United States General Accounting Office

GAO

Report to Congressional Requesters

September 2003

NUCLEAR REGULATORY COMMISSION

Oversight of Security at Commercial Nuclear Power Plants Needs to Be Strengthened

GAO-03-752

September 2003

NUCLEAR REGULATORY COMMISSION

Oversight of Security at Commercial Nuclear Power Plants Needs to Be Strengthened

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-03-752, a report to congressional requesters

Why GAO Did This Study

The September 11, 2001, terrorist attacks intensified the nation's focus on national preparedness and homeland security. Among possible terrorist targets are the nation's nuclear power plants—104 facilities containing radioactive fuel and waste. The Nuclear Regulatory Commission (NRC) oversees plant security through an inspection program designed to verify the plants' compliance with security requirements. As part of that program, NRC conducted annual security inspections of plants and force-on-force exercises to test plant security against a simulated terrorist attack. GAO was asked to review (1) the effectiveness of NRC's security inspection program and (2) legal challenges affecting power plant security. Currently, NRC is reevaluating its inspection program. We did not assess the adequacy of security at the individual plants; rather, our focus was on NRC's oversight and regulation of plant security.

What GAO Recommends

GAO is making recommendations to strengthen NRC's oversight at commercial nuclear power plants by promptly restoring annual security inspections and revising force-on-force exercises. NRC disagreed with many of GAO's findings, but did not comment on GAO's recommendations. GAO continues to believe its findings are appropriate and the recommendations need to be acted upon.

www.gao.gov/cgi-bin/getrpt?GAO-03-752.

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 has taken numerous actions to respond to the heightened risk of terrorist attack, including interacting with the Department of Homeland Security and issuing orders designed to increase security and improve plant defensive barriers. However, three aspects of its security inspection program reduced NRC's effectiveness in overseeing security at commercial nuclear power plants.

First, NRC inspectors often used a process that minimized the significance of security problems found in annual inspections by classifying them as "non-cited violations" if the problem had not been identified frequently in the past or if the problem had no direct, immediate, adverse consequences at the time it was identified. Non-cited violations do not require a written response from the licensee and do not require NRC inspectors to verify that the problem has been corrected. For example, guards at one plant failed to physically search several individuals for metal objects after a walk-through detector and a hand-held scanner detected metal objects in their clothing. The unchecked individuals were then allowed unescorted access throughout the plant's protected area. By making extensive use of non-cited violations for serious problems, NRC may overstate the level of security at a power plant and reduce the likelihood that needed improvements are made.

Second, NRC does not have a routine, centralized process for collecting, analyzing, and disseminating security inspections to identify problems that may be common to plants or to provide lessons learned in resolving security problems. Such a mechanism may help plants improve their security.

Third, although NRC's force-on-force exercises can demonstrate how well a nuclear plant might defend against a real-life threat, several weaknesses in how NRC conducted these exercises limited their usefulness. Weaknesses included using (1) more personnel to defend the plant during these exercises than during a normal day, (2) attacking forces that are not trained in terrorist tactics, and (3) unrealistic weapons (rubber guns) that do not simulate actual gunfire. Furthermore, NRC has made only limited use of some available improvements that would make force-on-force exercises more realistic and provide a more useful learning experience.

Even if NRC strengthens its inspection program, commercial nuclear power plants face legal challenges in ensuring plant security. First, federal law generally prohibits guards at these plants from using automatic weapons, although terrorists are likely to have them. As a result, guards at commercial nuclear power plants could be at a disadvantage in firepower, if attacked. Second, state laws vary regarding the permissible use of deadly force and the authority to arrest and detain intruders, and guards are unsure about the extent of their authorities and may hesitate or fail to act if the plant is attacked.

Contents

Abbreviations

DOE	Department of Energy
NRC	Nuclear Regulatory Commission
OSRE	Operational Safeguards Response Evaluation

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, D.C. 20548

September 4, 2003

The Honorable John D. Dingell
Ranking Minority Member
Committee on Energy and Commerce
House of Representatives

The Honorable Edward J. Markey
House of Representatives

The September 11, 2001, terrorist attacks on the World Trade Center and the Pentagon intensified the nation's focus on national preparedness and homeland security. Among possible terrorist targets are the nation's commercial nuclear power plants—104 facilities containing radioactive fuel and waste operating in 32 states. The Nuclear Regulatory Commission (NRC) licenses commercial nuclear power plants and requires the licensee, among other things, to protect the plants against a potential terrorist threat. The design basis threat—which NRC develops for these facilities—delineates the maximum number of terrorists that NRC expects plants to defend against, the extent of their training, and the weapons and tactics they could use.

To ensure that commercial nuclear power plants can be protected against the design basis threat and meet other security requirements, NRC requires each licensee to have an NRC-reviewed and -approved security plan before NRC allows the plant to operate. After the plant begins operations, NRC oversees plant security through an inspection program designed to verify that the plant continues to meet security requirements. As part of the security inspection program, NRC conducts annual security inspections of plants and conducts force-on-force exercises. During the security inspections, NRC reviews (1) the list of those who have access to the plant, (2) the plant's response to an unusual security event, (3) any changes to the security plan, and (4) samples of the plant's own assessment of its security. Since 1991, the inspection program has also included periodic force-on-force exercises, which are designed to simulate an attack on the plant that is based on the design basis threat. NRC also conducts nonrecurring inspection activities, such as special inspections to ensure that post-September 11, 2001, security enhancements have been implemented at each plant.

In 2001, NRC curtailed its annual security inspections and force-on-force exercises to redesign them for heightened security threats. Until the annual

security inspections are resumed sometime in 2004, NRC inspectors have been verifying that post-September 11, 2001, security improvements have been implemented at each plant and conducting special inspections if a serious problem is identified by the licensee in its quarterly self-assessment. In terms of force-on-force exercises, NRC is currently testing and evaluating these exercises under a pilot program that has resulted in five exercises being conducted since January 2003.

You asked us to review (1) the effectiveness of NRC's inspection program to oversee security at commercial nuclear power plants and (2) legal challenges currently affecting physical security at the power plants. We did not assess the adequacy of security at the nation's nuclear power plants. Rather, our focus was on NRC's oversight and regulation of plant security. In conducting our review, we analyzed NRC's inspection program from January 2000 through September 2001 and the force-on-force exercise program from January 1991 through September 2001. We also reviewed NRC's initiatives to enhance power plant security after September 11, 2001, as well as its efforts to ensure that the power plants implemented those initiatives. We met with NRC, the Department of Energy (DOE), and power plant representatives and obtained NRC advisories, orders, regulations, and inspections reports. To determine how NRC tests the power plants' security, we reviewed reports for 80 force-on-force exercises that NRC conducted through September 2001. We designed and completed a data collection instrument in order to organize specific elements that we extracted from these reports. We also held discussions with DOE officials to determine how they conduct force-on-force exercises at DOE's nuclear facilities and if there are any "promising practices" that might be applied to NRC's program. Finally, we obtained NRC's and industry officials' views on laws that could affect a licensee's ability to adequately secure commercial nuclear power plants. Appendix I contains a more detailed discussion of our scope and methodology.

Results in Brief

Since September 11, 2001, NRC has taken numerous actions to increase security at commercial nuclear power plants. However, three aspects of NRC's security inspection program have reduced its effectiveness in overseeing security at commercial nuclear power plants. First, during annual inspections, NRC inspectors often classified security problems as "non-cited violations" if the problem had not been identified frequently in the past or if the problem had no direct, immediate, adverse consequences at the time that it was identified. This classification tends to minimize the seriousness of the problems. Non-cited violations do not require a written

response from the licensee and do not require NRC inspectors to verify that each problem has been corrected. For example, guards at one plant failed to physically search several individuals for metal objects after a walk-through detector and a hand-held scanner detected metal objects in their clothing. The unchecked individuals were then allowed unescorted access throughout the plant's protected area. Although this incident appears serious, NRC issued a non-cited violation for it and rated the plant's security as meeting security objectives. Through its extensive use of non-cited violations, rather than reporting the problems as more serious cited violations, NRC may have overstated the level of security at power plants.

