ENCLOSURE

NRC Response to the GAO Report
"Oversight of Security at Commercial Nuclear Power Plants
Needs to be Strengthened"
(GAO-03-752, September 2003)

1. Inspection Program

GAO View:

"Ensure that NRC's revised security inspection program . . . [is] 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." **(Recommendations, page 24)**

NRC Response:

Since September 11, 2001, the NRC has made a number of modifications, as discussed below, to its security inspection program to focus resources on verifying that licensees are adequately implementing NRC regulations and orders. These changes have continued to target key licensee program areas, such as Access Control, Access Authorization, Physical Protection and Contingency Response that are the focus of NRC orders and advisories. The focus in security inspection oversight has resulted in a significant increase in NRC inspection effort following 9/11. In FY 2000, direct inspection effort (excluding force on force exercises) of approximately 1600 hours was expended on security inspections. In FYs 2001, 2002, and 2003, the corresponding direct inspection effort was approximately 3600, 2800, and 8200 (includes order followup) hours, respectively.

NRC continues to conduct its revised security inspection program following the terrorist attacks on September 11, 2001, and to verify that effective corrective actions are being taken by licensees as appropriate. The GAO report acknowledges that NRC developed a revised security inspection procedure to validate and verify licensee compliance with all aspects of the February 2002 Order that required security enhancements at nuclear power plants (see Report, page 8). This Order required extensive enhancements to security beyond what was previously required. The NRC's followup inspections remain an essential part of ensuring that the licensees have made the necessary upgrades in their security programs. In addition, as part of the Reactor Oversight Program, the NRC's baseline inspection program remains an important element of NRC's regulation of the nuclear industry, including verification of effective corrective actions by licensees. The NRC has been developing revised and enhanced security inspection procedures and plans to implement the new inspections beginning in January 2004.

NRC actions associated with non-cited violations is addressed under Item No. 5.

2. Resumption of the Force-on-Force Exercise Program

GAO View:

"Ensure that NRC's . . . force-on-force exercise program [is] restored promptly...." **(Recommendations, page 24)**

NRC Response:

NRC resume an enhanced pilot force-on-force exercise program well before issuance of the GAO report. The GAO report acknowledges that, in January 2003, the NRC resumed force-on-force exercises at nuclear power plants under a pilot program "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" (see Report, page 7). This pilot program is being used to test new approaches toward conducting exercises and is an important step in identifying weaknesses, artificialities, and other issues to increase realism before implementation of a new formal program to replace the Operational Safeguards Response Evaluation program. This pilot program is also being used to examine the impact of the new design basis threat and to indicate whether any additional changes are necessary to the security requirements.

As a part of the larger security oversight program, the force-on-force exercises allow NRC to assess the response of the licensees' security programs to simulated attacks. Therefore, the NRC initiated the pilot program early in 2003 after improvements to the program were developed in 2002 through a series of table-top security drills at seven sites that involved licensees, as well as local, State, and Federal offsite responders. Temporarily suspending the exercises in the aftermath of September 11, 2001, was appropriate from the standpoint of 1) protecting the safety of those that participate in the exercises, and 2) allowing security resources from both the industry and NRC to focus on the implementation of the advisories and orders issued following the terrorist attacks. The 11 exercises already completed this year have yielded lessons and insights on how to further enhance the exercise program, and have helped to confirm the adequacy of measures already imposed by the NRC. In fact, since the restart of force-on-force exercises early this year, NRC has already completed more exercises than were conducted in any previous year in the former Operational Safeguards Response Evaluation program (10 in 2000).

The NRC will continue to build enhancements into the pilot program and test new enhancements as we prepare to conduct about 21 force-on-force exercises in FY2004. The "pilot" designation of the enhanced force-on-force exercise program will be dropped in October 2004 to logically align with the effective date of the revised design basis threat. Our intent is that the last several exercises in FY 2004 in the pilot program will be identical in format and methodology with the exercises to be conducted in FY 2005. Moreover, the NRC has required licensees to conduct force-on-force exercises on their own at least annually. Other substantial training enhancements, details of which are safeguards information, have been directed by the Commission in an April 2003 Order. In the interim, the NRC intends to continue to refine the process for assessing licensee security and safety performance through the force-on-force exercises. The NRC has committed to

Congress, the Administration, and the American public to conduct the exercises in the enhanced program at least once every three years at each power reactor site, substantially more frequently than the once every eight years the exercises were conducted before the terrorist attacks.

