)(1), (2005).

DBT is safeguards information and thus has not been made available to the public, the rulemaking, which is under way, presents the DBT in less detail so that it can be made available to the public and includes a notice and opportunity for public comment. The act directed NRC to consider the events of September 11, 2001; the potential for an attack on facilities by multiple, coordinated teams of a large number of individuals; the potential for suicide attacks; and other factors. The April 2003 DBT already includes some (but not all) of the adversary characteristics listed in the Energy Policy Act, such as attackers who are willing to commit suicide, the potential for a waterborne assault, and the use of explosive devices. NRC officials told us that, as part of the current rulemaking, they would consider all of the factors listed in the Energy Policy Act, including those not currently in the DBT.

NRC Threat Assessment Staff Had to Decide on the Applicability of Intelligence Information to Nuclear Power Plants

Terrorist attacks have generally occurred outside the United States, and intelligence information specific to nuclear power plants is very limited. As a result, one of the NRC threat assessment staff's major challenges has been to decide how to apply this limited information to nuclear power plants in the United States. For example, one of the key elements in the revised DBT, the number of attackers, is based on NRC's analysis of the group size of previous terrorist attacks worldwide. According to NRC threat assessment staff, the number of attackers in the revised DBT falls within the range of most known terrorist cells worldwide.[13] Furthermore, the threat assessment staff told us they considered but decided against an even larger number of attackers in the draft DBT because a larger cell would face an increased potential of detection before it could successfully carry out a terrorist attack in the United States. The staff also concluded that multiple cells along the lines of the September 11, 2001, attacks would not necessarily target a single nuclear power plant. Intelligence and law enforcement officials we spoke with did not have information contradicting NRC's interpretation regarding the number of attackers (or other parts of the NRC DBT) but did point to the uncertainty regarding the size of potential attacks and the relative lack of intelligence on the terrorist threat to nuclear power plants.

NRC staff recommendations regarding other adversary characteristics also reflected the staff's interpretation of intelligence information. For example,

[13]In this report, "terrorist cell" refers only to terrorists who participate in an attack, not those who support but do not participate in an attack.

the staff considered increasing the vehicle bomb in the revised DBT to a range of sizes and ultimately recommended a size that was based on an analysis of previous terrorist attacks using vehicle bombs.[14] One of the largest vehicle bombs ever detonated was used in the 1996 bombing of the U.S. military residence in Saudi Arabia, and the maximum size of a vehicle bomb used in the United States—the 1995 bombing of the federal building in Oklahoma City—consisted of the equivalent of 4,800 pounds of TNT. Additional examples of NRC's interpretation of intelligence information and recommendations for the revised DBT included the following:

- The threat assessment staff recommended a maximum weight of equipment and explosives per attacker. The staff based this weight on the experience and professional knowledge of NRC staff and contractors with security backgrounds. In developing these limits, the staff evaluated the degree to which attackers would rely on speed of movement rather than be encumbered by large amounts of equipment. They also considered that a relatively small amount of explosives could cause a large amount of damage.

- The NRC staff recommended including a waterborne assault with a bomb size based on available intelligence on waterborne terrorist bombs. In addition, according to NRC, watercraft found near nuclear power plants would generally be constrained in terms of payload. Furthermore, the bomb size recommended by the staff was considered sufficient to significantly damage a nuclear power plant's water intake structure. The staff considered that a larger bomb would add little to the potential damage to the intake structure.

- The NRC staff supported the inclusion of equipment that is readily available through commercial sources but recommended against weapons with limited use by terrorists.

- The staff recommended against including infiltration into a nuclear power plant by air because their review of terrorist attacks did not demonstrate significant use of such tactics against a fixed site.

[14]The amount of explosives in a vehicle bomb is expressed in TNT but may consist of an equivalent amount of another type of explosive material.

Table 1 summarizes, by adversary characteristic, the key changes to the DBT recommended by the NRC staff and the final changes approved by the NRC commissioners.

Table 1: Summary of Key Changes to the NRC DBT for Nuclear Power Plants

Adversary characteristic	NRC staff's recommended DBT	April 2003 revised DBT, as approved by NRC commissioners
Number of attackers	The staff recommended increasing the number of attackers to fall within the range of most known terrorist cells worldwide.	The commission supported the number of attackers recommended by the NRC staff.
Vehicle bomb	The staff recommended increasing the maximum size of a vehicle bomb based on an analysis of previous attacks using vehicle bombs. The staff considered a larger vehicle bomb size but decided against the larger size after obtaining comments from stakeholders, including the nuclear industry.	The commission supported the staff recommendation.
Weapons	The staff refined and expanded the list of weapons that could be used in an attack. The staff decided against recommending certain weapons after obtaining comments from stakeholders, including the nuclear industry.	The commission retained most weapons recommended by the staff but removed certain weapons the staff had recommended.
Inside assistance	Active or passive.	Active or passive. The commission added a provision that the likelihood of an active insider can be reduced by a human reliability program, which consists of policies and procedures, such as substance abuse testing, designed to help ensure the reliability of personnel.
Weight of equipment and explosives	Based on the degree to which attackers would rely on speed of movement rather than be encumbered by large amounts of equipment.	The commission reduced the weight recommended by the staff.

Source: GAO analysis of NRC information.

NRC Generally Established Requirements Less Rigorous Than DOE's DBT for Radiological Sabotage

According to the NRC staff's report on recommended changes to the DBT for nuclear power plants, NRC has a long-standing commitment to work closely with DOE in an effort to maintain comparable protection for comparable facilities. Thus, as part of the process for revising the DBT for nuclear power plants, NRC monitored and exchanged information with DOE, which also has a DBT for comparable facilities that process or store

radiological materials and are, therefore, potential targets for radiological sabotage.[15] However, while certain aspects of the two agencies' DBTs for radiological sabotage are similar, NRC generally established less rigorous requirements than DOE—for example, with regard to the types of equipment that could be used in an attack. Additional information regarding key adversary characteristics found in both agencies' DBTs includes the following:

- *Number of attackers*. Both DOE and NRC based the number of attackers on intelligence on the size of terrorist cells. According to DOE officials, it is challenging to find intelligence on terrorist activities that can be considered equivalent to a ground assault on a fixed facility such as a nuclear power plant or DOE site. However, DOE officials said they used similar intelligence as NRC to derive the number of attackers.

- *Vehicle bomb*. DOE and NRC officials provided us with similar analyses of intelligence information on previous terrorist attacks using vehicle bombs. In particular, DOE and NRC officials told us that most vehicle bombs used in terrorist attacks are smaller than the size vehicle bomb in NRC's revised DBT. DOE officials also said that site-specific characteristics affect the size of vehicle bomb that sites are capable of defending against.

- *Weapons*. The DOE DBT includes a number of weapons not included in the NRC DBT. Inclusion of such weapons in the NRC DBT for nuclear power plants would have required plants to take substantial additional security measures. Furthermore, DOE included other capabilities in its DBT that are not included in the NRC DBT. As discussed below, NRC staff considered some of the weapons in DOE's DBT for inclusion in the DBT for nuclear power plants but removed them while drafting the DBT.

[15]In response to the attacks of September 11, 2001, both NRC and DOE undertook reviews of their DBTs. DOE issued its DBT 1 month after NRC, in May 2003, and revised its DBT again in October 2004 and most recently in November 2005. While NRC required nuclear power plants to implement security enhancements in response to its April 2003 DBT by October 29, 2004, DOE is not requiring full compliance with its DBT for radiological sabotage until October 2006 in order to allow its sites adequate time to implement security measures. For further information on the DOE DBT, see GAO, *Nuclear Security: DOE's Office of the Under Secretary for Energy, Science and Environment Needs to Take Prompt, Coordinated Action to Meet the New Design Basis Threat*, GAO-05-611 (Washington, D.C.: July 15, 2005); and *Nuclear Security: DOE Needs to Resolve Significant Issues Before It Fully Meets the New Design Basis Threat*, GAO-04-623 (Washington, D.C.: Apr. 27, 2004).

DOE established an even more stringent DBT for its sites that store nuclear weapons (or material that could be used in a nuclear weapon). The security objective for these sites is to prevent the theft or detonation of a nuclear weapon. DOE decided on a more stringent DBT to protect nuclear weapons facilities than sites with the potential for radiological sabotage in accordance with its graded approach, which provides for a higher level of protection to sites with greater potential consequences to public health and safety in the event of a terrorist attack. According to DOE officials, the consequences of theft or detonation of a nuclear weapon would be "orders of magnitude" greater than radiological sabotage at a DOE site or nuclear power plant.

Consistent with DOE's graded approach, NRC officials told us they do not consider comparisons between the DOE DBT for nuclear weapons facilities and the NRC DBT for nuclear power plants valid. NRC considers that the potential consequences of the theft of material that could be used in a nuclear weapon could be much greater than radiological sabotage at a nuclear power plant. Furthermore, according to NRC officials, terrorists seeking to steal or detonate a nuclear weapon would require greater capabilities to accomplish their objectives than terrorists seeking to cause radiological sabotage. For example, theft of a nuclear weapon (or material that could be used in a weapon) would require terrorists to defeat a site's security systems when entering and leaving a site. In contrast, attackers willing to commit suicide in the process of causing the release of radiological material from a nuclear power plant would have to overcome security to enter a site and reach a target set but would not have to leave the site. Like DOE, NRC uses a graded approach to security, and, therefore, the NRC DBT for NRC-licensed facilities that store or process material that could be used in a nuclear weapon is more stringent than the NRC DBT for nuclear power plants.

NRC's Process for Obtaining Feedback on the Draft DBT Created the Appearance of Industry Influence on the Threat Assessment Staff's Analysis of Intelligence Information

NRC staff sent a draft DBT to stakeholders in January 2003, held a series of meetings with them to obtain their comments, and received written comments. In addition to nuclear power plant licensees and NEI, which represents the nuclear industry, these stakeholders included other federal agencies and government authorities in affected states. NRC specifically sought and received feedback from the nuclear industry on what is reasonable for a private security force to defend against and the cost of and time frame for implementing security measures to defend against specific

adversary characteristics.[16] During the same period that the threat assessment staff was receiving industry and other stakeholder feedback, they continued to analyze intelligence information and modify the draft DBT. In April 2003, NRC staff submitted their final draft DBT to the commissioners for their review and approval, together with a summary of stakeholder comments.

