

July 1, 2008

The Honorable Barbara Boxer
Chairman, Committee on Environment
and Public Works
United States Senate
Washington, D.C. 20510

Dear Madam Chairman:

Chapter 14, Section 170D, of the Atomic Energy Act of 1954 (42 U.S.C. 2201 et seq.), as amended by the Energy Policy Act of 2005, requires the U.S. Nuclear Regulatory Commission (NRC) to submit an annual report to Congress, classified form and unclassified form, that describes the results of each security response evaluation (i.e., force-on-force (FOF) inspections) conducted and any relevant corrective action taken by a licensee during the previous year. On behalf of the Commission, I am transmitting the report for calendar year 2007. I am also providing additional information regarding the overall security and safeguards performance of the commercial nuclear power industry and Category I fuel cycle facilities to keep you informed of the NRC's efforts to protect a key segment of our Nation's electric power infrastructure and strategic special nuclear material against terrorist attacks. The Safeguards Information version of this report will be transmitted under separate cover.

The NRC is committed to protecting the public health and safety, promoting the common defense and security, and protecting the environment. Conducting FOF exercises and implementing the security inspection program are just two of a number of regulatory oversight activities the NRC performs to ensure the secure use and management of radioactive materials by the commercial nuclear industry.

During calendar year 2007, the NRC conducted 199 security inspections at nuclear power plants (of which 22 were FOF inspections). These inspections identified 122 findings, of which 117 were of very low security significance and 5 were of low-to-moderate security significance. The results of the security inspections conducted at Category I fuel cycle facilities are discussed in the Safeguards Information version of this report. Whenever a finding is identified during a security inspection, the NRC ensures that the licensee implements adequate compensatory measures immediately to correct the problem. Compensatory measures can be, for example, additional armed personnel and/or physical barriers to strengthen a licensee's response capabilities. Compensatory measures are usually effective short-term fixes until a more comprehensive analysis can be conducted to identify long-term permanent solutions.

As stated in prior reports, the NRC staff communicated FOF inspection results to Congressional, State, and local stakeholders when a licensee did not demonstrate an effective protective strategy; beginning in 2008, the staff revised the procedures to inform the appropriate Congressional, State, and local stakeholders of all FOF inspection results regardless of exercise outcome. The NRC makes available for any member of Congress or Congressional oversight committee staff the unclassified and classified reports, as appropriate, for any FOF inspection in their State or Congressional District through the Office of Congressional Affairs. The same offer will be extended, as appropriate under existing protocols and requirements, to governor-appointed State Liaison Officers. Also in 2008, the NRC staff began to engage public

stakeholders to explore means to increase the timely availability of security performance information while appropriately protecting site vulnerability information that would be useful to adversaries.

The Commission is confident that nuclear power plants and Category I fuel cycle facilities continue to be among the best protected private sector facilities in the Nation, and through our inspection and oversight processes, the NRC is committed to ensuring strong security at these facilities. Please do not hesitate to contact me if you need additional information.

Sincerely,

/RA/

Dale E. Klein

Enclosure: As stated

cc: Senator James M. Inhofe

Identical letter sent to:

The Honorable Barbara Boxer
Chairman, Committee on Environment
and Public Works
United States Senate
Washington, D.C. 20510
cc: Senator James M. Inhofe

The Honorable John D. Dingell
Chairman, Committee on Energy
and Commerce
United States House of Representatives
Washington, D.C. 20515
cc: Representative Joe Barton

Report to Congress on the Security Inspection Program for Commercial Power Reactor and Category I Fuel Cycle Facilities: Results and Status Update

Annual Report for Calendar Year 2007

Manuscript Completed: July 2008
Date Published: July 2008

Office of Nuclear Security and Incident Response
U.S. Nuclear Regulatory Commission

PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This report fulfills the requirements of Chapter 14, Section 170D, of the Atomic Energy Act of 1954 (42 U.S.C. 2201 et seq.), as amended by the Energy Policy Act of 2005, which states that “not less often than once each year, the Commission shall submit to the Committee on Environment and Public Works of the Senate and the Committee on Energy and Commerce of the House of Representatives a report, in classified form and unclassified form, that describes the results of each security response evaluation conducted and any relevant corrective action taken by a licensee during the previous year.” This report covers calendar year 2007. In addition to information on the security response evaluation program (force-on-force inspections), the NRC is providing additional information regarding the overall security performance of the commercial nuclear power industry and Category I fuel cycle facilities to keep Congress and the public informed of the NRC’s efforts to protect the Nation’s electric power infrastructure and strategic special nuclear material (SSNM) against terrorist attacks.

Paperwork Reduction Act Statement

This NUREG does not contain information collection requirements and, therefore, is not subject to the requirements of the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.).

Public Protection Notification

The NRC may not conduct or sponsor, and a person is not required to respond to, a request for information or an information collection requirement unless the requesting document displays a currently valid OMB control number.

PAGE INTENTIONALLY LEFT BLANK

CONTENTS

| | |
|--|-----|
| ABSTRACT | iii |
| CONTENTS | v |
| EXECUTIVE SUMMARY | vii |
| ABBREVIATIONS | ix |
| 1. INTRODUCTION..... | 1 |
| 2. REACTOR SECURITY OVERSIGHT PROCESS..... | 3 |
| 2.1 Overview | 3 |
| 2.2 Significance Determination Process..... | 5 |
| 2.3 Findings and Violations..... | 6 |
| 3. FORCE-ON-FORCE INSPECTION PROGRAM..... | 7 |
| 3.1 Overview | 7 |
| 3.2 Program Activities in 2007..... | 7 |
| 3.3 Results of Inspections | 8 |
| 3.4 Discussion of Corrective Actions..... | 10 |
| 3.5 Future Planned Activities..... | 10 |
| 4. SECURITY BASELINE INSPECTION PROGRAM..... | 11 |
| 4.1 Overview | 11 |
| 4.2 Results of Inspections | 11 |
| 5. OVERALL REACTOR SECURITY ASSESSMENT | 13 |
| 5.1 Overview | 13 |
| 5.2 Performance Indicators | 13 |
| 5.3 Security Cornerstone Action Matrix..... | 13 |
| 6. CAT I FACILITY OVERSIGHT PROGRAM | 15 |
| 6.1 Overview | 15 |
| 6.2 Results of Inspections | 15 |
| 7. STAKEHOLDER COMMUNICATIONS..... | 17 |
| 7.1 Communications with Public and Industry..... | 17 |
| 7.2 Communications with Local, State, and Federal Agencies | 18 |
| 7.3 Openness Initiative..... | 18 |