Second, NRC does not have a centralized process for routinely collecting, analyzing, and disseminating security inspections to identify problems that may be common to plants or to provide lessons learned in resolving a security problem. Third, although force-on-force exercises could demonstrate how well a nuclear plant might defend against a real-life threat, several weaknesses in how NRC conducted past exercises limited their usefulness. Specifically, (1) NRC conducted these exercises at each nuclear power plant once every 8 years; (2) the licensees used plant defenses during the exercises that were enhanced beyond those used during normal operations; (3) the attacking forces were not trained in terrorist tactics; (4) participants used unrealistic weapons (e.g., rubber guns instead of laser equipment, which would better simulate weapon fire); (5) exercises did not test the full extent of the design basis threat; and (6) exercise reports were often late. As a result, the exercises did not provide information on a power plant's ability to defend against the maximum design basis threat and permanent correction of problems may have been delayed. Furthermore, NRC has made only limited use of some available administrative and technological improvements that would make force-on-force exercises more realistic and provide a more useful learning experience.

Commercial nuclear power plants face legal challenges in ensuring physical plant security. First, federal law generally prohibits private citizens—including guards at these plants—from using automatic weapons, although terrorists are likely to have them. As a result, guards at commercial nuclear power plants could be at a disadvantage in firepower if attacked. Second, state laws vary regarding the permissible use of deadly force and the authority to arrest and detain intruders. According to NRC's force-on-force reports and NRC officials, plant guards are unsure about when and if they can use deadly force, and guards are unclear about what authority they have to arrest and detain intruders. As a result, guards may

hesitate or fail to take action if a plant comes under attack. NRC has recognized the impact of these federal and state laws on security and has sought federal legislation to address these legal challenges.

We are making recommendations to the NRC Commissioners to restore and strengthen NRC's oversight of security at commercial nuclear power plants—specifically, NRC's annual inspection program and force-on-force exercises. In reviewing a draft of this report, NRC did not comment on our conclusions and recommendations. NRC did comment that our report failed to reflect changes made to the program since September 11, 2001, and that the issues addressed in the report were relatively minor and were appropriately addressed. While we agree that NRC has taken many actions since September 11, we note that most of these actions related to enhancing security at the plants and did not relate to NRC's oversight efforts. In fact, since September 11, NRC has suspended the two major elements of its oversight program, baseline inspections and force-on-force exercises. We believe that the issues cited in this report, such as improperly screening individuals entering the plant, are not minor, and that promptly restoring the annual security inspections and force-on-force exercises will improve NRC's oversight responsibilities.

Background

NRC is an independent agency established by the Energy Reorganization Act of 1974 to regulate civilian use of nuclear materials. NRC is headed by a five-member commission. The President designates one commission member to serve as Chairman and official spokesperson. The commission as a whole formulates policies and regulations governing nuclear reactor and materials safety, issues orders to licensees, and adjudicates legal matters brought before it. Security for commercial nuclear power plants is primarily the responsibility of NRC's Office of Nuclear Security and Incident Response. This office develops overall agency policy and provides management direction for evaluating and assessing technical issues involving security at nuclear facilities, and it is NRC's safeguards and security interface with the Department of Homeland Security, the intelligence and law enforcement communities, DOE, and other agencies.[1] The office also develops and directs the NRC program for response to incidents, and it is NRC's incident response interface with the Federal Emergency Management Agency and other federal agencies. NRC

[1]DOE operates facilities that contain radioactive material used in its nuclear weapons program.

implements its programs through four regional offices. Figure 1 shows the location of commercial nuclear power plants operating in the United States. (See app. II for a list of the commercial nuclear power plants, their locations, and the NRC regions that are responsible for them.)

Figure 1: Commercial Nuclear Power Plants in the United States

Source: GAO analysis of NRC data.

Commercial nuclear power plants are also subject to federal and state laws that control certain matters related to security functions, such as the possession and use of automatic weapons by security guards and the use of deadly force.

NRC Security Regulation and Oversight

NRC begins regulating security at a commercial nuclear power plant when the plant is constructed. Before granting an operating license, NRC must approve a security plan for the plant. Since 1977, NRC has required the plants to have a security plan that is designed to protect against a design basis threat for radiological sabotage.[2] Details of the design basis threat are considered "safeguards information" and are restricted from public dissemination.[3] The design basis threat characterizes the elements of a postulated attack, including the number of attackers, their training, and the weapons and tactics they are capable of using. The design basis threat, revised twice since it was first issued in 1977, requires the plants to protect against "a determined violent external assault by stealth, or deceptive actions" or "an internal threat of an insider, including an employee in any position." Under the 1977 design basis threat, plants had to

- add barriers to vital equipment and work zones and develop identification and search procedures for anyone entering restricted areas;
- upgrade alarm systems and internal communication networks and control keys, locks, and combinations; and
- maintain a minimum number of guards, armed with semiautomatic weapons, that had to be on duty at all times (unless NRC granted an exemption that allowed fewer guards).

In 1993, in response to the first terrorist attack on the World Trade Center in New York City and to a vehicle intrusion at the Three Mile Island nuclear power plant in Pennsylvania, NRC revised the design basis threat for radiological sabotage to include the possible use of a vehicle bomb. This action required the installation of vehicle barriers at the power plants. On April 29, 2003, NRC issued a revised design basis threat that the commission believes is the "largest reasonable threat against which a regulated private guard force should be expected to defend under existing law." NRC has given the power plants 18 months to comply with the new design basis threat.

[2]Radiological sabotage against a nuclear power plant is a deliberate act that could directly or indirectly endanger the public health and safety by exposure to radiation.

[3]Safeguards information is unclassified sensitive information.

NRC's inspection program is an important element in its oversight effort to ensure that commercial nuclear power plants comply with security requirements. Security inspectors from the agency's four regional offices conduct annual inspections at each plant. These inspections are designed to check that the power plants' security programs meet NRC requirements in the areas of access authorization, access control, and response to contingency events. The inspections also involve reviewing changes to the plant's security plan and random samples of the plant's own assessment of its security. NRC suspended its inspection program in September 2001 to focus its resources on the implementation of security enhancements. NRC is currently revising the security inspection program.

NRC also conducted force-on-force exercises under the security inspection program. These force-on-force exercises, which were referred to as Operational Safeguards Response Evaluation (OSRE) exercises, were designed to test the adequacy of a plant's capability to respond to a simulated attack. NRC began conducting these exercises in 1991 but suspended them after September 11, 2001. NRC intends to restructure the program. It has recently begun a series of pilot force-on-force exercises that are designed to provide a more rigorous test of security at the plants and to provide information for designing a new force-on-force exercise program. No date has been set for completing the pilot program or for initiating a new, formal force-on-force program.

NRC Actions to Enhance Security at Commercial Nuclear Power Plants since September 11, 2001

In order to respond to the heightened risk of terrorist attack, NRC has had extensive interactions with the Department of Homeland Security and the Homeland Security Council on security at commercial nuclear power plants. NRC also has issued advisories and orders that were designed to increase the size and improve the proficiency of plant security forces, restrict access to the plants, and increase and improve plant defensive barriers. On October 6, 2001, NRC issued a major advisory, stating that the licensees should consider taking immediate action to increase the number of security guards and to be cautious of temporary employees. NRC conducted a three-phase security inspection, checking the licensees to see if they had complied with these advisories. Each licensee's resident inspector[4] conducted phase one, which was a quick overview of the licensee's security program using a headquarters-prepared survey. During

[4]NRC resident inspectors are stationed at each commercial nuclear power plant facility. The resident inspectors are not security specialists, focusing primarily on plant safety.

phase two, NRC's regional security inspectors conducted a more thorough survey of each plant's security. During phase three, which concluded in January 2002, NRC's regional security inspectors reviewed each licensee's security program to determine if the licensee had complied with the additional measures suggested in the October 6, 2001, advisory.