In its written comments on the January 2003 draft DBT, NEI objected to the size of the vehicle bomb, the inclusion of certain weapons, and the inclusion of an active violent insider. The NRC staff's draft DBT submitted to the commissioners reflected some (but not all) of NEI's objections. The reasons for NEI's objections to key adversary characteristics and changes to the NRC threat assessment staff's recommendations included the following:

- *Vehicle bomb*. NEI objected to the vehicle bomb in the draft DBT because of its assessment of (1) the low probability of a vehicle bomb of the size proposed by NRC, (2) the likelihood that federal authorities or local law enforcement would detect a large vehicle bomb, and (3) the inability of some sites to protect against the size of the vehicle bomb proposed by NRC because of insufficient land for installation of vehicle barrier systems at a necessary distance. Instead, NEI agreed that it would be reasonable to protect against a smaller vehicle bomb. In its recommendations to the commissioners, the NRC staff subsequently reduced the size of the vehicle bomb to the amount proposed by NEI. After review, the staff's reason for agreement with NEI was that vehicle bombs as large as that included in the draft provided to stakeholders had rarely been used in previous terrorist attacks and would not be reasonable or practical to include in the DBT.

- *Weapons*. NEI argued against the inclusion of a number of weapons. For example, NEI wrote that (1) one particular weapon recommended by the NRC staff would render the ballistic shielding used at nuclear power plants obsolete, and (2) another proposed weapon would initially cost $1 million to $7 million per site to defend against, with annual recurring costs of up to $2 million per site. Furthermore, NEI argued that these weapons (as well as the vehicle bomb size initially proposed by the NRC

[16]According to NRC, the agency routinely prepares regulatory analyses of costs and benefits when establishing regulations and implementation guidelines, including those that involve security.

staff) would be indicative of an enemy of the United States, which sites are not required to protect against under NRC regulations. In the final draft submitted to the NRC commissioners, the NRC staff removed a number of weapons NEI had objected to. The staff reasoned that the weapons had rarely been used in armed assaults, or had been used infrequently in terrorist assaults despite their wide availability and use by violent criminals in the United States.[17] NRC staff did not remove one particular weapon NEI had objected to, which, according to NRC's analysis, has been a staple in the terrorist arsenal since the 1970s and has been used extensively worldwide. (As discussed below, the NRC commissioners later voted to remove this particular weapon.)

- *Inside assistance.* NEI wrote that the nuclear power industry had taken a number of steps to reduce the likelihood of an active violent insider—for example, it tightened the process for granting employees unescorted access to nuclear power plants. Furthermore, NEI wrote that the industry had been unable to identify cost-effective solutions to defend against an active violent insider, and that costs would range from $2 million to $8 million per site for equipment and $5 million per site per year for additional personnel. Despite these objections, the NRC staff recommended the inclusion of an active violent insider in the final draft of the DBT. (The NRC commissioners later allowed nuclear power plants to reduce the likelihood of an active violent insider through a human reliability program.)

The chief of NRC's threat assessment staff told us that NRC did not make changes to the draft DBT based solely on industry views. Rather, according to NRC officials, the changes were made based on multiple internal analyses and discussions among the threat assessment staff and higher levels of review within NRC and its Office of Nuclear Security and Incident Response, which includes the Threat Assessment Section. Nevertheless, in our view, the process NRC used to obtain feedback from stakeholders, including the nuclear industry, created the opportunity for, and appearance of, industry influence on the threat assessment regarding the characteristics of an attack.

When we raised this issue with NRC officials, they told us that under normal circumstances the threat assessment process is initially undertaken

[17]The NRC staff did recommend some of these weapons for inclusion in the DBT for NRC-licensed facilities storing nuclear material that could be used to construct a nuclear weapon.

utilizing intelligence and law enforcement information, with other stakeholders subsequently having an opportunity to provide feedback—for example, regarding the cost of implementing security measures in response to proposed changes to the DBT. Furthermore, NRC threat assessment staff and other intelligence agency officials told us they support the separation of intelligence analysis from other responsibilities, such as obtaining stakeholder feedback on changes to the DBT, in order to insulate analysis of intelligence from other considerations. However, according to NRC, the agency made a deliberate decision as part of the process for revising the DBT in 2003 to have the threat assessment staff analyze intelligence information and obtain stakeholder feedback simultaneously, rather than sequentially, in order to accelerate the process in response to the increase in the terrorist threat. NRC officials said that in considering future changes to the DBT, NRC plans to ensure the initial separation of intelligence analysis from interaction with stakeholders.

The NRC Commission Made Key Policy Judgments about Changes to the DBT without Criteria on Threats That a Private Security Force Could Reasonably Defend Against

The NRC staff provided the commissioners with a number of documents to consider in making the final decision on changes to the DBT. These included, but were not limited to, two assessments in the fall of 2002 on the terrorist threat to nuclear power plants (one specifically on the potential use of vehicle bombs) and a final paper in April 2003 with the staff recommendations for revisions to the DBT. The April 2003 document also included a summary of comments on the draft DBT received from the nuclear industry and other federal and state agencies; a summary of NEI's estimates of the cost of and time frame for implementing security measures to address specific changes to the DBT; and an updated assessment of the terrorist threat to nuclear power plants. The NRC commissioners told us they also had direct contacts with intelligence agencies that provided them with information on the terrorist threat.

The commissioners made the final decision on changes to the DBT by majority vote.[18] While the commission largely supported the NRC staff's recommendations for changes to the DBT, it also made some significant changes that reflected policy judgments. Specifically, the commissioners considered whether any of the recommended changes to the DBT constituted characteristics representative of an enemy of the United States,

[18]Four commissioners were serving at the time the DBT was revised, with one seat vacant. According to commission procedures, any change to the prior DBT required a majority vote, with at least three commissioners supporting the change.

which sites are not required to protect against under NRC regulations. In approving the revised DBT, the commission stated that nuclear power plants' civilian security forces cannot reasonably be expected to defend against all threats, and that defense against certain threats (such as an airborne attack) is the primary responsibility of the federal government, in coordination with state and local law enforcement officials. In connection with this position, the commission directed NRC's Office of General Counsel to prepare a paper for commission approval articulating the factors to be considered in determining whether particular characteristics of an attack constitute an enemy of the United States. (Officials from NRC's Office of General Counsel told us they prepared a document with an analysis of this issue for the commission, but that the document was not a decision paper for approval by the commissioners.)

We recognize that consideration of issues such as what is reasonable for a private security force to defend against is an appropriate role of the commission in approving changes to the DBT. However, in approving the revised DBT, the commission did not identify explicit criteria for determining whether specific adversary characteristics constitute an enemy of the United States or criteria for what is reasonable for a private security force to defend against. For example, the commission did not define whether the criteria include the cost for nuclear power plants to defend against an adversary characteristic or the efforts of local, state, and federal agencies to address particular threats. The lack of such criteria can reduce the transparency of commission decisions to make changes to the threat assessment staff's recommendations. NRC officials said detailed criteria on what is reasonable for a private guard force would reduce the commissioners' discretion in approving changes to the DBT. Furthermore, in NRC's view, the basis for the commission's policy decisions and direction to the NRC staff regarding the DBT are sufficiently articulated in the commission's voting record, in which individual commissioners provided the rationale for their votes, and in the related staff requirements memorandum, which documented the commission's decisions.

As indicated in table 1, the significant changes the commission made to the NRC staff's recommendations included removal of certain weapons, a decrease in the maximum amount of weight carried by the attackers, and mitigation of an active insider through a human reliability program. In other cases, such as the size of the vehicle bomb, the commission supported the recommendations of the NRC staff. Based on our review of the commissioners' voting records, the commission's decisions on key aspects of the DBT included the following:

- *Vehicle bomb.* A majority of commissioners voted to increase the maximum vehicle bomb to the size recommended by the NRC staff. However, one commissioner supported a larger vehicle bomb that the NRC staff had included in a previous draft of the DBT. The commissioner recognized that some sites would not have sufficient property to install vehicle barrier systems far enough from the plants to protect against the larger vehicle bomb and suggested NRC could provide such sites with an exemption and require them to protect against a smaller vehicle bomb.

- *Weapons.* The commission decided to remove two weapons the NRC staff had recommended for inclusion in the revised DBT. As part of this decision, the commission directed the staff to conduct an in-depth analysis of the additional defensive capabilities, changes to sites' protective strategies, and costs associated with protecting against one of the weapons. Removal of weapons from the revised DBT was significant because of the strength of the NRC staff's intelligence analysis supporting their inclusion. For example, in the April 2003 report to the commissioners, the NRC staff reported that while one such weapon had not been used in the United States, it had been found in weapons caches in the United States. Similarly, the staff noted the use of the other weapon in captured terrorist training videos and its ready availability. The document summarizing the commission's changes to the proposed DBT did not provide a reason for excluding these weapons. However, in written comments on their votes, one commissioner identified these weapons as representative of an enemy of the United States; another commissioner agreed that threat data showed an increased possibility of the use of these weapons but stated that NRC staff needed to assess whether it would be reasonable for a private security force to defend against such weapons. One of the commissioners supported inclusion of these weapons in the DBT, as well as other weapons the staff had not recommended, but nevertheless told us there was more agreement than disagreement among the commissioners about what weapons should be included. The same commissioner told us he supported inclusion of one of the weapons because he considered the means for defending against it to be affordable.

- *Weight of equipment and explosives.* In voting to decrease the maximum weight of equipment, weapons, and explosives (such as grenades) per attacker in the final DBT, three of the commissioners indicated they supported decreasing the weight that an attacker could

be expected to carry. In their written comments, the three commissioners indicated that the staff's recommendation regarding carry weight would require further study—for example, to determine whether the greater amount of weight could reduce the capability of the attack force by reducing individual attackers' mobility.

- *Inside assistance.* The commission added language to the DBT stating that a human reliability program for monitoring employees at the sites could reduce the likelihood of an active insider. To qualify, the sites' human reliability program would have to include background checks, substance abuse testing, psychological evaluations, annual supervisory review, and periodic background reinvestigations. The commissioners told us they made this decision based, in part, on the long-standing assumption by NRC that a human reliability program reduces the likelihood of an active insider. The commissioners also told us that other factors, such as increased awareness about the potential for an attack in the communities where nuclear power plants are located, would reduce the likelihood of an active insider.