List of Figures

| | |
|--|----|
| Figure 1: Cornerstones of the Reactor Oversight Process..... | 3 |
| Figure 2: Inspectable areas of the Security Cornerstone..... | 5 |
| Figure 3: Summary of First Cycle of FOF Inspection Findings at NPPs..... | 9 |
| Figure 4: Summary of CY 2007 Security Inspection Findings at NPPs..... | 12 |

List of Tables

| | |
|--|----|
| Table 1: CY 2007 FOF Inspection Program Summary at NPPs..... | 8 |
| Table 2: Cumulative FOF Inspection Program Results at NPPs..... | 9 |
| Table 3: CY 2007 Security Inspections (Without FOF)..... | 12 |
| Table 4: CY 2007 Security Inspection Findings (Without FOF)..... | 12 |
| Table 5: Summary of Security Action Matrix..... | 14 |

EXECUTIVE SUMMARY

This report fulfills the requirements of Chapter 14, Section 170D, of the Atomic Energy Act of 1954 (42 U.S.C. 2201 et seq.), as amended by the Energy Policy Act of 2005, which states that “not less often than once each year, the Commission shall submit to the Committee on Environment and Public Works of the Senate and the Committee on Energy and Commerce of the House of Representatives a report, in classified form and unclassified form, that describes the results of each security response evaluation conducted and any relevant corrective action taken by a licensee during the previous year.” This is the third annual report, which covers calendar year (CY) 2007. In addition to information on the security response evaluation program (force-on-force (FOF) inspections), the U.S. Nuclear Regulatory Commission (NRC) is providing additional information regarding the overall security performance of the commercial nuclear power industry to keep Congress and the public informed of the NRC’s efforts to protect the Nation’s electric power infrastructure and special nuclear material (SNM) against terrorist attacks.

The NRC is committed to protecting public health and safety, promoting the common defense and security, and protecting the environment. Conducting FOF exercises and implementing the security inspection program are just two of a number of regulatory oversight activities the NRC performs to ensure the secure use and management of radioactive materials by the commercial nuclear industry. In support of these activities, the NRC employs relevant intelligence information and vulnerability analyses to determine realistic and practical security requirements and mitigative strategies. Further, a risk informed, graded approach is used to establish appropriate regulatory controls, enhance NRC inspection efforts, assess the significance of issues, and influence timely and effective corrective action by licensees of commercial nuclear power plants for identified deficiencies. These practices use interagency cooperation to develop an integrated approach to the security of nuclear facilities and contribute to NRC’s comprehensive evaluation of licensee security performance.

This report describes the results of the NRC’s security inspection program, including the nuclear reactor security baseline inspection program and exercises conducted as part of FOF inspections. The reporting period included herein is January 1, 2007, through December 31, 2007.

During CY 2007, the NRC conducted 199 security inspections at nuclear power plants (of which 22 were FOF inspections). These inspections identified 122 findings of which 117 were of very low security significance and 5 were of low to moderate security significance. The results of the security inspections conducted at CAT I fuel cycle facilities are discussed in the Safeguards Information version of this report.

PAGE INTENTIONALLY LEFT BLANK

ABBREVIATIONS

| | |
|-------|--|
| ASM | additional security measure |
| BWXT | BWX Technologies |
| CAF | composite adversary force |
| CAT I | Category I |
| CY | Calendar Year |
| DBT | design basis threat |
| DOD | Department of Defense |
| DOE | Department of Energy |
| EPA | Energy Policy Act |
| FOF | force-on-force |
| HEU | highly-enriched uranium |
| IDS | intrusion detection system |
| MC&A | material control and accounting |
| MILES | Multiple Integrated Laser Engagement System |
| NCV | non-cited violation |
| NFS | Nuclear Fuel Services |
| NPP | nuclear power plant |
| NR | Office of Naval Reactors |
| NRC | U.S. Nuclear Regulatory Commission |
| OCA | owner controlled area |
| PA | protected area |
| PI | performance indicator |
| PPSDP | Physical Protection Significance Determination Process |
| ROP | reactor oversight process |
| SDP | significance determination process |
| SL | severity level |
| SNM | special nuclear material |
| SSNM | strategic special nuclear material |
| URI | unresolved item |

PAGE INTENTIONALLY LEFT BLANK

1. INTRODUCTION

The Energy Policy Act of 2005 amended Chapter 14, Section 170D, of the Atomic Energy Act to require, in part, that “not less often than once each year, the Commission shall submit to the Committee on Environment and Public Works of the Senate and the Committee on Energy and Commerce of the House of Representatives a report, in classified form and unclassified form, that describes the results of each security response evaluation conducted and any relevant corrective action taken by a licensee during the previous year.” This report fulfills the requirement for an unclassified report.

The U.S. Nuclear Regulatory Commission (NRC) is providing to Congress the third annual report on the results of the NRC’s security inspection program. This report for calendar year (CY) 2007 conveys the results of inspections for the reporting period. For background information, including a description of the evolution of the NRC’s security inspection program, please refer to Appendix A to last year’s “Report to Congress on the Security Inspection Program for Commercial Power Reactor and Category I Fuel Cycle Facilities: Results and Status Update” (NUREG-1885, Vol. 1).

This report provides an overview of the NRC’s security inspection program and force-on-force (FOF) program and summaries of the results of those inspections. NRC’s communications and outreach activities with the public and other stakeholders (including other Federal agencies) will also be described. Unless otherwise noted, this report does not include security activities or initiatives of any class of licensee other than power reactors or Category I fuel cycle facilities. Category I fuel cycle facilities are those which use or possess formula quantities of strategic special nuclear material (SSNM). SSNM is defined in 10 CFR 74.4 as uranium-235 (contained in uranium enriched to 20 percent or more in the uranium-235 isotope), uranium-233, or plutonium.