NRC used the results from the three-phase security inspection in developing its February 25, 2002, order requiring licensees to implement additional security mechanisms.[5] Many of the order's requirements were actions suggested in previous advisories. The licensees had until August 31, 2002, to implement these security requirements. In December 2002, NRC completed a checklist to provide assurance that the licensees had complied with the order. In addition, NRC developed a security inspection procedure to validate and verify licensee compliance with all aspects of the order. NRC estimates that this procedure will be completed by December 2003. On August 14, 2003, NRC stated that 75 percent of the power plants had been inspected for compliance with the order.

NRC also took action on an item that had been a security concern for a number of years—the use of temporary clearances for temporary workers. Commercial nuclear power plants use hundreds of temporary employees for maintenance—most frequently during the period when the plant is shut down for refueling. In the past, NRC found instances in which personnel who failed to report criminal records had temporary clearances that allowed them unescorted access to vital areas.[6] In its October 6, 2001, advisory, NRC suggested that licensees limit temporary clearances for temporary workers. On February 25, 2002, NRC issued an order that limited the use and duration of temporary clearances, and, on January 7, 2003, NRC issued an order to eliminate the use of these clearances.[7] NRC now requires a criminal history review and a background investigation to be completed before allowing temporary workers to have unescorted access to the power plants.

[5]NRC Order EA-02-026.

[6]The vital area, within the protected area, contains the plant equipment, systems, devices, or material whose failure, destruction, or release could endanger the public health and safety by exposure to radiation. This area is protected by guard stations, reinforced gates, surveillance cameras, and locked doors.

[7]NRC Order EA-02-261.

On April 29, 2003, in addition to issuing a new design basis threat, NRC issued two orders that are designed to ensure that excessive work hours do not challenge the ability of security forces in performing their duties and to enhance the training and qualification program for security forces.

Three Aspects of NRC's Security Inspection Program Inhibit Effective Oversight

NRC's security inspection program may not be fully effective because of weakness in three areas. First, during the annual inspections conducted from 1999 until September 2001, NRC's regional security specialists used a process to categorize the seriousness of security problems that, in some cases, minimized their significance. As a result, NRC did not track these problems to ensure that they had been permanently corrected and may have overstated the level of security at power plants. Second, NRC does not routinely collect and disseminate information from security inspections to NRC headquarters, other NRC regions, or other power plants. Dissemination of this information may help other plants to correct similar problems or prevent them from occurring. Third, NRC has made limited use of some available administrative and technological improvements that would make force-on-force exercises more realistic and provide a more useful learning experience.

NRC's Inspection Practices Minimize the Significance of Some Security Problems

NRC ensures that commercial nuclear power plants maintain security by monitoring the performance and procedures of the licensees that operate them. NRC's inspection program is the agency's only means to verify that these plants comply with their own NRC-approved security plans and with other NRC security requirements.

NRC suspended its annual security inspection program after September 11, 2001, and currently is revising the program. NRC does not expect a new security inspection program to be implemented until some time in 2004. Although NRC has temporarily suspended its annual security inspections, it continues to check a plant's self-assessments and conduct an inspection if the licensee identifies a serious problem.

Under the previous security inspection program, initiated in 1999 and suspended in 2001, NRC used a "risk informed" performance-based system (the Reactor Oversight Process) that was intended to focus both NRC's and the licensees' resources on important safety matters. In an attempt to focus NRC attention on plants with the most serious problems, and to reduce regulatory burdens on the nuclear industry, the Reactor Oversight Process

relied heavily on performance assessment data generated by the licensees and submitted quarterly to NRC. In the security area, these licensee self-assessments provided NRC with data on (1) the operation of security equipment (such as intrusion detectors and closed-circuit television cameras), (2) the effectiveness of the personnel screening program (including criminal history and background checks), and (3) the effectiveness of the employee fitness-for-duty program (including tests for substance abuse and behavioral observations). Under guidelines for these self-assessments, licensees are required to report only the most serious problems. NRC inspectors followed a multistep process to monitor security, including verifying the licensees' self-assessments and conducting their own annual inspection. NRC inspectors did not verify all aspects of the licensees' self-assessments. Instead, the inspectors made random checks of the quarterly self-assessments during their annual security inspection of the plant.

During the inspections, the inspectors reviewed the following aspects of security at each plant:

- *Access authorization and fitness for duty (performed annually).* Inspectors interviewed supervisors and their staffs about procedures for recognizing drug use, possession, and sale; indications of alcohol use and aberrant behavior; and records of testing for suspicious behavior. These procedures were designed to ensure that the licensee conducts adequate personnel screening and enforces fitness-for-duty requirements—functions considered critical to protect against an insider threat of radiological sabotage.

- *Access control (performed annually).* Inspectors observed guards at entry points during peak hours, checked screening equipment, read event reports and logs, checked access procedures for the plant's vital area, and surveyed data in the security computers. For example, inspectors observed searches of personnel, packages, and vehicles for contraband (i.e., firearms, explosives, or drugs) before entry into the protected area and ensured that the guards granted only authorized persons unescorted access to the protected and the vital areas of the plant.

- *Response to contingency events (performed triennially).*[8] Inspectors tested the licensee's physical security by testing the intrusion detection system.

- *Random checks of changes to security plans (performed biennially).* Under NRC regulations, licensees can change their security plans without informing NRC if they believe that the change does not decrease the effectiveness of the plan. Inspectors reviewed security plan changes and could have physically examined a change if an issue arose.

If NRC inspectors detected a security problem in these areas, they determined the problem's safety significance and whether it violated the plant's security plan or other NRC requirements. If a violation occurred, and the inspectors determined that the problem was "more than minor," they used a "significance determination process" to relate the violation to overall plant security. According to NRC officials, the significance determination process is also being revised. Under the process previously used, the inspectors assigned a violation one of the following four ratings: very low significance, low to moderate significance, substantial significance, and high significance. For violations more serious than very low significance, the licensee was required to prepare a written response, stating the actions it would take to correct the problem. However, violations judged to be of very low significance—usually categorized as non-cited violations—were routinely recorded; entered into the plant's corrective action plan; and, from NRC's perspective, closed. Violations were judged to be of low significance and categorized as a non-cited violation if the problem had not been identified more than twice in the past year or if the problem had no direct, immediate, adverse consequences at the time it was identified. In addition, for non-cited violations, NRC did not require a written response from the licensee and did not routinely follow up to ensure that a permanent remedy had been implemented unless the non-cited violation was randomly selected for review of the licensee's corrective action program.

We found that NRC frequently issued non-cited violations. NRC issued 72 non-cited security violations from 2000 to 2001 compared with no cited security violations during the same period. In addition, NRC issued non-cited violations for security problems that, while within NRC's guidance for

[8]A contingency event is any event that could impact on the security of the plant.

non-cited violations, appear to be serious and seem to justify the formality and follow-up of a cited violation. For example:

- At one plant, an NRC inspector found a security guard sleeping on duty for more than half an hour. This incident was treated as a non-cited violation because no actual attack had occurred during that time, and because neither he nor any other guard at the plant had been found sleeping more than twice during the past year.

- At another plant, a security officer falsified logs to show that he had checked vital area doors and barriers when he was actually in another part of the plant. The officer was the only protection for this area because of a "security upgrade project."