In addition to making changes to specific elements of the DBT for nuclear power plants, the commission provided overall policy direction on NRC's oversight of security of the sites. In particular, recognizing that an attack on a site could exceed the characteristics identified in the DBT, the commission directed the staff to continue coordinating with DHS and other federal and state authorities to help assure the security of nuclear power plants. For example, the commissioners told us that NRC works with the Federal Aviation Administration to address the threat of air strikes against a site. Similarly, NRC supports and participates in DHS comprehensive security reviews of nuclear power plant sites.

Other significant policy direction included the following:

- The commission affirmed the NRC staff's operating assumption that there may be no specific advance warning of an attack on a nuclear power plant but indicated that a general warning of a potential attack may be provided.

- The commission directed the staff to continue providing the commissioners with assessments of specific adversary characteristics, including those not in the revised DBT, and to provide additional recommendations as part of the semiannual review of threats to nuclear power plants. However, the commission also indicated its expectation

that there would be a period of "regulatory stability" (a period with no major changes to security regulations) in order to allow sites time to adjust to the changes already made to the DBT and other security requirements.

- The commission supported the clarification that sites are not required to "defeat" an attack, because such a requirement could require sites' security forces to employ offensive tactics beyond what is allowed under law for private security forces. Rather, the commission supported the requirement that sites protect against radiological sabotage by preventing the destruction or disablement of vital equipment.

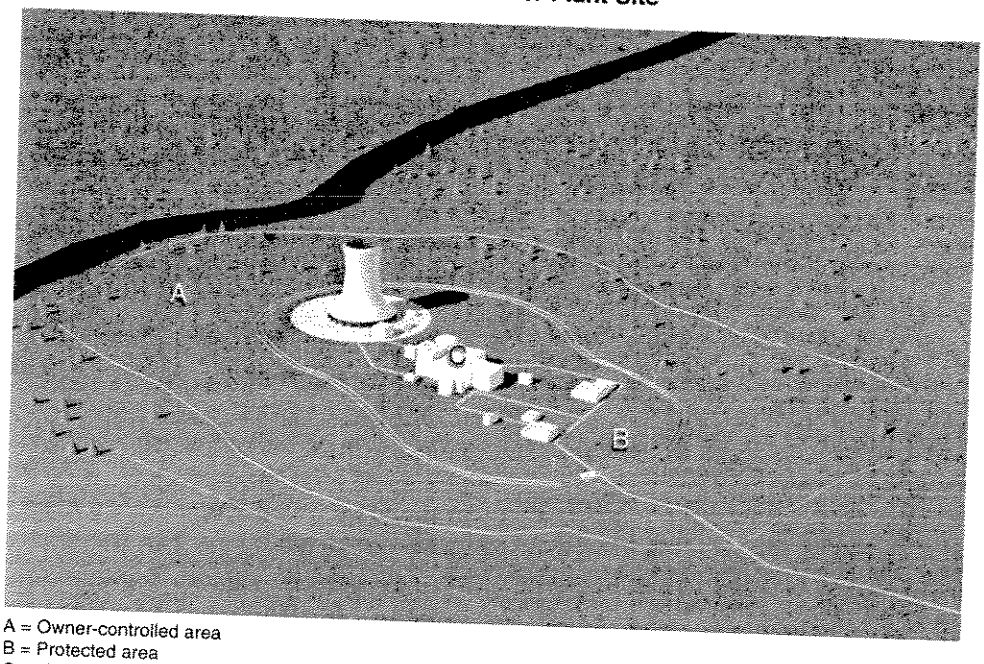
Nuclear Power Plants Made Substantial Changes to Their Security to Address the Revised DBT, but NRC Inspections Have Uncovered Problems

The four nuclear power plant sites we visited made substantial changes after the September 11, 2001, attacks and in response to the revised DBT, including measures to detect, delay, and respond to the increased number of attackers and to address the increased vehicle bomb size. According to NRC, other sites took comparable actions to defend against the revised DBT. Despite the industry's considerable efforts, the changes have not been completely without problems and licensees can continue to make improvements. For example, NRC baseline and force-on-force inspections have found that the security changes have not always met NRC's requirements.

Sites Addressed the Increase in the Number of Attackers by Implementing Security Enhancements Designed to Detect, Delay, and Respond to an Attack

The four sites we visited all implemented a "defense-in-depth" strategy, with multiple layers of security systems that attackers would have to defeat before reaching vital areas or equipment and destroying or disabling systems sufficient to cause an elevated release of radiation off site. The sites varied in how they implemented these measures, primarily depending on site-specific characteristics such as topography and on the degree to which they planned to interdict attackers within the owner-controlled area and far from the sites' vital area, as opposed to inside the protected area but before they could reach the vital equipment. (See fig. 1 for a diagram of the areas commonly found at nuclear power plants.) NRC officials told us that licensees have the freedom to design their protective strategies to accommodate site-specific conditions, so long as the strategies satisfy NRC requirements and prove successful in a force-on-force inspection.

Figure 1: Diagram of a Sample Nuclear Power Plant Site



A = Owner-controlled area
B = Protected area
C = Vital area

Source: Nuclear Energy Institute.

Note: The owner-controlled area refers the land and buildings within the site boundary, and the owner can limit or allow access to it for any reason. The protected area is within the owner-controlled area and requires a higher level of access control. The vital area contains the sites' vital equipment, the destruction of which could directly or indirectly endanger public health and safety through exposure to radiation.

The sites we visited implemented security measures corresponding to the three elements generally recognized as constituting an effective security system for defending fixed sites. These include early detection of an attack, sufficient delay for security officers to report to their defensive positions, and capability of the security force to respond to the attack:

- *Detection.* At all four sites, the owners installed additional cameras throughout different areas of the sites and instituted random patrols in the owner-controlled areas.[19] The owner-controlled areas generally

[19]By an order in February 2002, NRC required plants to enhance security in the owner-controlled areas.

contain undeveloped property and administrative buildings that would not be targets for terrorists seeking to commit radiological sabotage. Nevertheless, by upgrading security in this area, the sites increased the chance that they would detect attackers before the attackers would be able to approach or infiltrate the protected area, where they might be able to gain access to vital equipment. Patrols can be used to accommodate areas of the sites that are remote or where the view of cameras is obstructed, while cameras provide for a safer inspection of questionable activities than sending a security officer.

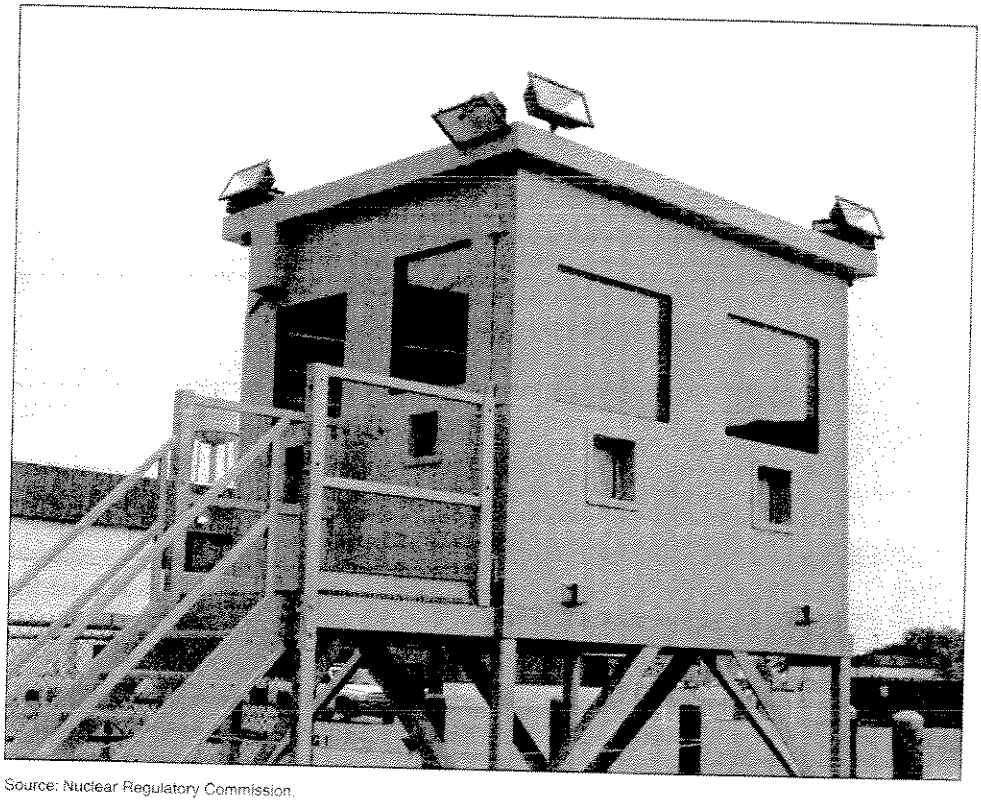
- *Delay.* The sites we visited installed a variety of devices designed to delay attackers and allow security officers more time to respond to their posts and fire upon attackers. The sites generally installed these delay devices throughout the protected areas so that attackers would have to defeat multiple security systems before reaching vital areas or equipment. For example, the sites installed fences outside the buildings housing the reactors and other vital equipment and blocked off entrances to make it more difficult for attackers to enter the buildings. Similarly, the sites installed a variety of delay devices within the reactor and other buildings, some of which are permanent and others that security officers would deploy in the event of an attack.