3. Weaknesses in the Force-on-Force Exercises

GAO View:

GAO identified several weaknesses in the force-on-force exercises conducted by the NRC prior to September 11, 2001, including inadequate training of attacking forces, unrealistic weapons, and other artificialities.

NRC Response:

The NRC initiated the force-on-force pilot program in January 2003, well in advance of GAO's release of its report, specifically to enhance the realism and value of the exercises and reduce the artificialities that NRC staff had previously identified. In the pilot exercises, the mock adversary forces are composed of trained security force members or law enforcement officials, who are advised by knowledgeable NRC contractors with extensive experience in terrorist tactics. As a result of the 11 exercises conducted thus far, the NRC staff has identified options for improving both the mock adversary forces and the exercise controllers. Through the pilot program, the NRC and industry have been implementing a number of other enhancements to make the exercises more realistic, including:

- Initiating attacks from within the Owner Controlled Area rather than at the Protected Area barrier;

- Using Multiple Integrated Laser Engagement System (MILES) gear to enhance the realism of the weapons and combat;

- Improving adversary preparation for the attacks with enhanced access to insiders;

- Enhancing training of exercise controllers to ensure the safety and objectivity of the exercises, while reducing artificialities; and

- Including emergency preparedness and operations staff in the exercises to provide a more realistic evaluation of licensee response.

In response to the concern that the exercises should be conducted more frequently, it is important to point out that NRC had already decided to increase the frequency of the force-on-force exercises conducted by NRC to at least once every 3 years (compared to a former baseline of once every 8 years). In addition, as part of the order requiring enhancements to security force training and qualifications, NRC has already required licensees to periodically conduct their own exercises to improve qualifications and readiness. In the pilot program, the adversaries represent a more complete range of

enhanced adversary characteristics based on the revised design basis threat, to the extent simulated attacks can be safely carried out.

4. Disallowing Supplementation of Security Force Personnel

GAO View:

The GAO expressed concern that NRC needs to prohibit 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. **(Recommendations, page 24)**

NRC Response:

As previously noted in NRC's letter to Mr. James Wells, GAO, dated August 15, 2003, NRC disallowed supplementation of security forces during exercises prior to September 11, 2001, in a November 17, 2000, memorandum. This prohibition continues in the current force-on-force pilot program. With respect to enhancing licensee security plans, in April 2003 NRC required that security plans, contingency plans, and training and qualification plans for power reactors be upgraded to provide protection against the revised design basis threat, well in advance of GAO's report.

5. Minimizing the Significance of Security Problems

GAO View:

"NRC inspectors often used a process that minimized the significance of security problems found in annual inspections by classifying them as 'non-cited violations' . . . 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. . . 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." (from the highlights at the beginning of the report and **Results in Brief**, page 2)

"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" (see Report, page 11). "Examples included a sleeping guard, falsification of security patrol logs, failure to physically search an individual, and the disabling of tamper alarms on an access door to a vital area" (see Report, page 12).

"[B]ecause of NRC's extensive use of non-cited violations, the performance rating may not always accurately represent the security level of the plant." (see Report, page 13)

"[W]e 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." (see Report, page 26)

NRC Response:

As previously noted in NRC's August 7, 2003, letter to Mr. James Wells, GAO, 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. Non-cited violations are a part of all the inspection programs in the NRC, not just those involving security.

The NRC requires power reactor licensees to enter the finding in their corrective action program; furthermore, the NRC's process requires that a sampling of those corrective actions are reviewed by NRC inspectors during subsequent inspections to ensure that the process is being properly implemented.