- At another plant, NRC inspectors categorized two security problems as non-cited violations because they had not occurred more than twice in the past year. In one incident, an inspector observed guards who failed to physically search several individuals for metal objects after a walk-through detector and a hand-held scanner detected metal objects in their clothing. The unchecked individuals were then allowed unescorted access throughout the plant's protected area. Also, security was compromised in a vital area—where equipment that could be required to protect public health and safety is located—when an inspector found that tamper alarms on an access door had been disabled. In this case, the only compensatory measure implemented was to have a guard check the location once during each 12-hour shift.

In addition to NRC's annual inspections, NRC will conduct an inspection if a plant's quarterly self-assessment identifies a serious security problem. Between 2000 and 2002, only 4 of the 104 plants reported security problems that required NRC to conduct a follow-up inspection. In 2000, each plant identified that equipment for controlling access to the plant's protected area was often broken, requiring extra guards as compensation. None of the 104 plants' self-assessments identified any security problems in 2001, 2002, or the first 6 months of 2003.

Once every 3 months, NRC develops performance summaries for each of the nuclear power plants it regulates. In the security area, NRC uses each plant's self-assessment performance indicators and its own annual inspections as the basis for each plant's quarterly rating. The performance rating can range from "meeting security objectives" to "unacceptable." The ratings are displayed on NRC's Web site, which is the public's main link to

NRC's assessment of the security at each plant. However, because of NRC's extensive use of non-cited violations, the performance rating may not always accurately represent the security level of the plant. For example, the plant where the sleeping guard was found was rated as meeting security objectives for that period. NRC also rated security as meeting objectives at the plant where physical searches were not conducted for metal detected by scanners.

NRC Does Not Systematically Collect, Analyze, and Disseminate Information That May Improve Security at All Plants

NRC does not have a routine, centralized process for collecting, analyzing, and disseminating security inspections to identify problems that may be common to other plants or to identify lessons learned in resolving a security problem that may be helpful to plants in other regions. NRC headquarters only receives inspection reports when a licensee challenges the findings from security inspections. Following the inspection, the regional security specialist prepares a report that is then sent to the licensee for comment. If the licensee does not challenge the report's findings, the report is filed at the region. If the licensee challenges the findings, a NRC headquarters security review panel meets to resolve the issue. At this point, headquarters security specialists may informally retain copies of the case, but, officially, headquarters returns the files to the region, which replies to the licensee.

According to NRC headquarters officials, they do not routinely obtain copies of all security inspection reports because headquarters files and computer databases are insufficient to hold all inspection reports. In addition, some of the reports contain safeguards information and can only be transferred by mail, courier, or secure fax. Instead, headquarters only has a list of reports in its computer database—not the narrative details that include safeguards information. According to headquarters officials, regional NRC security specialists may maintain their own information about security problems and their resolution, but they have not done this systematically nor have they routinely shared their findings with headquarters or the other regions.

NRC's Force-on-Force Exercises Are Limited in Their Usefulness

From 1991 through 2001, NRC conducted force-on-force exercises, called OSREs, at the nation's commercial nuclear power plants. Although these exercises have provided learning experiences for the plants and may have helped improve plant security, the exercises did not fully demonstrate the plants' security preparedness. The exercises were conducted infrequently, against plant security that was enhanced by additional guards and/or

security barriers, by simulated terrorists who were not trained to operate like terrorists, and with unrealistic weapons. In addition, the exercises did not test the maximum limits of the design basis threat, and inspectors often filed OSRE reports late. As a result, the exercises did not provide complete and accurate information on a power plant's ability to defend against the maximum limits of the design basis threat, and permanent correction of problems may have been delayed. Furthermore, NRC has made only limited use of some available administrative and technological improvements that would make force-on-force exercises more realistic and provide a more useful learning experience.

Exercises Were Conducted Infrequently

NRC was not required by law, regulation, or order to conduct OSRE exercises; however, NRC and the licensees believed that these exercises were an appropriate mechanism to test the adequacy of the plants' security plans, and all licensees agreed to participate in these exercises. Since there is no requirement, NRC started the OSRE program without guidance on how frequently the exercises should be conducted at each plant. NRC conducted OSRE exercises at each commercial nuclear power plant about once every 8 years. Sixty-eight power plant sites have conducted one OSRE exercise and 12 sites have conducted two exercises.

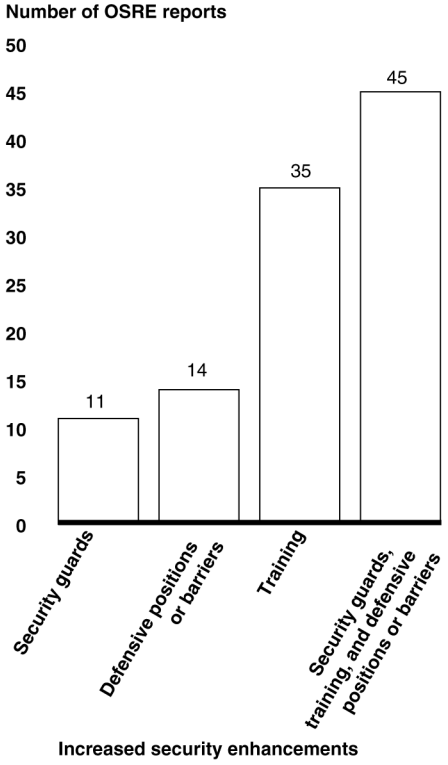
Like NRC, DOE conducts force-on-force exercises at its nuclear facilities.[9] DOE's regulations state that force-on-force exercises should be conducted at every facility once a year. According to DOE officials, annual inspections are important because DOE wants up-to-date information on security preparedness at each nuclear facility; and more frequent exercises require the facilities to maintain the quality of the security program because another drill is always only a few months away. According to NRC officials, they are planning to initiate a new force-on-force exercise program that will be based on ongoing pilot force-on-force exercises. They plan to conduct an exercise for each licensee every 3 years, which will require additional regional security inspectors.

[9]DOE's facilities differ from the commercial nuclear power plants that NRC oversees. Both of these types of facilities, however, contain radioactive material that must be protected. The security that is required to protect the facilities also differs; however, we believe that there are some similarities that allow for lessons learned or promising practices by one agency to have application by the other.

Exercises Were Conducted Against Enhanced Plant Defenses

According to NRC officials, they provided the licensee with up to 12 months' advance notice of OSRE exercises so that it could assemble a second team of security guards to protect the plant while the exercise was being conducted. However, the advanced notification also allowed licensees to enhance security prior to the OSRE exercises, and they were not required to notify NRC of any enhancements to their security plan. As a result, according to NRC officials, during the exercises, many plants increased the number of guards that would respond to an attack; added security barriers, such as additional fencing; and/or added defensive positions that they did not previously have. According to our review of all 80 OSRE reports, at least 45—or 56 percent—of the exercises were conducted against plant defenders who had received additional training for the exercise or against enhanced plant security features, such as additional guards or defensive positions or barriers. Figure 2 shows the number of OSRE reports that stated that the exercises were conducted against (1) guard forces that were larger than those provided for in the security plan; (2) increased defensive positions or barriers; (3) guards that had received additional training; and (4) guard forces that were larger than those provided for in the security plan, guards that had received additional training, or plants that had enhanced defensive positions or barriers.

Figure 2: Security Enhancements Made before OSRE Exercises



Source: GAO analysis of NRC OSRE reports.

Although we found 11 instances in which plants had increased the number of security guards for the OSRE exercises, an NRC official told us that the number was actually higher but was not reported in the OSRE reports. According to this official, 52 of the first 55 OSREs conducted used more guards than provided for in the plants' security plans. For these plants, the number of guards used exceeded the number called for in the security plan by an average of 80 percent. According to this official, using additional guards impaired the realism of the exercise because in the event of an actual attack, only the number of guards specified in the security plan would protect the plant.