- *Response.* Each of the four sites we visited constructed bullet-resistant structures at various locations in the protected area or within buildings, increased the minimum number of security officers defending the sites at all times, and expanded the amount of training provided to them.[20] Security officers are stationed in the bullet-resistant structures or move to them during an attack, at which point they can fire at attackers through gun ports while not exposing themselves to the attackers' gunfire. (See fig. 2 for an example of a bullet-resistant structure.) Having more security officers on duty at any given time means that more individuals can respond to more locations in the event of an attack. It can also increase the sites' ability to detect attackers by allowing more security officers to observe the owner-controlled area and monitor video cameras. Security managers at each site told us they also made changes to their training—for example, to train officers to use new

[20]The sites had first increased the number of security officers in response to the September 11 attacks. Furthermore, an NRC security order, issued in February 2002, required sites to have a minimum number of security officers stationed in the protected area and immediately available to respond to an attack.

security equipment or to comply with NRC's training order, issued at the same time as the revised DBT. Moreover, each of the licensees told us they implemented measures to comply with NRC's requirements limiting the number of hours security officers can work to 72 hours during a 7-day period.[21] The majority of the security officers we interviewed told us that their training was adequate or had improved and that they generally did not experience fatigue on the job.

Figure 2: Example of a Bullet-Resistant Structure



Source: Nuclear Regulatory Commission.

[21]On April 29, 2003, the same day NRC issued the revised DBT, NRC issued a publicly available order establishing more stringent requirements for security force work-hour controls.

Security managers at the four sites considered the layouts of their sites and the paths that attackers might use to reach vital equipment in deciding where to deploy these enhancements. As a result, the sites employed different protective strategies that primarily varied by the degree to which they implemented an external strategy designed to interdict attackers within the owner-controlled area, but far from the sites' vital area, rather than an internal strategy designed to interdict attackers inside the protected area. For example, one site with a predominantly external strategy installed an intrusion detection system in the owner-controlled area. While NRC requires all sites to have an intrusion detection system at the perimeter of the protected area,[22] security managers at this site decided to install a second intrusion detection system so that security officers would be able to identify intruders as soon as they cross into the owner-controlled area. The site was able to install such a system because of the large amount of open, unobstructed space in the owner-controlled area. Similarly, the protective strategy at another site focused on the ability of security officers to deny attackers access to the vital area buildings. The site uses cameras and patrols to detect attackers in the owner-controlled area and deploys security officers in bullet-resistant structures. From the structures, located on the roof and attached to the walls of the vital area buildings, security officers could fire upon attackers before they could enter the buildings.

In contrast, security managers at the other two sites we visited described protective strategies that combined elements of an external strategy and an internal strategy. At both sites, the external strategy included bullet-resistant structures positioned so that security officers could fire on attackers attempting to enter vital area buildings. Other security officers are stationed inside the vital area buildings and would move to bullet-resistant structures within the buildings to interdict attackers who defeat the external security. At one of these sites in particular, security managers decided to implement a protective strategy that relied more heavily on interdicting attackers inside the protected area. The site uses elements of an external strategy, such as cameras and patrols for detecting attackers in the owner-controlled area, but in contrast to the sites described above, relies to a lesser extent on security officers to stop the attackers in the owner-controlled area. Instead, security managers told us they had implemented an internal protective strategy by identifying "choke

[22]This NRC requirement for an intrusion detection system at the protected area perimeter existed prior to the 2003 revisions to the DBT.

points"—locations inside the protected area attackers would need to pass before reaching their targets—and installing bullet-resistant structures at the choke points where officers would be waiting to interdict the attackers. Security managers at the site also told us one of the reasons for implementing a more internal strategy was their desire to maintain radiation doses to security officers as low as is reasonably achievable. In particular, the internal strategy allowed the site to not install bullet-resistant structures on one side of the site, where security officers who would be stationed in the structures could receive elevated radiation doses.

In addition to the security enhancements we observed, security managers at each site described changes they plan to make as they continue to improve their protective strategies, such as adding fencing to block a path attackers might use to enter the protected area and a device at the entrance to the site that can detect explosives. Security managers at three of the sites we visited also told us the number of security officers on duty at any one shift exceeded the minimum number of security officers that NRC requires be dedicated to responding to attacks.[23] (The fourth site maintained the minimum number of armed dedicated security officers.) According to NRC's analysis, sites typically exceeded the minimum number of responders required by NRC.

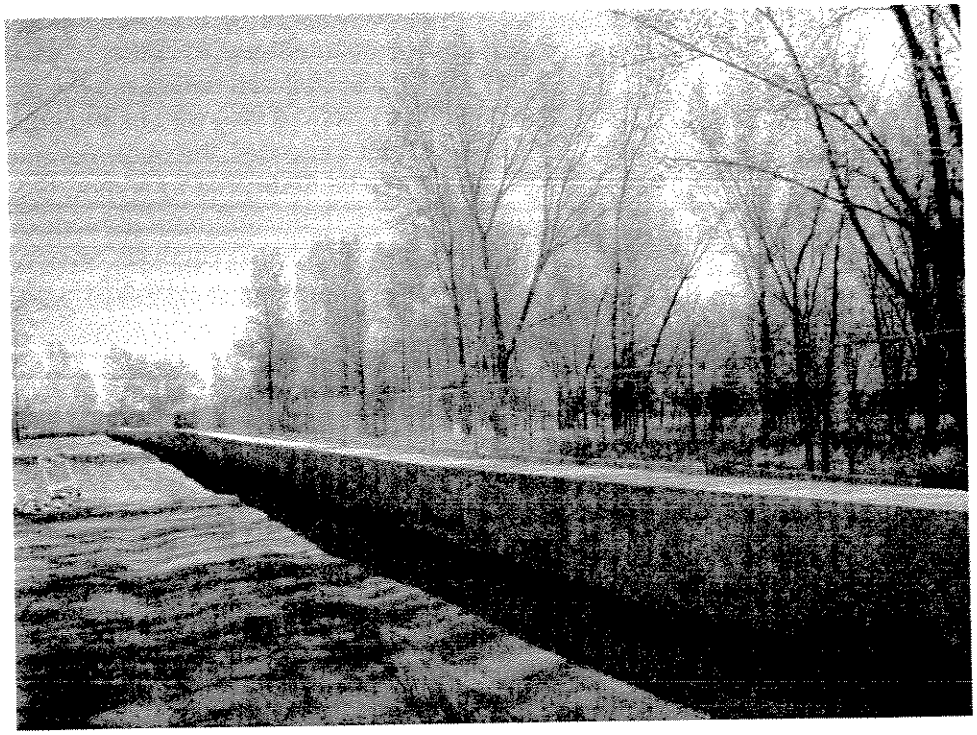
Sites Addressed the Increase in the Size of a Vehicle Bomb by Designing Comprehensive Systems of Sturdy Barriers

To protect against the increase in the vehicle bomb size, the licensees at the sites we visited designed comprehensive systems consisting of sturdy barriers to prevent a potential vehicle bomb from approaching the sites and to channel vehicles to entrances where security officers could search them for explosives and other prohibited items. Prior to increasing the maximum size vehicle bomb sites must defend against, NRC required the sites to have a vehicle barrier system encircling the reactors and other vital equipment and set at a distance far enough from the plants to prevent a smaller vehicle bomb from damaging vital equipment and releasing radiation. After NRC increased the maximum size of the vehicle bomb in the revised DBT, plants installed a second vehicle barrier system at an even greater distance from the vital equipment, while also keeping the original vehicle barrier systems as a second layer of defense.

[23]These numbers do not include additional security officers at each site who are responsible for security functions such as conducting vehicle searches and manning the central and secondary alarm stations.

At the sites we visited, the new vehicle barrier systems consisted of rows of large steel-reinforced concrete blocks, or (at one plant) large boulders weighing up to 7 tons in combination with piles of smaller rocks. (See fig. 3 for an illustration of a vehicle barrier system.) The vehicle barrier systems either completely encircled the plants (except for entrances manned by armed security officers) or formed a continuous barrier in combination with natural or manmade terrain features, such as bodies of water or trenches, that would prevent a vehicle from approaching the sites.

Figure 3: Example of a Vehicle Barrier System



Source: GAO.

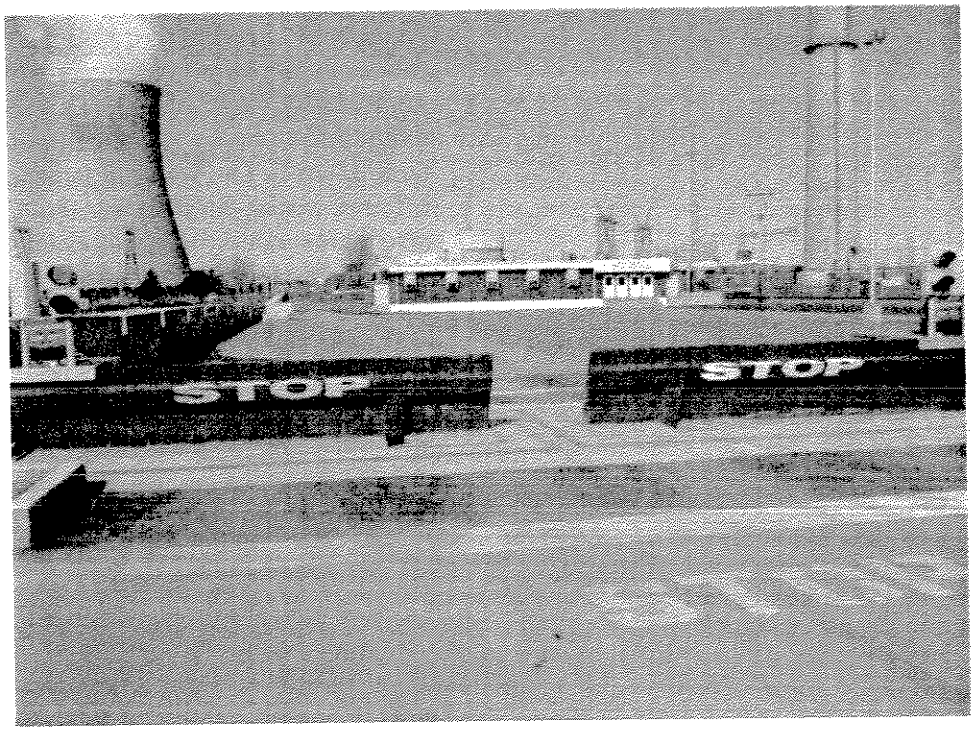
Licensees at the four sites adapted their vehicle barrier systems to the unique conditions at each site. The vehicle barrier systems also shared many features in common and generally consisted of a combination of the following basic elements:

- *Vehicle searches.* Generally, the security managers told us they implemented procedures to search vehicles at the entry point to the outer vehicle barrier systems. (NRC requires sites to search all vehicles capable of carrying more than a certain amount of TNT and to search a random sample of vehicles capable of carrying a smaller amount of explosives). Examples of search procedures included visual examination of the compartments of vehicles and use of detection equipment to test for explosives. Security managers told us security officers would conduct a second search of all vehicles, regardless of size, at a second checkpoint where vehicles pass through the inner vehicle barrier system. During this search, security officers would look for weapons and other prohibited equipment in addition to any explosives.