PAGE INTENTIONALLY LEFT BLANK

2. REACTOR SECURITY OVERSIGHT PROCESS

2.1 Overview

The NRC continues to implement the Reactor Oversight Process (ROP), which is the agency's program for ensuring plant safety, radiological safety, security, and emergency preparedness at operating nuclear power plants. The basic principles and philosophy of the ROP are to ensure that a defined, repeatable, and objective process is applied to identify findings, determine their significance, and document results in accordance with ROP program guidance. Program instructions and inspection procedures help provide assurance that licensee actions and regulatory response are commensurate with the safety or security significance of the particular event, deficiency, or weakness. Within each ROP cornerstone (see Figure 1), NRC resident inspectors, headquarters, and regional inspectors conduct NRC inspections using detailed inspection procedures. Based on the results of those inspections, appropriate regional and headquarters' project, technical, and management staff conduct reviews of the inspection findings to determine the final significance of the findings and ensure consistent application of the NRC enforcement process. Since 9/11, the security cornerstone assessment process was separated from the other cornerstone assessment process for information protection. The conduct of all inspections, identification of findings, final review and determination of significance of findings, contribute to an assessment of licensee performance within each of these two assessment processes.

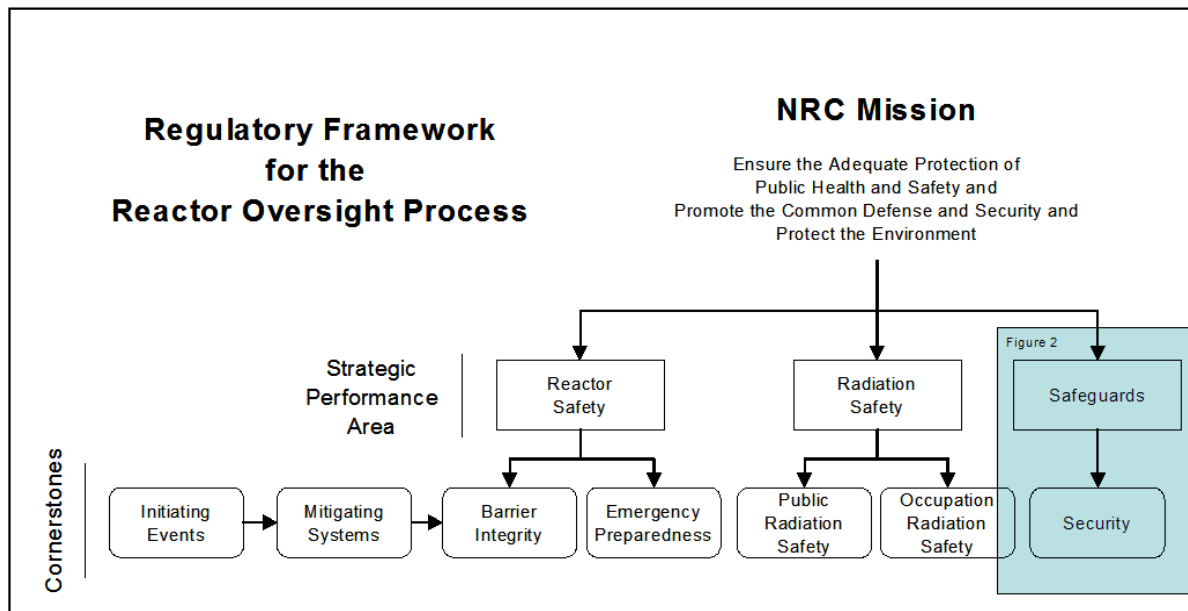


Figure 1: Cornerstones of the Reactor Oversight Process

As part of post 9/11 actions, the NRC issued a number of Orders requiring licensees to strengthen security programs in a number of areas. Based on those Orders, the NRC significantly enhanced its baseline security inspection program for commercial nuclear power plants (NPP). This inspection effort resides within the "security cornerstone" of the agency's ROP. The security cornerstone focuses on the following five key licensee performance attributes: access authorization, access control, physical protection systems, material control and accounting (MC&A), and response to contingency events. Through the results obtained from all oversight activities, including baseline security inspections and performance indicators (PI), the NRC determines whether licensees comply with requirements and can provide high

assurance of adequate protection against the design basis threat (DBT) for radiological sabotage.

The security cornerstone's baseline inspection program has the following four objectives: (1) to obtain information providing objective evidence that the security and safeguards at NRC-licensed NPPs are maintained in a manner that contributes to public health and safety and promotes the common defense and security; (2) to determine that licensees have established measures to deter, detect, and protect against the DBT of radiological sabotage as required by regulations and other Commission mandates such as orders; (3) to determine the causes of declining performance in the physical protection arena before such performance reaches a level that may result in a degradation to reactor safety or undue risk to public health and safety; and (4) to identify those significant issues that may have generic or cross-cutting applicability. These objectives help to ensure the secure use and management of radioactive materials.

During 2007, licensees reported data on the following three PIs in security: (1) Protected Area Security Performance Index, (2) Personnel Screening Program, and (3) Fitness-for-Duty/Personnel Screening Program. The data reported by the licensees was compared to an established set of thresholds to determine their significance, which is represented by the colors green, white, yellow, and red (in order of increasing severity). Before 2004, the PIs measured aspects of the licensees' security programs that were not specifically inspected by the NRC's baseline inspection program. However, with the enhanced security inspection program issued in 2004, the NRC now inspects all the aspects of licensees' security programs that the PIs measured. In December 2007, the NRC informed power reactor licensees that they no longer need to report two of the three PIs. The Protected Area Security Performance Index was retained as it also promotes good maintenance practices for security barriers.

The security cornerstone's baseline inspection program is comprised of 11 "inspectable areas" to be reviewed periodically at each power reactor facility (see Figure 2). Three of the inspectable areas (Information Technology Security, Material Control and Accounting, and Irradiated Fuel Transportation) are under development and will be included in the inspection program at a later date. One of the inspectable areas, contingency response, is assessed through the conduct of FOF inspections, which are described in detail in the next section. In addition, each NPP and CAT I licensee received a comprehensive MC&A inspection during the CY 2006 to CY 2007 time period. In the future, MC&A inspections will be conducted on a routine basis to ensure that licensees take adequate measures to control the risk of loss, theft, or diversion of SNM. Material Control and Accounting and Physical Protection of Shipments of Spent Nuclear Fuel inspections are conducted by using interim guidance. Information Security Technology interim inspection guidance is pending development.