Plants that used increased numbers of guards, increased training, or increased defensive positions or barriers fared better in the OSREs than those that used the plant defenses specified in the security plan. According to the OSRE reports, of the 45 plants that increased plant defenses beyond

the level specified in the security plan, 10 (or 22 percent) failed to defeat the attackers in one or more of the exercises conducted during the OSRE. However, of the 35 plants that used only the security levels specified in the security plan, 19 (or 54 percent) failed to defeat the attackers in one or more exercises conducted during the OSRE.

The increased training and preparation for the OSRE exercises provided an opportunity for the licensee to examine its security program and upgrade the program in areas found lacking. However, according to an NRC official, the licensee could decrease security to previous levels after the exercise. Consequently, the exercise only provided an evaluation of the "ramped up" security and provided little information on the plant's normal day-to-day security. According to this official, NRC could not hold a licensee accountable for ramping down after the OSRE exercise because the enhanced training and additional barriers were not part of the licensee's security plan, and NRC can only hold the licensee accountable for its security plan. NRC has not required that security enhancements implemented to prepare for OSRE exercises be included as part of the plants' security plans. However, as of November 2000, NRC no longer allowed the licensee to increase the number of guards or add defensive positions or security barriers for OSRE exercises. Between November 2000 and the suspension of the program in September 2001, only eight OSREs were conducted.

DOE—which also provides its facilities with advanced notice of a scheduled force-on-force exercise (up to 1 year) and allows the facility to upgrade its security for the exercise—requires that any enhancements to security that are implemented for the exercise become integrated into the facility's security plan. DOE inspectors conduct follow-up visits to verify that the enhancements have been maintained.

Adversary Forces Were Not Trained in Terrorist Tactics

Licensees used off-duty guards, guards from other licensees, and management personnel as the simulated adversary force for OSRE exercises, but these forces may not have accurately simulated the dangers of an attack. The guards on the adversary force had training only in defending the plant, not in terrorist and offensive tactics or in the use of weapons that a terrorist might have. Furthermore, plant managers participating in the drill had little or no training or experience, even in defensive tactics. Finally, some members of the adversary force could have a vested interest in having the licensee's guard force successfully defeat them in attempting simulated radiological sabotage, thereby demonstrating an adequate security program.

In contrast, DOE uses a trained, simulated composite adversary force in all of its force-on-force exercises. This force includes guards from all departmental facilities.[10] Team members are trained in offensive tactics and, according to DOE officials, have an "adversary" mind-set, which allows them to think and act like terrorists.

According to NRC officials, as part of the pilot program, they are assessing the characteristics, training, and selection of the adversary force. They said that they also have reviewed DOE's composite adversary team methods, attended DOE's adversary training school, and are assessing the DOE program's relevance to NRC activities.

Exercises Used Unrealistic Weapons

Adversary and plant defensive forces generally used rubber weapons during OSRE exercises. Although under some circumstances, such as very confined spaces, rubber weapons would be the most practical, in general, rubber weapons do not simulate actual gunfire or provide real-time experience. Licensee employees (controller judges) had to determine whether a guard or adversary member's weapon hit its intended target. This led to unrealistic exercises. For example, in one OSRE exercise, the controller judges reported that they could not determine when weapons were "fired" or if a person was hit.

DOE usually uses Multiple Integrated Laser Equipment to simulate weapon fire and provide real-time experiences. Multiple Integrated Laser Equipment consists of weapons-mounted laser transmitters and laser sensors on the guard forces and adversary team members. When a laser gun is fired and hits a target, an alarm registers the hit, thereby allowing the participants to simulate weapon fire and participate in real-time exchanges.

A few NRC OSRE exercises used Multiple Integrated Laser Equipment. According to one OSRE report, the use of laser guns provided realistic scenarios and simulated the stress of an actual engagement. Consequently, the exercise showed results that "significantly helped in evaluating the effectiveness of both the defensive strategy and the officers executing the strategies." NRC officials said that they are conducting a $1.4 million assessment of the use of Multiple Integrated Laser Equipment.

[10]DOE, Office of Independent Oversight and Performance Assurance, *Inside Oversight*, Special Edition, June 2002, 1-2.

Exercises Did Not Test the Full Extent of the Design Basis Threat

NRC never tested several aspects of the design basis threat in the OSRE exercises. As a result, NRC could not determine the plants' capability to defend against the maximum credible terrorist attack. According to the NRC official who was in charge of the OSRE program, NRC did not use and test certain adversary capabilities because the exercises would have been too rigorous, would have resulted in too many exercises in which the adversaries achieved their objectives, and thus may have resulted in the elimination of the OSRE program. The second round of OSRE exercises, begun in 2000, was originally planned to include all of the adversary capabilities. However, from the beginning of the second round of OSREs to the suspension of the program in September 2001, none of the OSREs included all adversary capabilities.

DOE tests the full adversary capabilities of the design basis threat and often goes beyond those capabilities. DOE officials believe it is important to test the licensee's security against all of the adversary capabilities so that DOE can determine how secure the facility is and what improvements are needed.

Operational Safeguards Response Evaluation Reports Were Not Timely

NRC had a program goal of issuing OSRE reports 30 to 45 days after the end of the exercise, but 46 of 76 reports (60 percent) were not issued within the required time.[11] Delays in releasing a report to the licensee may have affected the timeliness of permanent corrective actions and diminished the effectiveness of feedback on the exercise. On average, NRC issued OSRE reports to the licensees 98 days after the end of the exercises. The OSRE reports addressed any problems that needed to be corrected and specified how long the licensee had to correct the problem. NRC communicated the results of the exercise to the licensee at a closeout meeting. If a concern was severe and made the licensee vulnerable to security breaches, the licensee was required to provide temporary protection to address that concern until it implemented a permanent correction. However, the OSRE reports have specified an average of 51 days to permanently correct a concern after the report was issued. As a result, nearly 5 months elapsed between when the exercise was completed and when the report was issued and a permanent correction was required.

[11]Four of the 80 reports did not contain the information that was necessary to determine the time required to issue the report.

Federal Law Limits the Type of Weapons That Guards Can Use, and State Laws Vary on Guards' Authority to Deal with Intruders

Commercial nuclear power plants face challenges in securing their plants against intruders because federal and state laws limit security guards' ability to defend these plants. Federal law generally prohibits private ownership of automatic weapons, and there is no exemption in the law for security guards at commercial nuclear power plants.[12] As a result, no nuclear power plants use automatic weapons in their defense. However, terrorists attacking a nuclear power plant could be armed with automatic weapons or other advanced weapons. NRC officials believe that a terrorist attacking a nuclear power plant could obtain and use any weapon that can be purchased on the black market, while guards generally have to rely on semiautomatic pistols, rifles, or shotguns. As a result, guards at nuclear power plants could be at a great disadvantage in terms of firepower, if attacked.

According to NRC officials, the use of fully automatic weapons would provide an important option to plants as they make security decisions about a number of factors, such as the number of plant guards, the positioning of guards at the facilities, and the quality and capabilities of surveillance equipment. According to these officials, plants will have more options in developing the appropriate combination of security elements if guards have the authority to carry automatic weapons. NRC recognizes, however, that some plant sites face special conditions under which fully automatic weapons might not be beneficial or practicable.

[12]Automatic weapons manufactured before 1986, prior to the Firearms Owners' Protection Act (18 U.S.C. 921 et. seq.) are regulated by the National Firearms Act (26 U.S.C. 5801 et. seq.), which allows civilian ownership provided certain requirements are met. States may further restrict ownership of automatic weapons.