- *"Overwatches."* The sites stationed security officers in bullet-resistant structures, or "overwatches," from which the officers could observe the vehicle searches and provide backup support in case of an attack. Like the other bullet-resistant structures installed by the sites, these structures included gun ports for firing at attackers.

- *"Active" vehicle barrier systems.* These systems were installed in the roadways leading into the plants and were designed to block unauthorized vehicles from entering the site. They consisted either of steel plates that could be raised or lowered or rolling gates. (See fig. 4 for an example of an active vehicle barrier system.) Security officers in multiple locations, such as alarm stations and overwatches, could activate the systems if security officers manning the vehicle entrances, who are more vulnerable to attack, were unable to do so. At two of the plants, the barriers were always in the closed position and required two security officers at separate locations to open them. At the other two plants, the barriers were generally in the open position but could be closed by a single security officer to prevent unauthorized entry.

Figure 4: Example of an Active Vehicle Barrier System



Source: GAO.

In some cases, the new vehicle barrier systems at the sites we visited appeared to exceed the requirements necessary to protect against the revised DBT. For example, security managers at one site told us that the vehicle barrier system was wider than necessary in order to protect against the vehicle bomb. Furthermore, in at least some areas of the sites, the new vehicle barrier systems were farther from the reactors and other vital equipment than necessary to protect the sites against the size of vehicle bomb in the revised DBT. In particular, security managers at the site with a more external protective strategy decided to take advantage of the large amount of open, unobstructed property surrounding the site to create a large zone between the vehicle barrier system and the site buildings. Although we generally toured the complete perimeter of the vehicle barrier systems at the four sites, we did not calculate how far the barrier systems were installed from the vital equipment, test the equipment performance, or determine how well security officers conducted vehicle searches. Like

other aspects of security at the plants, these factors would affect how well the vehicle barrier systems would work in the event of a terrorist attack.

In addition, the sites implemented other related measures, such as winding lanes designed to cause vehicles to slow down as they approach entrances; emergency exits to facilitate evacuation of employees from the plant; devices to block unauthorized trains from reaching the plant; parking lots outside the vehicle barrier system for use during an outage to limit the number of additional vehicles entering the vehicle barrier systems and requiring searches; and, at one site, receiving deliveries at an off-site warehouse to limit the number of trucks entering the site.

Sites Have Generally Complied with NRC Security Requirements and Performed Well in Force-on-Force Inspections, but Problems Remain

As of November 1, 2005, NRC had completed force-on-force inspections—testing sites' ability to defend against the revised DBT—at 20 sites. NRC officials told us, and our review of baseline and force-on-force inspection reports indicated, that plants have generally complied with their security plans and other NRC security requirements and have generally performed well during force-on-force inspections.[24] However, we also noted from the reports, as well as from our own observations, that sites have encountered a range of problems in meeting NRC security requirements, including a force-on-force inspection in which the site had problems demonstrating it could defend against the revised DBT. (According to NRC officials, inspectors do not leave the site at which a problem is identified until it is corrected or until sufficient compensatory measures are put in place.) Twelve of the 18 baseline inspection reports and 4 of the 9 force-on-force inspection reports we reviewed identified problems or items needing correction. These findings, such as failures in the intrusion detection system at one site and not including certain elements of training at several sites, demonstrate that NRC's baseline and force-on-force inspections are important to identifying problems that need correction. (See app. II for a discussion of the findings in the force-on-force and baseline inspection reports we reviewed.)

[24]NRC officials told us that 11 sites required extensions to the deadline for implementing their new security plans but have since implemented all of the security measures described in the plans in accordance with NRC-approved schedules. A common reason for the extensions was the scarcity of bullet-resistant steel, which was in high demand in Iraq. This was the case at one site we visited. Another site we visited required an extension due, in part, to a limited supply of cement for the vehicle barrier system.

During a force-on-force inspection at one site, we observed that although the security measures appeared impressive, the site's ability to defend against the DBT was at best questionable. The site's security measures were similar to those we observed at other sites, such as an intrusion detection system equipped with cameras for assessing alarms, bullet-resistant structures both in the protected and vital areas, and a vehicle barrier system consisting of large concrete blocks and large boulders. However, some or all of the attackers were able to enter the protected area in each of the three exercise scenarios. Furthermore, attackers made it to the targets in two of the scenarios, although the outcomes of the two scenarios were called into question by uncertainties regarding whether the attackers had actually been neutralized before reaching the targets. NRC, in turn, raised concerns about the site's lack of "defense in depth" and concluded that it could not validate the licensee's protective strategy in the two scenarios. NRC noted that security officers' ability to interdict attackers was impacted due to problems in the site's detection and assessment, and that, in two of the scenarios, security officers left the external bullet-resistant structures to which they were assigned and transitioned to internal positions once they could account for the number of attackers in the revised DBT. This meant that the security officers left positions that covered a "breach" the attackers had made in the protected area perimeter. As a result of the inspection, NRC required the licensee to install additional security equipment immediately after the inspection, NRC inspectors remained on site until the equipment was put in place, and NRC decided to conduct another force-on-force inspection at the site.

At the follow-up force-on-force inspection at the same site, which we also observed, the licensee told us it had spent an additional $37 million to improve security in the 6 months following the first inspection. Some of these changes were clearly visible, such as elevating the bullet-resistant structures that had been on the ground to give officers greater visibility and firing opportunities, razing several buildings to reduce opportunities for attacker concealment, and increasing the distance between the vehicle barrier system and the protected area in a part of the site. The licensee also told us about other changes directly related to the internal aspect of the protective strategy, including positioning more security officers within the vital area, installing additional cameras to increase security officers' ability to detect attackers, and creating new bullet-resistant structures that provided additional protected positions for firing upon the attackers. From the second exercise, NRC officials concluded that they could evaluate the protective strategy and that the site had adequately defended against a DBT-style attack.

In addition to our observations of security during force-on-force inspections, GAO security experts who accompanied us to the four other sites we visited suggested a number of opportunities to improve security at the sites. While our experts did not find a lack of compliance with NRC regulations or an inability to defend the sites against the adversary characteristics in the revised DBT, the suggestions support our assessment that security at nuclear power plants is an ongoing process of identifying and implementing potential improvements. For example, at one site, we observed a bullet-resistant enclosure in which curtains—installed to reduce glare from the sun—obstructed the view through windows, and video equipment associated with surveillance cameras blocked access to several gun ports. We suggested that the site consider replacing the curtains with tinted glass and providing the security officer in the bullet-resistant enclosure with better access to the gun ports. At another site, we suggested that the addition of a bullet-resistant structure on one side of the site would provide the site's security force with greater opportunity to interdict attackers entering on that side of the site.

NRC Has Significantly Improved the Force-on-Force Inspection Program, but Challenges Remain

NRC has made a number of improvements to the force-on-force inspection program, several of which address recommendations we made in our September 2003 report on NRC's oversight of security at commercial nuclear power plants. We had made our recommendations when NRC was restructuring the force-on-force program to provide a more rigorous test of security at the sites in accordance with the DBT, which was also under revision.[25] For example, we had recommended that NRC strengthen the force-on-force inspections by (1) conducting the inspections more frequently at each site, (2) using laser equipment to better simulate attackers' and security officers' weapons, and (3) requiring the inspections to make use of the full terrorist capabilities stated in the DBT, including the use of an adversary force trained in terrorist tactics.

NRC has taken a number of actions as part of its restructuring of the force-on-force program that satisfy the recommendations we made to strengthen the program. For example, NRC has begun conducting the exercises more frequently at each site and is using laser equipment to simulate weapons. Furthermore, the attackers in the force-on-force exercise scenarios we

[25]The current force-on-force inspection program has been in place since November 2004. For further information on NRC's efforts and our recommendations, see GAO-04-1064T and GAO-03-752.

observed used many of the adversary characteristics of the revised DBT, including the number of attackers in the revised DBT, a vehicle bomb, a passive insider, and explosives. In addition, NRC officials told us that the adversaries were trained in military tactics. Nevertheless, in observing three force-on-force inspections and discussing the program with NRC officials, we noted the following issues that continue to warrant NRC's attention:

- *Problems with laser equipment.* At the three force-on-force inspections we observed, the sites used laser equipment to simulate firing live weapons. In general, the equipment appeared to help make the inspections a realistic test of security at the sites. For example, laser equipment provides a much more reliable account of shots fired in comparison with the equipment NRC and the sites had been using, which relied on the judgment of individual participants to determine shooting accuracy. However, problems in using the equipment contributed to NRC's limited ability to evaluate security at one of the sites. In part because of problems with the laser equipment, NRC decided to conduct a second force-on-force inspection at this site. The second inspection made better use of the laser equipment, which proved to be a valuable tool in determining that several security officers engaged attackers unsuccessfully by firing at the attackers while they were too far away. NRC raised this issue to the licensee in the context of improving training so that security officers would not waste ammunition on targets that are beyond the range of their weapons.

- *Inspection schedules.* The way in which NRC schedules force-on-force exercises may create artificialities that enable sites to perform better than they otherwise would. NRC officials said they notify sites of the date of their force-on-force inspection only 8 to 12 weeks in advance. Nevertheless, NRC may be able to further reduce the artificiality of the inspection schedules and thereby enhance its ability to test security at the sites. For example, in each of the exercises we observed, NRC followed the same schedule for conducting nighttime and daytime attacks. Furthermore, the adversary force typically initiated the attack soon after the opening of the exercise "window" (the agreed-upon time for the exercise to begin). Consequently, the sites' security forces might have been able to anticipate the approximate time that the attack would begin, and industry observers from other sites might have more information than necessary prior to inspections at their own sites about NRC's standard practices for conducting the inspections. NRC officials told us that, while the attacks began soon after the opening of the

exercise window in the exercises we observed, the attackers do sometimes wait longer in order to increase the level of uncertainty among the site's security force and thereby create a more realistic scenario.