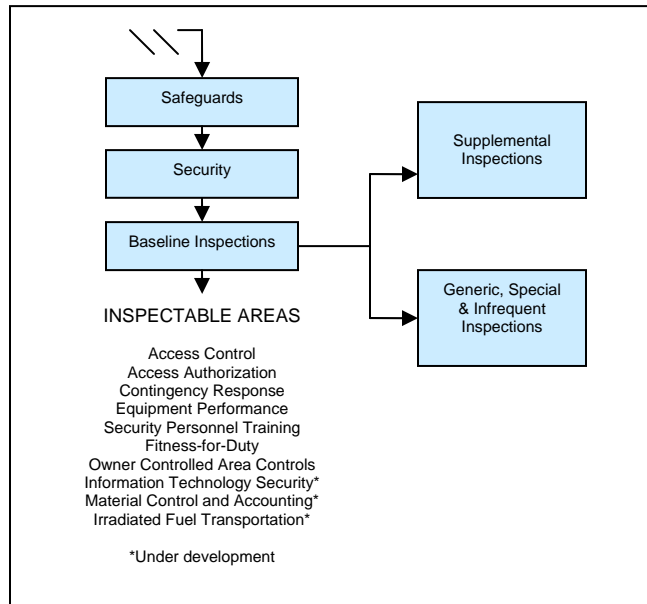


Figure 2: Inspectable areas of the Security Cornerstone

Where performance issues have been identified at a particular licensee, supplemental inspections may be conducted to investigate a particular deficiency or weakness that exceeds a certain level of significance. In certain situations, the NRC may conduct generic, special, or infrequent inspections. Such inspections are not part of the baseline or supplemental inspection program and would only be conducted after a review and assessment of a particular security or safeguards event or condition. These types of inspections include, but are not limited to, resolution of employee concerns, security matters requiring particular focus, and licensee plans for coping with security force strike or walkout. During this reporting period, there were seven reactive inspections at NPPs, including both special and augmented inspections. These reactive inspections covered topics such as inattentive security officers, inadequate searches of packages and material, and testing and maintenance of intrusion detection systems.

2.2 Significance Determination Process

The Significance Determination Process (SDP) for NPPs uses risk insights, where appropriate, to help NRC inspectors and staff determine the significance of inspection findings. Security-related findings are evaluated using the baseline Physical Protection Significance Determination Process (PPSDP). These findings include both programmatic and process deficiencies. The PPSDP provides the security significance of any security program deficiency. If it is unclear whether or not an observation is a finding, it will be documented in the inspection report as an unresolved item (URI) until clarifying information can be gathered. A URI is an issue requiring additional information to determine acceptability, if it is a finding, or if it constitutes a deviation or violation. Such a matter may require additional information from the licensee or may require additional guidance or clarification/interpretation of the existing guidance.

FOF findings are evaluated using the FOF PPSDP. The significance of findings associated with FOF adversary actions is dependent on the impact of the critical equipment (referred to as a target set) and a determination of whether or not these actions could have had an adverse impact on public health and safety. Other security-related findings identified during FOF activities are also evaluated using the baseline PPSDP. These findings may include programmatic and process deficiencies that are not directly related to an FOF inspection

outcome, but are identified during the FOF exercise. In situations where the NRC cannot clearly determine the outcome of an exercise, the exercise will be considered indeterminate, and an additional exercise will be conducted if appropriate.

2.3 Findings and Violations

Inspection findings typically document the identification of violations and non-cited violations (NCV) of NRC requirements, and they are categorized by significance. Inspection findings are assigned colors as follows: green (very low security significance), would normally be described in inspection reports as NCVs, white (low to moderate security significance), yellow (substantial security significance), and red (high security significance) potentially will be cited as a Notice of Violation requiring a written response by the licensee unless sufficient information has been provided to the NRC. The Commission uses its discretion for particularly significant violations to impose civil penalties in accordance with Section 2.34 of the Atomic Energy Act of 1954, as amended. White, yellow, and red findings are considered greater than green.

All CAT I fuel cycle facilities' inspection findings and those findings at commercial power reactor facilities resulting in violations that have willful aspects, potential or actual safety consequences, or potential impact on the NRC's ability to perform its regulatory function are not evaluated through the SDP and dispositioned through the traditional enforcement process. These violations are categorized in terms of four levels of severity to show their relative importance or significance. Severity Level (SL) I has been assigned to violations that are the most significant. SL I and II violations are of very significant regulatory concern. In general, violations that are included in these severity categories involve actual or high potential consequences on public health and safety. SL III violations are cause for significant regulatory concern. SL IV violations are less serious but are of more than minor concern. Violations at SL IV involve noncompliance with NRC requirements that are not considered significant based on a security risk.

3. FORCE-ON-FORCE INSPECTION PROGRAM

3.1 Overview

An FOF inspection, which is typically conducted over the course of 2 weeks, includes both table-top drills and exercises that simulate combat between a mock commando-type adversary force and the licensee security force. At a nuclear power plant, the adversary force attempts to reach and damage key safety systems and components that protect the reactor's core or the spent fuel pool, potentially causing a radioactive release to the environment. At other facilities the adversary force may attempt theft or diversion of SNM. The licensee's security force, in turn, interposes itself to prevent the adversaries from causing such a release. In addition to significant participation of plant operators and NRC personnel, these exercises may include observers from an array of Federal, State, and local law enforcement agencies and emergency planning officials.

In conducting FOF inspections, the NRC notifies the licensee in advance for operational and personnel safety and logistical purposes. This notification provides adequate planning time for licensee coordination of two sets of security officers - one for maintaining actual plant security and the other for participating in the exercise. In addition, arrangements must be made by the licensee for a group of individuals who will control and monitor each exercise. A key goal of the NRC is to balance personnel and plant safety with maintaining actual plant security during an exercise that is as realistic as possible.

In preparation for an FOF exercise, information from table-top drills, which probe for potential deficiencies in the licensee's protective strategy, are factored into a number of commando-style attack scenarios. Other information that may be factored into an FOF inspection could include security baseline inspection results and security plan reviews. Any potential deficiencies in the protective strategy identified during FOF exercises are promptly reviewed and corrected before NRC inspectors leave the licensee's site.¹

3.2 Program Activities in 2007

In 2007, the FOF inspection program continued to focus on effectively evaluating licensee protective strategies while maintaining regulatory stability and consistency in the evaluation process. The staff continued to work with the nuclear industry to improve the standards of training and qualifications for exercise controllers. In 2007, the staff endorsed the industry's revised controller guidance document. The NRC remains committed to working with the industry to improve the realism and effectiveness of the FOF inspection program and will continue to pursue methods to improve certain exercise simulations and the controller responses to those simulations.