Commercial nuclear power plants also face security challenges because of the absence of nationwide legal authority and clear guidance on when and how guards can use deadly force in defending these plants. According to NRC's regulations,[13] a guard should use deadly force in protecting nuclear power reactors against sabotage when the guard has a reasonable belief that such force is necessary for self-defense or the defense of others. However, in general, state laws govern the use of deadly force by private sector persons, and these laws vary from state to state. For example, under New Hampshire statutes, guards may not use deadly force if they can safely retreat from the encounter.[14] In contrast, Texas statutes allow guards to use deadly force in defense of private land or property, which includes nuclear power plants, without retreating, if such action is necessary to protect against another's use of unlawful force.[15] In still other states, such as Virginia and Michigan, no state statutes specifically address the issue, and the courts decide whether deadly force was appropriate in a given situation.

NRC officials believe that guards—concerned about their right to act—might second-guess, hesitate, delay, or fail to act appropriately against an attacker, thereby increasing the risk of a successful attack on the nation's nuclear power plants. During OSRE exercises, NRC officials presented guards with various scenarios that could involve the use of deadly force. In 7 of the 80 OSRE reports we reviewed (about 9 percent) NRC found that the guards did not understand or did not properly apply its guidance on the use of deadly force.

[13]10 C.F.R. 73.55(h)(5).

[14]N.H. Rev. Stat. 627.4.

[15]TX Pen. Code, Sections 9.41-9.43.

Finally, guards at nuclear power plants do not have nationwide legal authority and clear guidance on when and how to arrest and/or detain intruders at the nation's plants. NRC officials believe that there is a question about whether federal authority can be directly granted to private security guards who are not deputized. State laws governing this authority vary. For example, in South Carolina, private security guards' authority to arrest and/or detain intruders on plant property is similar to local law enforcement officials' authority.[16] However, in most states, these guards have only the arrest authority afforded every U.S. citizen.[17]

To enable nuclear power plants to better defend against attacks, NRC has sought federal legislation that would authorize the use of deadly force to protect the plants. Legislation has not been enacted but is currently pending on arrest and detain authority.

Conclusions

NRC has taken several actions to respond to the heightened risk of attack following the September 11, 2001, terrorist attacks and, in April 2003, issued a new design basis threat that the commercial nuclear power plants must be prepared to defend against. However, NRC's past methods for ensuring that plants are taking all of the appropriate defensive measures—the annual security inspections and the force-on-force exercises—had significant weaknesses. As a result, NRC's oversight of these plants may not have provided the information necessary for NRC to ensure that the power plants were adequately defended.

In particular, NRC's past use of non-cited violations for security problems that appear to be serious is detrimental to ensuring the plants' security because NRC did not require follow-up to ensure that a non-cited violation was corrected. Lack of follow-up reduces the likelihood that needed improvements will be made. Moreover, NRC may have overstated security levels when it provided a "meeting security objectives" rating to some plants having non-cited violations that appear to have serious security implications. NRC could not have known whether some non-cited

[16]S.C. Code Section 40-18-110.

[17]Citizen's arrest authority evolved from old English law. Some states have statues specifying and clarifying citizen's arrest authority, and others rely on common law citizen's arrest authority. Generally, under common law, a private citizen may arrest another when there is probable cause to believe that the other person is committing or has committed a felony in the citizen's presence.

violations, such as guards found asleep on duty or failure to physically search for metal detected by scanners, were vulnerabilities that could have been exploited. However, accepting such vulnerabilities post-September 11, 2001, opens the power plants to undue risk. Furthermore, NRC may be missing opportunities to better oversee and improve security at the plants because it does not routinely collect, analyze, and disseminate information on security enhancements, problems, and solutions among the plants and within the agency. Such a mechanism may help other plants to improve their security.

Similarly, the force-on-force exercises were not realistic enough to ensure the identification and correction of plants' security vulnerabilities. Untrained adversary teams, temporarily enhanced defenses, and rubber weapons used in past force-on-force exercises simply do not compare with simulated attack exercises using technologically advanced tools that provide realistic, real-time experience. Furthermore, NRC was not required to conduct these exercises and has done so infrequently, thereby making plants even less prepared to address an attack. In addition, in the past, exercises have not addressed the full range of the design basis threat. Finally, delays in issuing reports on the OSRE exercises may have resulted in delays in the permanent correction of known security problems.

NRC is in the process of revising both its security inspection program and its force-on-force exercise program. What these programs will consist of when they are revised is currently unknown. NRC expects its security inspection program to be restored by 2004 and will decide the future of its force-on-force program after completing its pilot program—at a date yet to be determined. Revisions of these programs provide NRC with an opportunity to use the lessons learned from the suspended programs to strengthen them and make them more relevant to the post-September 11, 2001, environment.

Until these programs are restored, NRC is relying on plants' self-assessments and the force-on-force pilot program as its mechanisms to oversee security at the nation's nuclear power plants. The self-assessments rely on the licensees to identify problems, which then prompts NRC to conduct security inspections. Since the inspection program was curtailed in 2001, the plants have not identified any serious security problems in their self-assessments. Therefore, it is critical for NRC to revise and restore promptly its annual security inspections and force-on-force exercises to fulfill its oversight responsibilities.

Recommendations for Executive Action

To strengthen NRC's security inspection program, we recommend that the NRC Commissioners

- ensure that NRC's revised security inspection program and force-on-force exercise program are restored promptly and require that NRC regional inspectors conduct follow-up visits to verify that corrective actions have been taken when security violations, including non-cited violations, have been identified;
- ensure that NRC routinely collects, analyzes, and disseminates information on security problems, solutions, and lessons learned and shares this information with all NRC regions and licensees; and
- make force-on-force exercises a required activity and strengthen them by
  - conducting the exercises more frequently at each plant;
  - using laser equipment to ensure accurate accounts of shots fired;
  - requiring the exercises to make use of the full terrorist capabilities stated in the design basis threat, including the use of an adversary force that has been trained in terrorist tactics;
  - continuing the practice, begun in 2000, of prohibiting licensees from temporarily increasing the number of guards defending the plant and enhancing plant defenses for force-on-force exercises, or requiring that any temporary security enhancements be officially incorporated into the licensees' security plans; and
  - enforcing NRC's requirement that force-on-force exercise reports be issued within 30 to 45 days after the end of the exercise to ensure prompt correction of the problems noted.

Agency Comments and Our Evaluation

We provided a draft of this report to NRC for its review and comment. NRC stated that our report did not provide a balanced or useful perspective of its role in ensuring security at commercial nuclear power plants. NRC believed that our report was "of a historical nature," focusing on NRC's oversight of power plants before September 11, 2001, and that our report failed to reflect the changes NRC has made to its program since September

11. Furthermore, NRC commented that our characterization of non-cited violations as minimizing the significance of security problems is a serious misrepresentation. NRC said that the "anecdotal" issues noted in the draft report were "relatively minor issues" and that it treated them appropriately.

We agree that NRC has taken numerous and appropriate actions since September 11, 2001, and that additional security procedures have been, and are being, put in place to increase power plant operators' attention to enhancing security. Our draft report had discussed many of these actions, and we have added additional language to the report to more fully reflect these actions. We note that most of these actions were advisories or requirements for the licensee to enhance plant physical security and did not relate to NRC's oversight activities. With respect to NRC oversight of security at the nuclear power plants, NRC has suspended the two primary elements of its oversight program, the security inspection program and the OSRE exercises and has not yet resumed them. NRC's oversight actions since September 11 have been interim in nature; it has conducted ad hoc inspections and some force-on-force exercises as part of a pilot program. NRC said that it plans to reinstitute the security inspection and the force-on-force exercise programs in the future, but it does not now know what the revised programs will consist of. As a result, we remain convinced that it was appropriate to examine NRC's security oversight program before September 11. In the absence of any formal post-September 11 oversight program, this was the only way to systematically assess the strengths and weaknesses of NRC's oversight. Our recommendations are directed at strengthening the oversight programs and making NRC's oversight more relevant to the post-September 11 environment.