- *Testing of sites' internal security strategies.* Given the amount of resources invested in preparing for and implementing a force-on-force inspection, we believe inspections should test the full extent of sites' "defense-in-depth" strategies, including both the external and internal elements of the strategies. However, the force-on-force exercises end when a site's security force successfully stops an attack. Consequently, if the security force stops an attack before the attackers enter the vital area, NRC would not have an opportunity to observe how the security force would perform in the event that the attackers successfully defeat the site's external security strategy. In a number of the force-on-force exercises we observed, the security force did, in fact, stop the attackers early in the scenario. According to NEI officials, force-on-force inspections would be more valuable if NRC allowed the adversaries to challenge each layer of defense until reaching their targets, or being defeated at the last possible point of defense. NRC officials also told us such an approach is worth considering but that NRC would have to first determine how to implement it.

- *Operational security.* At two of the force-on-force inspections we observed, we noted areas in which "operational security"—the protection of information about the planned scenarios for the mock attacks—could be improved. For example, during a safety "walk down"—a physical site check conducted prior to every exercise scenario to ensure the safety of exercise participants—a site employee made motions that may have alerted security officers to the targets the adversaries would be trying to reach that evening. In another inspection, security officers could observe adversaries getting into position inside the protected area prior to the start of an exercise, potentially providing clues about the route the adversaries would use to enter the site. We also observed that each force-on-force exercise was attended by a large number of people who had access to scenario information, after signing a nondisclosure form, thus increasing the chance that details about an exercise scenario might be compromised. While we recognize that procedures such as safety walk downs and prepositioning of adversary teams are necessary to the proper conduct of the force-on-force inspections, lapses in operational security have the potential to give security officers knowledge that would allow them to perform better

than they would otherwise and raise questions about whether the force-on-force inspections are a true test of the sites' protective strategy. According to NRC officials, NRC inspectors have been instructed to be vigilant regarding any indications that a site's security force may have received advance knowledge of an attack scenario, and procedures for safety walk downs have been revised to improve operational security.

- *Standards for controllers.* NRC relies on the sites to assign and train controllers to observe each participant (both the adversaries and security officers) in the force-on-force inspections.[26] In the three inspections we observed, the level of security expertise and training among the controllers varied among the sites. For example, one site assigned as controllers plant employees who did not have security-related backgrounds but who volunteered to help. In its force-on-force inspection report for this site, NRC concluded that the level of controller training was a factor in the force-on-force exercises not being brought to a definitive conclusion. (As discussed above, NRC decided to conduct another force-on-force inspection at this site.) In contrast, another plant used personnel with security backgrounds. NEI has prepared a set of guidelines for controllers in force-on-force inspections that NRC has reviewed. NEI has also created a controller-training workshop in which NEI shares lessons learned from force-on-force exercises.

- *Quality of feedback to licensee.* The quality of the feedback among the force-on-force inspections we observed was inconsistent. In particular, during the first inspection, NRC failed to discuss with the licensee several potential problems raised by the NRC team after each scenario. In the two subsequent inspections we observed, NRC appeared to have improved the quality of its feedback to the licensees. Specifically, the team leader provided the licensee with concise feedback that accurately reflected what the team members had expressed in closed NRC meetings. An NRC official told us that, based on comments from us as well as from NRC team members, NRC took measures to improve the quality of the feedback.

[26]Controllers are individuals provided by the licensee who observe each security officer and attacker to ensure the safety and effective conduct of the exercise. They make decisions about aspects of the exercise that are necessarily artificial, such as the use of explosives or any other device that could cause actual damage to a site or its security equipment. Controllers are also responsible for alerting security officers or attackers about events that are part of an exercise scenario but not actually simulated, such as an explosion or loss of power.

- *Force-on-force inspection schedule.* So far, NRC is on schedule to conduct the first round of force-on-force inspections at all sites within 3 years. As we reported in 2004, NRC is planning to conduct an inspection at each site every 3 years instead of every 8 years, as the agency had been doing.[27] NRC initiated a new force-on-force program in November 2004, together with a 3-year schedule to complete inspections at all sites, after the revised DBT took effect on October 29, 2004. NRC officials told us they had completed inspections at 20 (or about 31 percent) of the 65 sites as of November 1, 2005. Furthermore, NRC officials told us that three teams are conducting the inspections and that NRC is hiring additional force-on-force personnel. Given the importance of the force-on-force inspections in demonstrating how well a nuclear power plant might defend against a real-life threat, we believe it is important that NRC devote the necessary resources to ensure that it continues to meet the inspection schedule.

Conclusions

The nuclear power industry and NRC have taken very seriously the need to protect nuclear power plants against a potential terrorist attack and have made important investments to this end. However, NRC's process for revising the DBT for nuclear power plants raises a fundamental question—the extent to which the DBT represents the terrorist threat as indicated by intelligence data versus the extent to which it represents the threat that NRC considers reasonable for the plants to defend against. Specifically, NRC's process for deciding on the DBT raised the possibility that the industry may have inappropriately influenced the staff's interpretation of intelligence data. The NRC threat assessment staff obtained the views of the nuclear industry on a draft of the revised DBT while they continued to assess intelligence information, and the staff made industry-recommended changes to the DBT even though the intelligence information had not changed. We recognize that NRC should and would want to obtain feedback from the industry and other stakeholders on the implications of the proposed changes before finalizing the DBT. In addition, NRC has stated that it has altered its process for obtaining industry feedback so that the threat assessment staff interacts with industry only after it has made its proposals for changes to the DBT. However, this approach does not entirely eliminate the appearance of industry influence. Threat assessment is a continuous process, and this sequential approach would still allow for

[27]In addition to triennial force-on-force inspections, NRC requires licensees to conduct and document additional security force training drills.

interactions between the agency's threat assessment staff and the nuclear industry. Assigning responsibility for obtaining feedback from the nuclear industry to an office within NRC other than the Threat Assessment Section would further reduce any appearance of industry influence on the process of assessing the terrorist threat to nuclear power plants. The commissioners would then be able to review the threat assessment staff's recommended changes to the DBT with confidence that the recommendations are based strictly on an assessment of the threat. In making the final decision to revise the DBT, the commissioners would also consider industry feedback on the staff's recommendations.

Furthermore, the commissioners did not have explicit criteria that they used as the basis for removing certain weapons from the DBT recommended by the NRC staff. Consideration of what is reasonable for a private security force to defend against, as well as industry views on proposed changes to the DBT, is an appropriate function of the commissioners. However, explicit criteria setting out the factors and how they would be weighed to determine what adversary characteristics are not reasonable for a private security force to defend against would have provided greater transparency for the commissioners' decisions to exclude certain characteristics from the DBT. Such criteria would also potentially increase the rigor and consistency of the process. The underlying process used by NRC was logical and well defined and should enable NRC to produce a more credible DBT if these shortcomings are addressed.

In our visits to nuclear power plants, we saw a clear connection between the changes in the DBT and the plants' recent security enhancements. The plants' response to the revised DBT and other NRC orders following the September 11 terrorist attacks has been substantial and, in some cases, has gone beyond what was required. Nevertheless, because the plants essentially designed their security to defend against the DBT outlined by NRC, their capability to defend against an attack is essentially limited to how similar such an attack would be to the DBT. Therefore, it is imperative that NRC and the plants continue to work with DHS and other federal, state, and local authorities to ensure they have coordinated their efforts to defend plants in the event of an attack, particularly one that exceeds the adversary characteristics in the revised DBT. Furthermore, although security has improved, the results of NRC's baseline and force-on-force inspections conducted thus far have uncovered some problems that needed to be addressed. Moreover, the effectiveness of any nuclear power plant's security depends on the various parts and systems working well together during the stress of an actual attack. Therefore, NRC's continued vigilance

at the plant level, especially in conducting force-on-force inspections, is needed to ensure that plants are consistently well protected.

In conjunction with revising the DBT, NRC has implemented improvements to its force-on-force inspection program that put the agency in a better position to evaluate the nuclear power plants' protective strategies. These improvements have addressed several of our previous recommendations regarding the force-on-force inspections. However, in observing three inspections, we noted additional opportunities for improvement, such as artificialities that could be further reduced to better test how plants would respond to an actual terrorist attack. Making further improvements to the force-on-force program would enhance NRC's ability to assure the public and Congress that nuclear power plants are capable of defending against a DBT-style terrorist attack.

Recommendations for Executive Action

To improve the process by which NRC makes future revisions to the DBT for nuclear power plants, we recommend that the NRC commissioners take the following two actions:

- Assign responsibility for obtaining feedback from the nuclear industry and other stakeholders on proposed changes to the DBT to an office within NRC other than the Threat Assessment Section, so that the threat assessment staff is able to assess the terrorist threat to nuclear power plants without creating the potential for or appearance of industry influencing their analysis. The commissioners, in turn, could consider both the staff's analysis of the terrorist threat and industry feedback to make the final determination as to whether and how to revise the DBT.

- Develop explicit criteria to guide the commissioners in their deliberations to approve changes to the DBT. These criteria should include setting out the specific factors and how they will be weighed in deciding what characteristics of an attack on a nuclear power plant would constitute an enemy of the United States, or otherwise would not be reasonable for a private security force to defend against.

We further recommend that the NRC commissioners continue to evaluate and implement measures to further strengthen the force-on-force inspection program. For example, NRC may be able to identify and reduce artificialities associated with the inspections to better test how nuclear power plants would respond to an actual terrorist attack.

Agency Comments and Our Evaluation

We provided a draft of this report to NRC for its review and comment. In its written comments (see app. III), NRC commended GAO's effort to ensure that the report is accurate and constructive. It also provided additional clarifying comments on two areas of the report pertaining to the process NRC used in 2003 to revise the DBT for nuclear power plants. First, NRC stated that the report should provide a better description of the context for the process by which the agency obtained industry input and the appearance of industry influence on the development of the revised DBT. NRC wrote that the agency made a deliberate decision to develop the revised DBT while simultaneously (rather than sequentially) seeking input from stakeholders, including the nuclear industry. NRC stated that this was a departure from its typical approach and was intended to advance public health and safety and the common defense and security, similar to other government actions taken after the September 11, 2001, terrorist attacks. In addition, NRC stated that it has returned to its normal sequential approach to developing DBT revisions and seeking input from stakeholders.