The composite adversary force (CAF) used for NPP inspections continued to meet expectations for a credible, well-trained, and consistent mock adversary force. NRC FOF team members provide necessary monitoring of information to assist the CAF in defining and developing mission plans used during FOF exercises. Additionally, FOF team members review CAF team briefings to ensure that the information provided in the briefings accurately reflect established parameters.

¹ See "Protecting Our Nation," and Office of Public Affairs "Backgrounder" on Force-on-Force. <http://www.nrc.gov/reading-rm/doc-collections/nuregs/brochures/br0314/>

3.3 Results of Inspections

Between January 1, 2007, and December 31, 2007, FOF inspections were conducted at 22 commercial NPPs. During the conduct of FOF inspections, three findings related to other areas of the security baseline program were identified: failure to evaluate adequately the effectiveness of a change to the Physical Security Plan, failure to include specific attributes in the firearms tactical qualification course, and failure to implement the requirements for a vehicle barrier system.

There were two findings related to the conduct of FOF inspections at two separate sites. Each finding was due to the failure of licensee armed security personnel to interpose themselves between the mock adversary and the vital areas and target set components. Each licensee implemented immediate compensatory measures followed by long-term corrective actions. Through weekly communications with each licensee, the NRC tracked the progress of the long-term corrective actions. In both cases, NRC inspectors observed additional exercises at the sites and verified the adequacy of the corrective actions.

As of the end of 2007, the first cycle of NPP FOF inspections was completed (64 sites). Table 1 below summarizes the 22 inspections conducted at NPPs in CY 2007. Details on the results of the inspections conducted at the CAT I fuel cycle facilities are discussed in the sensitive unclassified version of this report.

| | |
|----|---|
| 22 | Total number of inspections conducted |
| 5 | Total number of inspection findings |
| 2 | Total number of Green findings |
| 2 | Total number of greater than Green findings |
| 1 | Total number of SL IV violations |
| 0 | Total number of greater than SL IV violations |

Table 2 below summarizes the cumulative results of the FOF inspections conducted at NPPs since the first 3-year cycle began in November 2004, while Figure 3 provides a visual summary of the complete first cycle. As of December 31, 2007, which was the end of the first cycle, inspections were conducted at all commercial NPPs. During an FOF inspection, three FOF exercises are scheduled. If an exercise is canceled due to severe weather or other reasons, NRC management may consider less than three exercises to satisfy inspection requirements only when a licensee has successfully demonstrated an effective strategy in at least two exercises with no significant issues identified. If those conditions are not met, the team may have to expand the schedule or schedule a subsequent exercise. The two greater than Green findings identified in Table 2 below does not constitute an industry trend for the first 3-year FOF cycle.

| Table 2: Cumulative FOF Inspection Program Results at NPPs (November 2004 through December 2007) | |
|---|--|
| 66 | Total number of inspections conducted |
| 64 | Total number of inspection sites |
| 172 | Total number of exercises conducted |
| 2 | Total number of times a complete target set damaged or destroyed (simulated) |
| 10 | Total number of inspection findings |
| 6 | Total number of Green findings |
| 2 | Total number of greater than Green findings ² |
| 2 | Total number of SL IV violations |
| 0 | Total number of greater than SL IV violations |

Of the total number of exercises conducted, five exercises were inconclusive and deemed indeterminate. An indeterminate exercise is one where the NRC inspectors are unable to gather sufficient information to evaluate the licensee's protective strategy or to form a cogent conclusion. These exercises were indeterminate due to insufficient exercise control and/or administrative holds. Another six exercises were canceled because of potential safety concerns associated with dangerous weather conditions or a plant operational or safety issue. If an exercise is deemed indeterminate or is canceled due to severe weather or operational issues, the staff will make the determination when less than three exercises are acceptable. This determination will be contingent upon: (1) at least two exercises having been conducted, (2) both exercises having successfully demonstrated an effective protective strategy, and (3) no significant issues being identified. If those conditions are not met, the team may have to expand the schedule or schedule a subsequent visit.

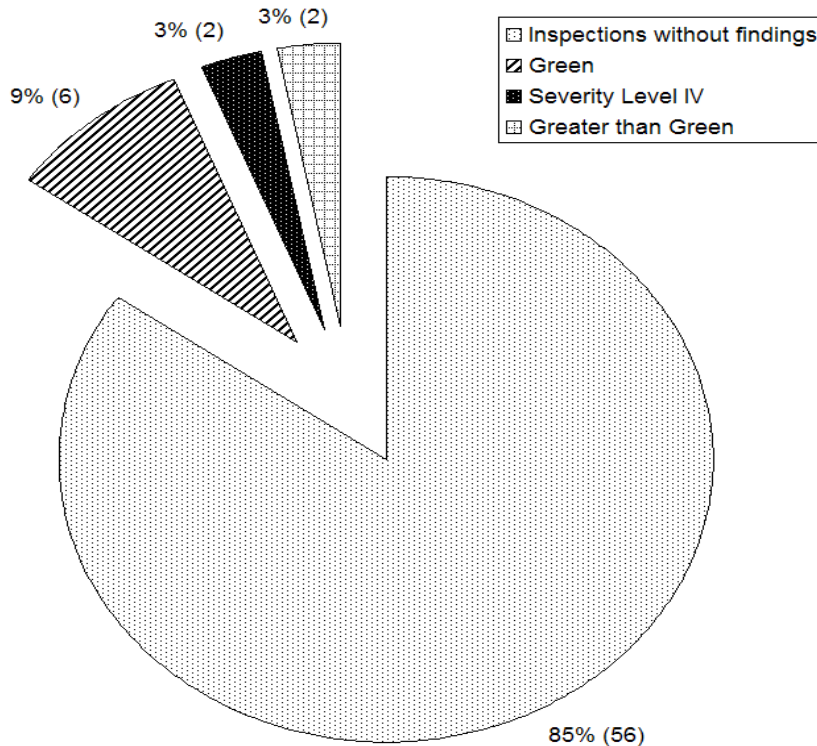


Figure 3: Summary of First Cycle of FOF Inspection Findings at NPPs

² Both Greater than Green findings occurred in CY 2007.