In that regard, while the NRC comments reference numerous efforts and enhancements, we note that, with one exception, these actions were designed to enhance power plant security and not to improve or enhance NRC's oversight program, which is the subject of this report. The one exception is NRC's force-on-force evaluation program, a major element in NRC's oversight program. In its comments, NRC stated that we failed to adequately reflect NRC's enhanced force-on-force evaluation program, including the increased frequency and greater degree of realism of the exercises. We disagree. NRC has not yet instituted a new force-on-force program, and our report reflects NRC's current force-on-force efforts. NRC suspended its old OSRE program after September 11, 2001, and is currently conducting pilot force-on-force exercises, which we describe in this report. NRC has not determined when a permanent program will be instituted or

what it will consist of when it is reinstituted. NRC plans to use the results of the pilot exercises to help formulate a new, permanent program.

We also disagree that the "anecdotal" issues cited in the draft report were "relatively minor issues" and do not believe that the continued extensive use of non-cited violations will achieve the best oversight. Sleeping guards, unauthorized access to protected areas, disabled alarms in the vital area, and failure to inspect visitors who set off alarms on metal detectors are all serious security problems that warrant NRC attention and oversight. NRC's belief that it should rely on the licensees to self-identify and correct these types of problems is troubling. Instead of discounting problems that are, on their face, quite worrisome, NRC should aggressively determine the root cause of the problems, formulate corrective actions, and follow up to ensure that the approved corrective actions have been implemented and that the implemented actions have corrected the problems. The use of non-cited violations delegates these activities and responsibilities to the licensees. NRC believes that such delegation is appropriate and that the use of non-cited violations contributes to an environment in which the licensee self-identifies and corrects problems, a behavior that NRC said it encourages. However, in the cases we cited, the delegation of responsibility for identifying and correcting security problems was not effective because all were security problems that the licensee failed to identify, but instead were found by NRC security inspectors.

Finally, NRC stated that its process requires it to review a sampling of the licensees' corrective actions to ensure that the licensees are implementing the corrective actions. NRC failed to note, however, that the requirement cited is part of the baseline security inspection program that was suspended after September 11, 2001, and that has not been reinstated. In addition, when NRC was conducting baseline security inspections, the program required corrective action checks only every 2 years, and the sample selected for checks included all corrective actions—safety and emergency preparedness, as well as security. As a result, NRC had no assurance that any security corrective actions would be selected for follow-up. Licensees should be involved in identifying and correcting problems. However, we believe that by delegating these functions to the licensee, NRC is abandoning its oversight responsibilities and, as a result, cannot guarantee that problems are identified and corrected.

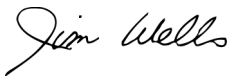
NRC did not comment on our recommendations for reinstituting and improving its baseline inspection and force-on-force exercise programs. Nevertheless, we hope that NRC decides to implement our

recommendations as it fulfills its 31 U.S.C. 720 requirement to submit a written statement of the actions taken on our recommendations. This statement is to be submitted to the Senate Committee on Governmental Affairs and the House Committee on Government Reform not later than 60 days after the date of this report's release, and to the Senate and House Committees on Appropriations with the agency's first request for appropriations made more than 60 days after that same date.

In addition to its overall comments and observations (see app. III), NRC provided a number of technical comments and clarifications, which we incorporated in this report as appropriate.

As arranged with your offices, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after the date of this letter. At that time, we will send copies of the report to interested congressional committees, the Chairman of the Nuclear Regulatory Commission, and the Director of the Office of Management and Budget. We will make copies available to others on request. In addition, this report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions about this report, please call me at (202) 512-3841 or contact me at Wellsj@gao.gov. Key contributors to this report are listed in appendix IV.



Jim Wells
Director, Natural Resources and Environment

Scope And Methodology

Our objectives were to review (1) the effectiveness of the Nuclear Regulatory Commission's (NRC) inspection program to oversee security at commercial nuclear power plants and (2) legal challenges currently affecting physical security at the power plants.

To meet these objectives, we visited NRC's Headquarters in Rockville, Maryland, and Region I in King of Prussia, Pennsylvania; obtained NRC advisories, orders, regulations, Operational Safeguards Response Evaluation (OSRE) reports, and annual security inspection reports; and interviewed officials who were knowledgeable about NRC's physical security requirements for nuclear power plants. We also visited the Limerick, Oyster Creek, and Calvert Cliffs power plants; obtained licensee documents and requirements regarding their security procedures; and interviewed licensee officials who were knowledgeable about the facilities' security plans, procedures, and NRC's nuclear power plant physical security regulations. During our visits, we observed the security measures that were put in place to reflect NRC's advisories and orders since the terrorist attacks of September 11, 2001.

To determine the extent of NRC's oversight of nuclear power plant security, we held discussions with NRC Region I security inspectors and officials in NRC's Office of Nuclear Security and Incident Response, Office of General Counsel, and Office of the Executive Director for Operations. We also held discussions with licensee officials at the Limerick, Oyster Creek, and Calvert Cliffs power plants on their security procedures and mechanisms and on their interaction with NRC security inspectors. In addition, we collected information on nuclear security from all NRC regional security offices.

To determine how NRC assesses the quality of daily security procedures and mechanisms against the licensees' security plans, we obtained and reviewed all 49 NRC inspection reports that contained a finding that was judged to be of moderate significance or higher. We also had discussions with officials in NRC's Office of Nuclear Security and Incident Response regarding the methods for conducting and reporting annual inspections and in NRC's Office of Enforcement regarding how security violations are administered.

To determine how NRC tests licensees against the design basis threat, we interviewed NRC officials to understand both the process for OSRE exercises and report writing and the follow-up procedures for any concerns found during an OSRE exercise. We also examined all OSRE reports from

each NRC licensee. We designed a data collection instrument in order to organize specific elements that were extracted from 80 OSRE reports. Two GAO analysts followed procedures to ensure the completeness of all data collection instrument entries. The data collection instrument data were entered into a spreadsheet file for analysis. To detect potential coding and keying errors, the accuracy of the data entered into the spreadsheet file was verified. We also held discussions with Department of Energy officials to (1) determine how they conduct force-on-force exercises at the department's nuclear facilities and (2) determine if there are any promising practices that might be applied to NRC's OSRE program.

To determine NRC's views on federal and state laws and on NRC institutional policies (i.e., regarding the use of automatic weapons, the authority to use deadly force, and the authority to arrest and detain) that could impact a licensee's ability to adequately secure commercial nuclear power plants, we discussed these issues with officials from NRC's Office of Nuclear Security and Incident Response and Office of General Counsel. Additionally, we discussed these same issues with industry officials who were specifically knowledgeable about these areas. We examined existing federal and state laws, and we also examined federal and state bills that have been proposed or are pending legislative passage.