We are pleased that NRC recognizes the need to separate the process of analyzing intelligence information from seeking input from stakeholders, including the nuclear industry. In response to NRC's earlier comments on the classified version of this report, which were essentially the same, we revised the reports to clarify that NRC deliberately decided to develop the revised DBT while simultaneously obtaining stakeholder input to speed up the process in the aftermath of the September 11, 2001, terrorist attacks. However, whether NRC chooses to use a simultaneous or sequential process, we continue to believe that the best approach would be to insulate the threat assessment staff from interactions with the nuclear industry by assigning responsibility for such interactions to a different office in NRC. This would best separate the fact-based analysis of the threat to commercial nuclear power plants from policy-level considerations regarding what is reasonable for a private security force to defend against. We also clarified our recommendation to indicate our view that the threat assessment staff should be insulated from interacting with the nuclear industry and other stakeholders.

Second, regarding the criteria the commission used to make decisions regarding the DBT, NRC wrote that a more comprehensive discussion in the report of the commission's deliberative decision-making process would provide important perspective. NRC stated that the agency first established a DBT for nuclear power plants in the late 1970s and has a long history in this area. Furthermore, NRC wrote that the commission's decision-making

authority does not require, and could be unduly restricted by, detailed prescriptive criteria. Finally, NRC stated its view that the basis for the commission's policy decisions and direction to the NRC staff with regard to the DBT are sufficiently articulated in the commission's voting record and related staff requirements memorandums.

We revised the reports to include NRC's view that the basis for the commission's policy decisions regarding the DBT is articulated in the commission's voting record and related staff requirements memorandum. However, based on our review of the voting record and staff requirements memorandum, as well as other documents related to the April 2003 revised DBT, we remain concerned that the basis for how the commissioners made decisions to exclude certain characteristics from the DBT is not as transparent as it could be. We did not find that the commissioners agreed upon a definition of "enemy of the United States" or explicit criteria for what adversary characteristics would not be reasonable for a private security force to defend against. For example, the memorandum accompanying the commission's April 2003 decision approving changes to the DBT for nuclear power plants did not provide the reason for the commission's decision to remove two weapons the NRC threat assessment staff had recommended for inclusion. Rather, the voting record showed that individual commissioners used differing criteria and emphasized different factors, such as cost or practicality of defensive measures. The staff requirements memorandum set forth the general criteria that a civilian security force cannot reasonably be expected to defend against all threats. Furthermore, the intent of our recommendation that NRC develop criteria for what adversary characteristics constitute an enemy of the United States, or otherwise would not be reasonable for a private security force to defend against, is not to restrict the commission's decision-making authority through detailed prescriptive criteria. Instead, the intent of our recommendation is to have general criteria or definitions to guide the commissioners' decisions and to provide greater transparency for commission decisions, the details of which are safeguards information and withheld from the public.

Finally, NRC commented that NRC and GAO staffs discussed potential issues related to the draft report that needed to be addressed. NRC also wrote that the draft report contained safeguards information, which should be removed prior to the report being made public. The potential issues have been resolved, and we have revised the report for the purpose of removing safeguards information. The resulting report is substantially the same as the classified version of the report, with the exception that the

classified version contains additional details about the DBT and security at nuclear power plants.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to interested congressional committees, the Chairman of NRC, and other interested parties. 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 contact me at (202) 512-3841 or wellsj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix IV.

Sincerely yours,

Jim Wells
Director, Natural Resources and Environment

Scope and Methodology

To examine the process the Nuclear Regulatory Commission (NRC) used to develop the April 2003 design basis threat (DBT) for radiological sabotage applied to nuclear power plants, we analyzed NRC's documentation of the process and conducted interviews with NRC threat assessment staff and other officials. In particular, we compared the adversary characteristics of the April 2003 revised DBT approved by the commissioners with the adversary characteristics in the previous DBT, as described in a February 2000 NRC staff position paper; the January 2003 draft DBT provided to stakeholders for comment; and the NRC staff's April 2003 recommended changes to the DBT submitted to the commissioners. Furthermore, for each component of NRC's process, we analyzed documents and conducted a series of interviews:

- To examine the role of intelligence analysis, we analyzed the NRC staff's reports on the terrorist threat to nuclear power plants and the results of their analysis of intelligence information on terrorist activities worldwide. The three key reports we analyzed included an October 2002 report on the use of vehicle bombs; a November 2002 report on the potential use of other adversary characteristics against nuclear power plants; and the April 2003 report that included the staff recommendations on the DBT. To obtain further insight into the NRC's use of intelligence information, we interviewed NRC officials, including the head of NRC's Threat Assessment Section; reviewed a description of the adversary characteristics screening process; and received briefings on the process from NRC. We also interviewed officials from other federal agencies, including the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). NRC redacted text from a number of the documents provided to us if the text contained classified information from other federal agencies, including the Department of Energy (DOE). As agreed with NRC, we identified the selected portions of the redacted text that we wanted to review, and NRC requested permission from the other agencies to provide the text to us. All of the agencies NRC contacted except one granted permission to release the redacted text to us.

- We compared NRC's April 2003 revised DBT with DOE's October 2004 DBT and February 2004 Terrorist Adversary Capabilities List and interviewed DOE Office of Security officials regarding the DOE DBT and differences with the NRC DBT. We also reviewed the September 2004 final report of the DOE DBT re-examination task force. We did not compare the implementation of security measures at DOE sites to

defend against the DOE DBT with security at commercial nuclear power plants.

- To examine NRC's consultation with the nuclear industry, we reviewed the written comments submitted by the Nuclear Energy Institute (NEI) on the January 2003 draft DBT and compared NEI's comments with the changes the NRC staff made to the draft DBT. We also interviewed NEI officials and senior officials at the nuclear power plant sites we visited, including some who served on the NEI working group responsible for security matters.

- To examine the decisions by the NRC commission, we analyzed the commission voting record (including written comments of individual commissioners), the April 2003 memorandum summarizing the commission's final decisions, and the NRC regulation on enemy of the United States (10 C.F.R. § 50.13). Furthermore, we interviewed three of the four commissioners who were serving on the commission at the time the DBT was revised and who participated in the decision-making process.[1] We interviewed the three commissioners as a group in a meeting that was not subject to the requirements of the Government in the Sunshine Act.[2] This meant that the commissioners could discuss previous actions, including their April 2003 decisions on changes to the DBT, but not the formulation of future policy. For example, we did not ask the commissioners about the potential for future changes to the DBT. In addition to this meeting, we met individually with the two commissioners who assumed their posts in 2005 and did not participate in the decision-making process for the April 2003 revised DBT.

To determine what actions nuclear power plants have taken to enhance security in response to the revised DBT, we interviewed staff from NRC's Office of Nuclear Security and Incident Response, reviewed security orders NRC has issued since September 11, 2001, and visited a nonprobability sample of four nuclear power plant sites.[3] We do not name the sites we

[1]The fourth commissioner was no longer serving on the commission at the time of our review.

[2]Pub. L. No. 94-409 (1976), 5 U.S.C. § 552b.

[3]Results from nonprobability samples cannot be used to make inferences about a population, because in a nonprobability sample some elements of the population being studied have no chance or an unknown chance of being selected as part of the sample.

visited in this report because information about security at particular sites is sensitive and considered safeguards information, and because the objective of our visits was to provide a general description of the changes in security sites implemented in response to the revised DBT, rather than the changes at a particular site. Prior to our site visits, we observed a baseline inspection at one site and a multiexercise force-on-force inspection at another site in order to better familiarize ourselves with NRC security requirements as well as sites' security equipment and strategies. We selected these two sites based on the timing of the activities.

To select the nonprobability sample of four sites we visited, we first eliminated certain sites, such as those we had recently visited for security-related work (including the two sites where we observed NRC inspections) and sites frequently visited by Congress. We then selected one site from each of the four NRC regions using the following criteria:

- sites representing different sizes and types of licensees, including licensees that own or operate a single nuclear power plant site, licensees that own or operate two to six sites, and licensees that own or operate seven or more sites;
- sites with different surroundings, such as different topography and proximity to water, in order to consider the effect of such factors on sites' security strategies;
- sites with security forces hired both directly as site employees as well as through a contractor, including one site that uses security officers employed by Wackenhut Corporation, which provides security services to about half of the nuclear power plant sites;
- sites with the two different categories of reactors licensed by NRC for operation in the United States—two sites with boiling-water reactors and two sites with pressurized-water reactors; and
- sites with different numbers of reactors.

At each of the four sites, we used a semistructured guide to interview security managers and other site officials, and interviewed a random selection of security officers. We worked with site management so that our interviews with the security officers did not interfere with their duties. We conducted individual interviews with security officers in private rooms, without the attendance of plant management or other plant staff. We also

examined security equipment and reviewed documents, including security plans, protective strategy documents, safeguards event logs, security officer work-hour records, training materials, and equipment testing records. GAO staff with a professional background in security accompanied us on our visits in order to provide the expertise needed to fully comprehend the sites' security equipment and strategies.

In addition to site visits, we reviewed 9 of the 16 force-on-force inspection reports and a sample of 18 baseline inspection reports that NRC had completed between November 2004 and the time we reviewed the reports.[4] The 18 baseline inspection reports we reviewed consisted of reports provided by NRC from each of the four regions, plus additional reports we randomly selected ourselves.[5] Time constraints prevented us from reviewing additional reports. We also discussed the revised DBT and security improvements at nuclear power plant sites with the Nuclear Energy Institute and the Project on Government Oversight, an independent nonprofit organization.[6]

To review NRC's progress in strengthening the conduct of force-on-force inspections, we observed a total of three inspections at two sites. Two of the inspections were at a site where NRC decided to conduct a second inspection as a result of the agency's limited ability to evaluate security during the first inspection. After the first inspection at this site, but before the second, we also attended a meeting at the site in which the licensee briefed NRC on security improvements the site had made in response to the first inspection, and we observed these improvements. GAO staff with a professional background in security accompanied us to the third inspection. In addition, as discussed above, we reviewed NRC reports on 9 of the 16 force-on-force inspections NRC had completed at the time we reviewed the reports. Finally, we interviewed NRC officials responsible for implementing the force-on-force inspection program. We conducted our

[4]In accordance with its inspection manual, NRC has 45 days to report the results of a force-on-force inspection. Thus, while NRC had completed 16 force-on-force inspections at the time of our review, only 9 reports were available to us to review for this report.