3.4 Discussion of Corrective Actions

If inspectors during the conduct of FOF inspection activities identify deficiencies that indicate a licensee potentially cannot demonstrate the ability to protect against the applicable Design Basis Threat (DBT) with high assurance or does not meet other regulatory requirements, that licensee must take immediate corrective actions or compensatory measures sufficient to restore regulatory compliance. NRC inspectors review any proposed compensatory measures and/or corrective actions and, once determined acceptable, must verify that those actions have been completed by the licensee before leaving the site. As appropriate, the licensee must also plan for long-term corrective actions with oversight from the NRC.

In many cases, though not required by regulation, licensees implement corrective actions in response to lessons learned from FOF inspections, even after demonstrating that their protective strategy can effectively protect against the DBT. Those corrective actions typically fall into one of the following three categories: procedural or policy changes, physical security and/or technology improvements and upgrades, and personnel or security force enhancements. In CY 2007, FOF inspectors have observed corrective actions taken in each of these categories.

As an example of a procedural or policy change, one licensee kept keys for a security response vehicle in an unprotected location. During an FOF exercise, the CAF team acquired those keys and used the vehicle to facilitate its simulated attack. Although the licensee was not in violation of NRC requirements and demonstrated an effective protective strategy, the site's security management recognized the potential vulnerability and made procedural changes to enhance its protective strategy based on the FOF exercise.

Licensees will also commonly make improvements to or add physical security structures and technologies based on lessons learned from FOF exercises. For example, if a licensee determines that the adversary team did not encounter enough delay throughout the simulated attack, extra delay barriers such as fences, or locks on doors or gates may be added. As another example, if a licensee determines that earlier detection and assessment is desirable (even after demonstrating an effective protective strategy in FOF exercises), the licensee may choose to add sensors, cameras, and/or lighting to the owner controlled area (the area of the facility beyond the boundary of the protected perimeter) to enhance the security posture.

Finally, licensees may commit to additional security personnel as a result of lessons learned from FOF exercises. Inspectors have observed situations where licensees determined that adding additional security personnel helped to ensure that licensees would have a greater opportunity to interdict adversaries at a greater frequency, further enhancing their ability to prevent the adversaries from completing their mission.

3.5 Future Planned Activities

In CY 2008, the second cycle of FOF inspections begins with 25 inspections scheduled for the year. Of the 25 inspections, 2 are follow-up inspections to test corrective actions and evaluate any other improvements licensees implemented as a result from previous FOF inspections. Although significant enhancements have been made, the NRC will continue to seek additional methods to improve realism in FOF exercises throughout the inspection cycle.

4. SECURITY BASELINE INSPECTION PROGRAM

4.1 Overview

The security baseline inspection program is a primary component of the security cornerstone of the ROP that the NRC uses to ensure plant and radiological safety, security, and emergency preparedness at operating NPPs. It is important to note that FOF inspections are just one piece of the NRC's overall security oversight process. In addition to FOF inspections, the security baseline inspection program includes the following inspectable areas: Access Authorization; Access Controls; Equipment Performance, Testing, and Maintenance; Protective Strategy and Evaluation; Security Training; the Fitness for Duty Program; and Owner Controlled Area Controls. Material Control and Accounting and Physical Protection of Shipments of spent nuclear fuel inspections are conducted by using interim guidance. Information Security Technology interim inspection guidance is pending development.

4.2 Results of Inspections

Tables 3 and 4 summarize the overall results of the security baseline inspection program of NPPs excluding FOF inspection results (which were discussed in Section 3). Figure 4 provides a graphical summary of the CY 2007 security baseline inspections. This information provides a summary overview of licensee performance within the Security Cornerstone.

For the purpose of this report, an inspection is considered complete after either (1) the inspection report is issued with no findings or (2) any findings have been dispositioned or any applicable enforcement action has been taken. For example, in 2007, the NRC conducted multiple inspections at the Peach Bottom NPP, some of which are ongoing in CY 2008, as a result of security officers that were inattentive to duty.³ In September 2007, Region I was shown a video tape of inattentive security officers at Peach Bottom, that was subsequently aired on WCBS (New York City). In response, the NRC conducted augmented inspections and, to ensure continued security plan effectiveness at Peach Bottom, issued a confirmatory action letter in October 2007. In February 2008, the NRC issued a White finding to Exelon for its failure to maintain the minimum number of available security responders and failure to maintain a behavior observation program. To date, the licensee's actions have been appropriate and no new findings have been identified. Investigations of this issue by the Office of Investigations and the Inspector General are ongoing. Any other findings that were not dispositioned during CY 2007 will be documented in the next annual report to Congress.

³ For more information regarding the inspection activities at Peach Bottom, see <http://www.nrc.gov/reading-rm/doc-collections/news/2008/08-005.i.html>.

| Table 3: CY 2007 Security Inspections (Without FOF) | |
|--|--|
| 177 | Total number of inspections conducted (includes special and augmented inspections) |
| 83 | Total number of inspections with findings |
| 94 | Total number of inspections without findings |
| 7 | Total number of special and augmented inspections conducted |

| Table 4: CY2007 Security Inspection Findings (Without FOF) | |
|---|---|
| 117 | Total number of inspection findings |
| 63 | Total number of Green findings |
| 1 | Total number of greater than Green findings |
| 51 | Total number of SL IV violations |
| 2 | Total number of greater than SL IV violations |