With respect to the examples of non-cited violations noted by GAO, the report portrayed the incidents as significant without providing a complete accounting of the evidence surrounding the findings. For example, in the specific incidence of a security force member found sleeping on the job cited in the report, the licensee took disciplinary action against the employee and retrained others involved. The licensee investigated the incident and found that overtime hours had contributed to the situation, took steps to relieve the strain on the security force, and met with employees to re-emphasize the importance of remaining attentive while on-duty. The NRC has remained aware of the progress at this plant. As a general matter, NRC also addressed the impact of overtime hours and fatigue on security force performance by imposing work hour controls in Orders issued in April 2003.

In another instance cited by GAO, NRC inspectors observed that a security officer falsified information in security logs. In this instance, the licensee also took disciplinary action, shared appropriate information about the incident with other licensees through the industry-wide Personnel Access Data System, and met with members of the security organization to remind them of the importance of accurate record-keeping. Consequently, in both cases, the licensee took appropriate action without NRC resorting to enforcement action to accomplish the desired outcomes.

6. Analyzing and Sharing the Results of Security Inspections:

GAO View:

"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." (see Report, page 3)

NRC Response:

Instead of one comprehensive system to collect, analyze, disseminate all information related to security issues, the NRC maintains several interfacing systems that effectively perform these functions. Due to the subject matter, these sources often contain sensitive and/or classified information and therefore require special handling so that the process of

sharing and analyzing does not risk unauthorized disclosure. It is also important to note that the findings represent a diverse range of licensees, and are often processed by a diverse range of experts within the NRC, such that information collected on one type of licensee may not be relevant to other types of licensees.

The information collected and analyzed by the NRC is provided by the inspection process, licensees via periodic reports, licensee representative and member organizations, and also from other sources such as Federal agencies, Federal, State and local law enforcement organizations, and certain international organizations. This information is carefully analyzed and prioritized for appropriate internal and external dissemination, and generic communications pertaining to lessons learned are developed and issued to licensees, as appropriate. To ensure that NRC staff with responsibilities in this area are kept informed of issues, there are multiple means of discussing and disseminating this information internal to the NRC, including weekly NRC senior management meetings, frequent conference calls between headquarters and security staffs in NRC regional offices, annual security counterpart conferences, and working group meetings dealing with specific security issues. To ensure that licensees and other external stakeholders are kept aware of the issues, the NRC uses various generic communications to licensees, e.g., Bulletins, Information Notices, Regulatory Issues Summaries and, when necessary, Orders. Furthermore, the NRC makes use of industry workshops, industry conferences, a recent protected web server and meetings such as the annual Regulatory Information Conference to disseminate guidance and information.

7. General

GAO View:

"While we agree that NRC has taken many actions since September 11, [2001], we note that most of these actions related to enhancing security at the plants and did not relate to NRC's oversight efforts."

NRC Response:

Contrary to GAO's statement, the NRC has taken substantial action to enhance NRC's oversight efforts for security at nuclear power reactors, including:

1. Conducting the pilot force-on-force exercise program and table-top drills to enhance the realism of these evaluations and assess the impacts of the security enhancements and changes in adversary characteristics;

2. Imposing security enhancements through Orders in February 2002, January 2003, and April 2003 that address general enhancements, access authorization, training and qualification, security force fatigue, and upgrades to reflect the revised design basis threat;

3. Conducting a revised inspection program to confirm effective implementation of the February 2002 security requirements

4. Advising licensees to report suspicious incidents, including flyovers, for prompt assessment of actionable threats and coordination with law enforcement agencies and the Department of Homeland Security;

5. Coordinating with other Federal agencies to enhance confirmation of the reliability and trustworthiness of licensee employees with unescorted access to protected areas or safeguards information;

6. Consolidating and streamlining NRC's security, safeguards, and incident response programs into a new Office of Nuclear Security and Incident Response;

7. Establishing a new Deputy Executive Director for Homeland Protection and Preparedness to provide oversight of cross-cutting functions within the NRC staff;

8. Developing a new baseline inspection program;

9. Recruiting, hiring, and training additional security experts to conduct inspections, licensing reviews, threat assessment, and related functions; and

10. Seeking legislative changes to ensure that security force personnel at licensed facilities have the necessary authority to effectively perform their duties in an elevated threat environment.