[5]NRC may complete a baseline inspection at one site over several visits to the site and produce a report for each visit. Because of this, the inspection scope of the 18 reports we reviewed varied.

[6]We did not discuss the details of the DBT with representatives of the Project on Government Oversight because such information is safeguards information.

work from November 2004 through January 2006 in accordance with generally accepted government auditing standards.

Details of Findings from NRC Reports on Baseline and Force-on-Force Inspections

Of the 27 baseline and force-on-force inspection reports we reviewed, NRC identified no findings in 11 of the reports but did describe a variety of problems with the sites' security in the remaining 16. The reports we reviewed included one on a force-on-force inspection we observed, in which NRC required the licensee to implement measures to address weaknesses in the site's protective strategy and decided to return for a second force-on-force inspection. The following are additional examples of NRC findings from the 16 reports, including corrective actions taken by the licensees:[1]

- In a baseline inspection at a site, several alarms failed to activate during a test of the intrusion detection system, which alerts security officers to the occurrence and location of a breach. Further testing identified multiple alarms that were not functioning properly, and the site subsequently declared the entire intrusion detection system inoperable. Prior to leaving the site, NRC inspectors confirmed that the site implemented compensatory measures to address problems with the intrusion detection system, and NRC determined that further inspection of the site at a later date was warranted. According to NRC, the subsequent inspection at the site confirmed that the problem had been corrected.

- During a force-on-force exercise at another site, NRC observed two officers performing duties other than their assigned patrols of the owner-controlled area. The patrols are a component of NRC's requirement for continuous surveillance of the owner-controlled area. Further inspection revealed that the security officers manning the site's central and secondary alarm stations were unaware that the owner-controlled area was not being continuously patrolled. In the event of an attack, owner-controlled area observations can be crucial both for setting a response in motion by detecting intruders as early as possible and for providing information about where attackers have entered the site and where they are going so that security officers know how to respond. According to NRC, the licensee took immediate corrective action. Also during this inspection, NRC observed that the licensee deployed too many officers in the force-on-force scenarios as a result of a misunderstanding. In particular, the licensee had temporarily increased the number of dedicated responders above the minimum listed in the security plan to respond to the increased national threat

[1]We did not verify the corrective actions taken by the licensees.

level. However, according to NRC, the additional officers did not play a role in stopping the attackers in the scenarios.

- In a baseline inspection, NRC observed three examples of failure to perform proper searches of personnel entering the protected area. For example, a security officer did not examine items that had alarmed a metal detector and allowed an individual to collect and carry the items into the protected area without further examination. Based on discussions with security officers and supervisors, NRC found that this deficiency was routine and commonly accepted at the site. NRC concluded that this situation had the potential to reduce the overall effectiveness of the protective strategy by allowing the uncontrolled introduction of weapons or explosives into the protected area. According to NRC, the licensee took immediate corrective action, and security staff were required to attend remedial training on search techniques and policy.

- In a force-on-force exercise, the attackers were able to destroy three out of four targeted components. NRC observed that the attackers faced an insufficient level of delay, which allowed them to reach the three components before being interdicted by security officers. According to the inspection report, sufficient delay is an essential component of a protective strategy to prevent radiological sabotage. As a result of the inspection, the licensee agreed to add delay locks to doors and relocate security officers to ensure they could interdict attackers.

- NRC found that a number of sites ran weapons-training qualification courses in which security officers were not trained in the way they would be expected to perform during an attack. For example, sites did not train security officers to use backup weapons for when they could not use their primary weapons, or to undergo the level of physical stress an officer would experience during an attack. At one of the sites, NRC also found that the site had lowered the minimum qualification score related to training security officers to use their weapons, potentially resulting in security officers being less qualified in the use of their weapons than what NRC believes is necessary. In addition, the licensee did not seek NRC approval for the change as mandated by NRC's regulations. However, NRC found that all of the security officers who had received the training before the issue was observed and corrected had qualified on the use of their weapons at the higher score. Furthermore, according to NRC, the agency issued amplified guidance

to all nuclear power plant sites regarding weapons-training qualification courses.

- During the force-on-force inspection we observed, NRC inspectors found that a site had not included the control room, spent fuel pool, and the alternative shutdown panel among its targets. NRC required the licensee to redevelop its target components for use in the force-on-force scenarios. The adequate identification of target components is vital to a site's ability to position security officers or direct them to locations where they can interpose themselves between the attacker and target components.

- In an inspection initiated after the licensee observed security officers who were inattentive at their posts, NRC inspectors found the licensee had recorded 19 incidences in which security officers worked more hours in a specific time period than allowed by NRC regulations. NRC concluded that failure to meet the work-hour limits increased the susceptibility of security officers to fatigue and had the potential to reduce the effectiveness of the site's protective strategy. According to the inspection report, the licensee identified several causes that contributed to the problem and took immediate corrective actions. According to NRC, the agency verified that the site updated its procedures to conform to NRC's work-hour regulations. (At the four sites we visited, we reviewed work-hour logs and found that each site had generally stayed within security officer work-hour limits.)

- In a baseline inspection, the licensee was unable to provide engineering documents to demonstrate the acceptable minimum safe standoff distance from the inner vehicle barrier system, which is designed to protect the site from a vehicle bomb. NRC requested that the licensee measure the distance between several structures and the closest part of the vehicle barrier system. The measurements showed that the barrier was too close to at least two structures. As immediate corrective and compensatory actions, the licensee installed additional vehicle barriers in the area of concern and implemented direct observation by a security officer.

Comments from the Nuclear Regulatory Commission

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

February 23, 2006

Mr. James E. Wells, Jr.
Director, Natural Resources
and Environment
U.S. Government Accountability Office
441 G Street NW
Washington, D.C. 20548

Dear Mr. Wells:

On behalf of the U.S. Nuclear Regulatory Commission (NRC), I am responding to your letter by e-mail dated February 7, 2006, requesting NRC review and comment on your unclassified, draft report, "Nuclear Power Plants: Efforts Made to Upgrade Security, but the Nuclear Regulatory Commission's Design Basis Threat Process Should Be Improved" (GAO-06-388). I appreciate your providing the NRC the opportunity to review this draft report and the willingness of you and your staff to maintain a continuing dialogue with the NRC. I also appreciate the time and effort that you and your staff have invested in reviewing this important topic and the care that you have taken to ensure that your report is accurate and constructive. I understand that the U.S. Government Accountability Office (GAO) plans to make a number of changes to enhance the report's accuracy, clarity, and context. Given NRC's current understanding of the report's contents, I am providing additional clarifying comments for your consideration on two areas of the report. Please note that these comments are the same as those I provided to you on January 24, 2006, on the classified version of this report, which the NRC previously reviewed.

First, GAO's draft report suggests that having detailed criteria for use during design basis threat (DBT) decision-making regarding radiological sabotage at nuclear power plants would increase transparency and reduce a potential for the appearance of arbitrariness. The Commission rejects any implication of arbitrariness. The Commission has been guided by the Atomic Energy Act and its regulations and the broad policy considerations that have been found pertinent during deliberations on the DBT. The Commission has a long history of experience in this area, having first established a DBT for nuclear power plants in the late 1970s. While additional delineation of relevant considerations might be useful in some circumstances, reasoned judgment within this and other areas of the Commission's statutory decision-making authority does not require, and in fact could be unduly restricted, by detailed prescriptive criteria. Moreover, consistent with governing statutes, the Commission utilized an appropriate decision-making process by providing for a majority Commission position on well-documented staff papers in order for actions to proceed, and documenting individual Commissioner views and proposed modifications for consideration by other Commissioners. With regard to the revised DBT, the report does not reflect the NRC's view that the basis for the Commission's policy decisions and direction to the NRC staff are sufficiently articulated in the Commission voting record and related staff requirements memoranda on the revised DBT. A more comprehensive discussion of the Commission's deliberative decision-making process in the report would provide important perspective, and the members of the NRC staff are available to work with you on a more comprehensive description.

-2-

Second, the NRC believes that the report should provide a better description of the context for NRC's actions regarding the opportunity for industry input and the appearance of industry influence on the development of the revised DBT in 2003. The process used for developing the revised DBT and obtaining stakeholder input was driven, in large part, by the post-9/11 threat environment and the need to enhance security at nuclear power plants. The agency made a deliberate decision to develop the revised DBT, while simultaneously (in lieu of sequentially) seeking input from stakeholders (including the nuclear industry). This was a departure from our typical approach, not unlike other government actions taken after 9/11, and was intended to advance public health and safety and the common defense and security in an expedited manner. As noted in my letter of January 24, 2006, the NRC has since returned to its normal sequential approach of first developing proposed DBT revisions, and then seeking comments on the proposed revisions from stakeholders. The NRC requests that your report fully explain this issue.

In addition, the NRC and GAO staffs have discussed potential issues related to the draft report that need to be addressed. Also, NRC staff believes that the current version of the draft report contains Safeguards Information and this information should be removed prior to the document being made public. It is my understanding these issues will be appropriately resolved.

Should you have any questions about these comments, please contact either Mr. William Dean at (301) 415-1703, or Ms. Melinda Malloy, at (301) 415-1785, of my staff.

Sincerely,

Luis A. Reyes
Executive Director
for Operations

GAO Contact and Staff Acknowledgments

GAO Contact

Jim Wells, (202) 512-3841 or wellsj@gao.gov

Staff Acknowledgments

In addition to the individuals named above, Raymond H. Smith, Jr. (Assistant Director), Joseph H. Cook, and Michelle K. Treistman made key contributions to this report. Also contributing to this report were John Cooney, Doreen Feldman, Andrew O'Connell, Judy K. Pagano, Keith A. Rhodes, Carol Herrnstadt Shulman, and Barbara Timmerman.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

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

PRINTED ON RECYCLED PAPER