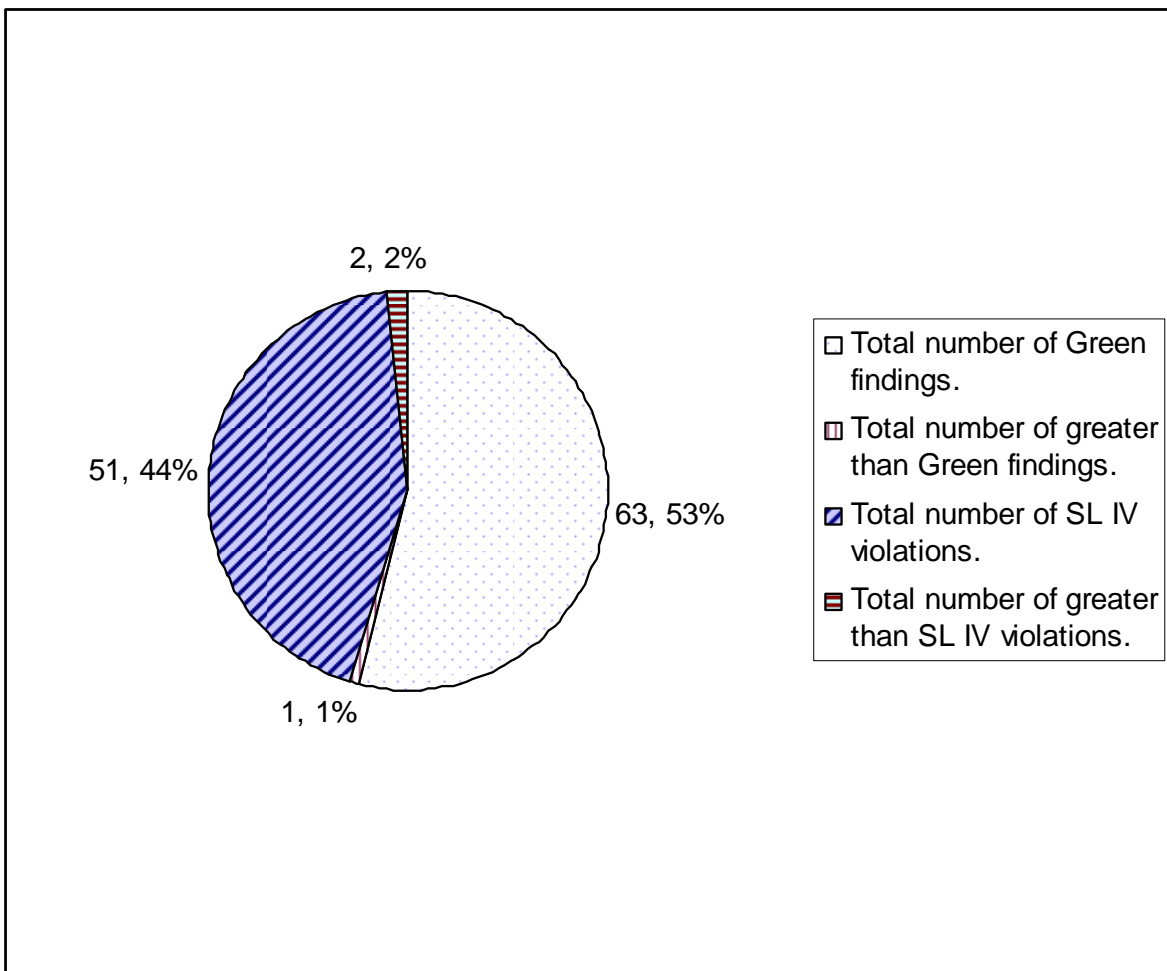


Figure 4: Summary of CY 2007 Security Inspection Findings at NPPs

5. OVERALL REACTOR SECURITY ASSESSMENT

5.1 Overview

The previous two sections described the results of the security baseline inspection program. The security assessment process collects the information from those inspections and PIs provided by NPP licensees to enable the NRC to arrive at objective conclusions about a licensee's security performance. Based on this assessment information, the NRC determines the appropriate level of agency response.

5.2 Performance Indicators

Licensees voluntarily report data on the following three performance indicators in security: (1) Protected Area Equipment, (2) Personnel Screening Program, and (3) Fitness-for-Duty/Personnel Screening Program. The NRC compares data reported by the licensees to an established set of thresholds to determine the data's significance, which is represented by the colors green, white, yellow, and red (in order of increasing severity). The PIs measure aspects of the licensees' security programs that are not specifically inspected by the NRC's baseline inspection program.

As of the end of CY 2007, all licensees reported that each security performance indicator was categorized as green. The NRC staff reviewed historical PI data and concluded that the Personnel Screening Program and the Fitness-for-Duty/Personnel Reliability PIs had a limited frequency of occurrence, rarely exceeding the predetermined thresholds, and NRC inspections already reviewed the performance objectives associated with the PIs. Additionally, the licensees are already required by regulation to report this information to the NRC for specific occurrences. As a result, the Commission approved the staff's plan to discontinue these two PIs, but maintain the Protected Area Equipment PI, and to evaluate the development of additional PIs to improve regulatory oversight of security operations.

5.3 Security Cornerstone Action Matrix

Similar to the ROP action matrix, the security cornerstone has the following five response columns: Licensee Response, Regulatory Response, Degraded Cornerstone, Repetitive Degraded Cornerstone, and Unacceptable Performance. Table 4 summarizes the number of plants by their performance as indicated by security cornerstone action matrix columns.

Most licensees fall into the Licensee Response column, which indicates that all assessment inputs (PIs and inspection findings) were green and the cornerstone objectives were fully met. Licensees that fall into the Regulatory Response column have assessment inputs that resulted in no more than one white input, and the cornerstone objective was met with minimal reduction in security performance. In CY 2007, four sites fell into this column.

The Degraded Cornerstone column categorizes a performance level indicated by multiple white inputs or one yellow input with the cornerstone objective met with moderate degradation in security performance. If a licensee falls into the Repetitive Degraded Cornerstone column, they have received multiple yellow inputs or at least one red input while meeting the cornerstone objective with longstanding issues or significant degradation in security performance. The most significant column in the security action matrix is the unacceptable performance column. Licensees in this column have overall unacceptable performance and margin for security. In CY 2007, no licensees fell into the degraded cornerstone, repetitive degraded cornerstone, or unacceptable performance categories.

| Table 5: Summary of Security Action Matrix⁴ | |
|---|---------------------------------|
| Number of Sites | Response Band |
| 60 | Licensee Response |
| 4 | Regulatory Response |
| 0 | Degraded Cornerstone |
| 0 | Repetitive Degraded Cornerstone |
| 0 | Unacceptable Performance |

⁴ NOTE: For the purpose of the security inspection program, Salem and Hope Creek are counted as one site, as they share a common security program, bringing the total number of reactor sites to 64.

6. CAT I FACILITY SECURITY OVERSIGHT PROGRAM

6.1 Overview

The NRC implements regulatory oversight of safeguards and security programs of two CAT I fuel cycle facilities. BWX Technologies (BWXT), located in Lynchburg, Virginia, and Nuclear Fuel Services (NFS) located in Erwin, Tennessee, manufacture fuel for government reactors. They also down blend highly-enriched uranium (HEU) into low-enriched uranium (LEU) for use in commercial reactors. Each CAT I facility stores and processes strategic special nuclear material (SSNM), which must be reliably protected against unauthorized access, theft, and diversion. The facilities have significantly enhanced their security posture since September 11, 2001.