U.S. Commercial Nuclear Power Plants That Are Licensed to Operate

Power plant	City	State	NRC region
Arkansas Nuclear 1	Russellville	AR	4
Arkansas Nuclear 2	Russellville	AR	4
Beaver Valley 1	McCandless	PA	1
Beaver Valley 2	McCandless	PA	1
Braidwood 1	Joilet	IL	3
Braidwood 2	Joilet	IL	3
Browns Ferry 1	Decatur	AL	2
Browns Ferry 2	Decatur	AL	2
Browns Ferry 3	Decatur	AL	2
Brunswick 1	Southport	NC	2
Brunswick 2	Southport	NC	2
Bryon 1	Rockford	IL	3
Bryon 2	Rockford	IL	3
Callaway	Fulton	MO	4
Calvert Cliffs 1	Annapolis	MD	1
Calvert Cliffs 2	Annapolis	MD	1
Catawba 1	Rock Hill	SC	2
Catawba 2	Rock Hill	SC	2
Clinton	Clinton	IL	3
Columbia Generating Station	Richland	WA	4
Comanche Peak 1	Glen Rose	TX	4
Comanche Peak 2	Glen Rose	TX	4
Cooper	Nebraska City	NE	4
Crystal River 3	Crystal River	FL	2
D C Cook 1	Benton Harbor	MI	3
D C Cook 2	Benton Harbor	MI	3
Davis-Besse	Toledo	OH	3
Diablo Canyon 1	San Luis Obispo	CA	4
Diablo Canyon 2	San Luis Obispo	CA	4
Dresden 2	Morris	IL	3
Dresden 3	Morris	IL	3
Duane Arnold	Cedar Rapids	IA	3
Edwin I. Hatch 1	Baxley	GA	2
Edwin I. Hatch 2	Baxley	GA	2
Fermi 2	Toledo	MI	3

(Continued From Previous Page)

Power plant	City	State	NRC region
Fort Calhoun	Omaha	NE	4
Ginna	Rochester	NY	1
Grand Gulf 1	Vicksburg	MS	4
H.B. Robinson 2	Florence	SC	2
Hope Creek 1	Lower Alloways Creek	NJ	1
Indian Point 2	New York	NY	1
Indian Point 3	New York	NY	1
James A. FitzPatrick	Oswego	NY	1
Joseph M. Farley 1	Dothan	AL	2
Joseph M. Farley 2	Dothan	AL	2
Kewaunee	Green Bay	WI	3
La Salle 1	Ottawa	IL	3
La Salle 2	Ottawa	IL	3
Limerick 1	Philadelphia	PA	1
Limerick 2	Philadelphia	PA	1
McGuire 1	Charlotte	NC	2
McGuire 2	Charlotte	NC	2
Millstone 2	New London	CT	1
Millstone 3	New London	CT	1
Monticello	Minneapolis	MN	3
Nine Mile Point 1	Oswego	NY	1
Nine Mile Point 2	Oswego	NY	1
North Anna 1	Richmond	VA	2
North Anna 2	Richmond	VA	2
Oconee 1	Greenville	SC	2
Oconee 2	Greenville	SC	2
Oconee 3	Greenville	SC	2
Oyster Creek	Toms River	NJ	1
Palisades	South Haven	MI	3
Palo Verde 1	Phoenix	AZ	4
Palo Verde 2	Phoenix	AZ	4
Palo Verde 3	Phoenix	AZ	4
Peach Bottom 2	Lancaster	PA	1
Peach Bottom 3	Lancaster	PA	1
Perry 1	Painesville	OH	3
Pilgrim 1	Plymouth	MA	1
Point Beach 1	Manitowoc	WI	3

(Continued From Previous Page)

Power plant	City	State	NRC region
Point Beach 2	Manitowoc	WI	3
Prairie Island 1	Minneapolis	MN	3
Prairie Island 2	Minneapolis	MN	3
Quad Cities 1	Moline	IL	3
Quad Cities 2	Moline	IL	3
River Bend 1	Baton Rouge	LA	4
Salem 1	Lower Alloways Creek	NJ	1
Salem 2	Lower Alloways Creek	NJ	1
San Onofre 2	San Clemente	CA	4
San Onofre 3	San Clemente	CA	4
Seabrook 1	Portsmouth	NH	1
Seqouyah 1	Chattanooga	TN	2
Seqouyah 2	Chattanooga	TN	2
Shearon Harris 1	Raleigh	NC	2
South Texas Project 1	Bay City	TX	4
South Texas Project 2	Bay City	TX	4
St. Lucie 1	Ft. Pierce	FL	2
St. Lucie 2	Ft. Pierce	FL	2
Summer	Columbia	SC	2
Surry 1	Newport News	VA	2
Surry 2	Newport News	VA	2
Susquehanna 1	Berwick	PA	1
Susquehanna 2	Berwick	PA	1
Three Mile Island 1	Harrisburg	PA	1
Turkey Point 3	Miami	FL	2
Turkey Point 4	Miami	FL	2
Vermont Yankee	Battleboro	VT	1
Vogtle 1	Augusta	GA	2
Vogtle 2	Augusta	GA	2
Waterford 3	New Orleans	LA	4
Watts Bar 1	Spring City	TN	2
Wolf Creek 1	Burlington	KS	4

Source: NRC.

Comments from the Nuclear Regulatory Commission

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

August 7, 2003

Mr. James Wells, Director
Natural Resources and Environment
United States General Accounting Office
441 G Street, NW
Washington, D.C. 20548

Dear Mr. Wells:

On behalf of the Nuclear Regulatory Commission (NRC), I am responding to your July 15, 2003, letter requesting the NRC's review of the draft report (GAO-03-752) entitled "Nuclear Regulatory Commission: Oversight of Security at Commercial Nuclear Power Plants Needs to be Strengthened." I appreciate the opportunity to provide comments to the General Accounting Office (GAO). I, and my fellow Commissioners, are concerned that this draft report does not provide an appropriately balanced or very useful perspective of the NRC's role in assuring nuclear power plant security.

The report, while it accurately describes some of the legal challenges that currently exist, fails to fully recognize the significant effort the NRC has made in the post-September 11, 2001, environment to strengthen what was already a very robust security program. The staff is preparing more detailed comments to address issues of correctness, currentness, and clarity. These comments will follow in a subsequent letter from the agency's Executive Director for Operations (EDO). However, I have several observations of note.

First, this report is of a historical nature, focusing almost exclusively on NRC's oversight of nuclear power plants prior to September 11, 2001. It thus fails to adequately reflect significant changes we have made to our program to meet the current challenges. These include:

- the extensive effort and direct oversight (substantially more than prior to 9/11) the NRC has provided at every nuclear plant while it revamps the security inspection program;
- a greatly enhanced personnel access authorization program through the application of new requirements and improved processes;
- enhanced training, qualification, and fitness-for-duty requirements for security forces;
- close interaction with the intelligence community that resulted in a revision to the Design Basis Threat which will require licensees to upgrade their security plans and defensive capabilities;
- an enhanced force-on-force evaluation program including increased frequency of drills and exercises and a greater degree of realism;

- significant outreach efforts to Federal, State and local organizations to improve the integrated response to an actual event; and

- extensive interactions with the Department of Homeland Security and the Homeland Security Council on security at commercial nuclear power plants. These efforts include protection of the national infrastructure as well as vulnerability assessments and mitigation strategies.

Second, the report's emphasis on non-cited violations as somehow "minimizing" the significance of security problems is a serious misrepresentation. The individual anecdotal issues noted in the report were appropriately treated within the NRC's enforcement process. NRC's regulatory process necessarily relies on licensees taking corrective actions. The use of non-cited violations contributes to an environment that fosters licensee self-identification and correction of problems, an important organizational behavior the NRC encourages. The NRC's process requires that a sampling of those corrective actions are reviewed during subsequent inspections to assure that the process is being properly implemented.

I note that the key issues you raised are relatively minor issues and had already been identified by the NRC before your review was initiated. Corrective actions for these issues either have been completed or are nearly complete.

Again, I appreciate the opportunity to comment on this draft report. As I noted earlier, the EDO will be responding soon with more detailed comments.

Sincerely,

Nils J. Diaz

GAO Contacts and Staff Acknowledgments

GAO Contacts

Andrea Wamstad Brown (202) 512-3319
Kenneth E. Lightner, Jr (202) 512-3471

Staff Acknowledgments

In addition to those named above, Jill Ann Roth Edelson, Kevin L. Jackson, William Lanouette, J. Addison Ricks, Carol Herrnstadt Shulman, and Barbara R. Timmerman made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

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

Order by Mail or Phone

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

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Public Affairs

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

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Service Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00