The primary objectives of the CAT I security oversight program are to ensure that the fuel cycle facilities are operating safely and securely in accordance with regulatory requirements and Commission Orders, detect indications of declining safeguards performance, investigate specific safeguards events and weaknesses, and identify generic security issues. NRC headquarters and regional security inspectors based at NRC offices in Atlanta, Georgia, and Rockville, Maryland, conduct inspections using detailed inspection procedures. The conduct of inspections, identification of findings, final review and determination of significance of the findings, provide overall assessment of licensee performance.

Similar to the reactor baseline inspection program, the CAT I security oversight program is applied to identify findings, determine their significance, document results, and assess licensees' corrective actions. The core inspection program requires three physical security areas ("inspection procedure suites") to be reviewed annually at each CAT I facility. These include HEU access control, HEU alarms and barriers, and other security topics such as security force training and contingency response. The core inspection program also requires 2 MC&A inspections annually and a transportation security inspection once every 3 years. NRC inspectors also review the U.S. Department of Energy's (DOE) audits of licensees' programs to protect classified material and information.

The core inspection program is complemented by the FOF inspection program, which is implemented by NRC Headquarters inspectors. In addition, NRC resident inspectors assigned to each CAT I facility provide an on-site NRC presence for direct observation and verification of licensee's ongoing activities. Through the results obtained from all oversight efforts, the NRC determines whether licensees comply with regulatory requirements and can provide high assurance of adequate protection against the DBT for theft and diversion of CAT I SSNM.

Similar to the ROP, plant-specific supplemental or reactive inspections may be conducted to investigate a particular deficiency or weakness. Such an inspection is not part of the core inspection program and would only be conducted after a review and assessment of a particular security or safeguards event or condition.

6.2 Results of Inspections

The results of the CAT I security inspections are included in the Safeguards Information version of this report.

PAGE INTENTIONALLY LEFT BLANK

7. STAKEHOLDER COMMUNICATIONS

7.1 *Communications with Public and Industry*

In 2006, the Commission reviewed several options that would make some security oversight information available to the public. The Commission decided to have the cover letters to NPP security-related inspection reports made available in the public domain. However, the information contained in the letters would have to be such that the letters do not identify actual or potential vulnerabilities at the inspected plant. The cover letters for NPP security-related inspection reports issued after May 8, 2006, are released to the public. To continue the NRC's practice of communicating clearly and frequently on operating plant and materials activities, the NRC will hold meetings with the public or other external stakeholders both in the vicinity of nuclear facilities and its headquarters and regional offices.

The restrictions the NRC placed on releasing security-related information to the public after September 11, 2001, also impacted the NRC's ability to share information with alleged who brought security-related concerns to the NRC. The restrictions have made it difficult to assure alleged that their concerns have been addressed, and a number of alleged have expressed dissatisfaction with this policy. Some, in an effort to obtain a satisfactory response, have chosen to pursue their concerns publicly by engaging elected officials and public interest groups and by disseminating their concerns via public websites or media outlets. In an effort to respond to this issue, the Commission has approved a three-tiered approach to responding to security alleged based on the severity of the concern raised and normal availability of the information to the alleged (i.e., the alleged is a member of a licensee's security force).

As an additional effort to inform and involve stakeholders in the regulatory process, the NRC continues to hold annual public meetings specifically on nuclear security issues.⁵ Additionally, security topics are presented at the NRC's Regulatory Information Conference held each spring in Rockville, Maryland.

The NRC also communicates with the industry to disseminate key lessons learned and generic issues. The NRC analyzes findings and observations from the security inspection program to determine if a potentially generic issue may exist across the industry. When applicable, the NRC staff supplements periodic security meetings held with the industry and develops generic communications or advisories as a means of effective communication to the industry for security-related issues. In CY 2007, the NRC issued six security advisories (SA) and one information notice (IN) covering a variety of topics (see list below). After each FOF inspection, NRC staff gathers lessons-learned in a variety of categories. Those lessons learned are disseminated to the industry through the Nuclear Security Working Group (NSWG), a consortium of security representatives from NRC-licensed facilities, in order to further the mutual goal of safe and realistic performance evaluations.

⁵ For more information on public meetings on security, please see <http://www.nrc.gov/security/security-safeguards.html>.

CY 2007 List of Generic Communications by title:

| | |
|----------|--|
| SA-07-01 | Use of Authentication Codes to Validate Caller ID |
| SA-07-02 | National Special Security Event – State of the Union Address – Power Reactors |
| SA-07-03 | National Special Security Event – State of the Union Address – Research and Test Reactors (RTR) |
| SA-07-04 | National Special Security Event – State of the Union Address – Power Reactors Radioactive Material Quantities of Concern (RAMQC) |
| SA-07-05 | National Special Security Event – State of the Union Address – Materials |
| SA-07-06 | Security Officers Inattentive to Duty |
| IN-07-20 | Use of Blank Ammunition |

7.2 Communications with Local, State, and Federal Agencies

In most NRC FOF inspections, representatives from local law enforcement agencies attend planning activities and observe the exercise to improve understanding of the licensee's response and coordination of integrated response activities. Other representatives from State emergency management agencies, State governments, the Government Accountability Office, and Congress have also observed FOF inspections.

The NRC's security action matrix also includes informing various levels of interested local, State, and Federal organizations of plants whose performance has declined. In addition, Homeland Security offices in several States routinely receive copies of security inspection reports from the NPPs located in their States.

The NRC continues to support the U.S. Department of Homeland Security/Homeland Security Council (DHS/HSC) initiative to enhance integrated response planning for power reactor facilities. The staff is continuing to work with DHS/HSC, the Federal Bureau of Investigation (FBI), and others to develop plans to further this initiative. In addition, the staff has coordinated with other Federal agencies and State and local security partners in completing the development of Emergency Action Levels for all imminent threats.

7.3 Openness Initiatives

In 2008, the NRC staff began to engage public stakeholders to explore means to increase the timely availability of security performance information while appropriately protecting site vulnerability information that would be useful to adversaries in a planning stage. The staff plans to conduct several public meetings before providing its recommendations to the Commission in late 2008.

Previously, The NRC staff communicated FOF exercise results to Congressional, State, and local stakeholders when a licensee did not demonstrate an effective protective strategy. In February 2008, the staff revised the communication plan to inform the appropriate Congressional, State, and local stakeholders of all FOF exercise results regardless of exercise outcome.