August 14, 2012

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

Dear Madam Chairman:

On behalf of the U.S. Nuclear Regulatory Commission (NRC), I am pleased to submit the 2011 "Report to Congress on the Security Inspection Program for Commercial Power Reactor and Category I Fuel Cycle Facilities: Results and Status Update." The Atomic Energy Act of 1954, as amended, 42 U.S.C. §2210d.(e), requires the NRC to submit a report to Congress, in both classified and unclassified form, that describes the results of each security response evaluation (i.e., force-on-force (FOF) exercises) conducted and any relevant corrective actions taken by a licensee during the previous year. Additionally, I am providing information regarding the overall security and safeguards performance of the commercial nuclear power industry and Category I (CAT I) fuel cycle facilities to keep you informed of the NRC's efforts to regulate the security standards for the Nation's civilian nuclear power infrastructure and strategic special nuclear material against terrorist attacks. Conducting FOF exercises and implementing the security inspection program are 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 power industry and CAT I fuel cycle facilities.

During calendar year 2011, the NRC conducted 225 security inspections (of which, 24 were FOF inspections) at commercial nuclear power reactors and CAT I fuel cycle facilities. These inspections identified 155 findings, 143 of which were of very low security significance and 12 were of greater than very low security significance. The Safeguards Information attachment to the report discusses the results of the security inspections conducted at commercial nuclear power reactors and CAT I fuel facilities. Whenever a finding is identified during a security inspection, the NRC ensures that the licensee implements adequate compensatory measures until the problem is corrected. Compensatory measures can include, for example, additional armed personnel and/or physical security measures to strengthen a licensee's response capabilities.

Through our inspection and oversight processes, the NRC is committed to effective regulation so that licensees continue to provide high assurance that their facilities remain secure.

The Attachment to the Enclosure transmitted herewith contains Safeguards Information. When separated from the Attachment, this transmittal document is decontrolled.

The NRC will make available for members of Congress, or Congressional Oversight Committee staff, the unclassified, Safeguards Information, and classified inspection reports, as appropriate, for any FOF inspection in their State or congressional district through the NRC's Office of Congressional Affairs. The same offer will be extended, as appropriate, under existing protocols and requirements, to Governor-appointed State Liaison Officers.

For this year, the inspection results for the CAT I fuel cycle facilities did not reach the classified level. Therefore, there is no Confidential attachment to this letter.

The Enclosure to this letter will be made publicly available by the NRC; however, the Attachment to the Enclosure contains Safeguards Information and is not for public disclosure. The Attachment to the Enclosure must be handled and stored in accordance with Title 10 of the *Code of Federal Regulations* (10 CFR) 73.21, "Protection of Safeguards Information: Performance Requirements," as noted and described in the cover sheet. Therefore, I request that access to this Attachment be limited to you and those of your staff who have a need-to-know. In addition, pursuant to Section 149 of the Atomic Energy Act of 1954, as amended, and 10 CFR 73.59, "Relief from Fingerprinting, Identification, and Criminal History Records Checks and Other Elements of Background Checks for Designated Categories of Individuals," access to the Attachment must be restricted to those members of your staff who have undergone fingerprinting for a prior U.S. Government criminal history check.

Please do not hesitate to contact me if you need additional information.

Sincerely,

/RA/

Allison M. Macfarlane

Enclosure:
Report to Congress on the Security Inspection Program for Commercial Power Reactors and Category I Fuel Cycle Facilities: Results and Status Update (Unclassified)

cc: Senator James M. Inhofe

Identical letters 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 Thomas R. Carper
Chairman, Subcommittee on Clean Air and
Nuclear Safety
Committee on Environment and Public Works
United States Senate
Washington, D.C. 20510
cc: Senator John Barrasso

The Honorable Fred Upton
Chairman, Committee on Energy
and Commerce
United States House of Representatives
Washington, D.C. 20515
cc: Representative Henry A. Waxman

The Honorable Ed Whitfield
Chairman, Subcommittee on Energy
and Power
Committee on Energy and Commerce
United States House of Representatives
Washington, D.C. 20515
cc: Representative Bobby L. Rush

The Honorable John Shimkus
Chairman, Subcommittee on Environment
and the Economy
Committee on Energy and Commerce
United States House of Representatives
Washington, D.C. 20515
cc: Representative Gene Green

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

Annual Report for Calendar Year 2011

Office of Nuclear Security and Incident Response
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This report fulfills the requirements of Section 170D of Chapter 14 of the Atomic Energy Act of 1954 (42 U.S.C. 2201 et seq.), as amended, which states, "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 seventh annual report, which covers calendar year 2011. In addition to information on the security response evaluation program (force-on-force inspections), the U.S. Nuclear Regulatory Commission (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 public health and safety, the common defense and security, and the environment through the effective regulation of the Nation's commercial nuclear power facilities and strategic special nuclear material.

Paperwork Reduction Act Statement

NUREG-1885, Rev. 5, "Report to Congress on the Security Inspection Program for Commercial Power Reactors and Category I Fuel Cycle Facilities: Results and Status Update," 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 Office of Management and Budget control number.

PAGE INTENTIONALLY LEFT BLANK

CONTENTS

ABSTRACT iii

ACRONYMS vii

1. INTRODUCTION 1

2. REACTOR SECURITY OVERSIGHT PROCESS 3

2.1 Overview 3
2.2 Significance Determination Process 5
2.3 Findings and Violations 5
2.4 Cyber Security 6

3. FORCE-ON-FORCE INSPECTION PROGRAM FOR NUCLEAR POWER PLANTS 7

3.1 Overview 7
3.2 Program Activities in 2011 8
3.3 Results of Force-on-Force Inspections 8
3.4 Discussion of Corrective Actions 9
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 Indicator 13
5.3 Security Cornerstone Action Matrix 13

6. CATEGORY I FUEL CYCLE FACILITY SECURITY OVERSIGHT PROGRAM 15

6.1 Overview 15
6.2 Results of Inspections 16

7. STAKEHOLDER COMMUNICATIONS 17

7.1 Communications with the Public, Licensees, and Other Stakeholders 17
7.2 Calendar Year 2011 List of Generic Communications by Title 18
7.3 Communications with Local, State, and Federal Agencies 18

FIGURES

Figure 1: Cornerstones of the Reactor Oversight Process....3
Figure 2: Inspectable Areas of the Security Cornerstone 4
Figure 3: Summary of Calendar Year 2011 Baseline Security Inspection Findings at Nuclear Power Plants....12

TABLES

Table 1: Calendar Year 2011 Force-on-Force Inspection Program Summary for Nuclear Power Plants 9
Table 2: Calendar Year 2011 Security Inspections at Nuclear Power Plants (without Force-on-Force)....11
Table 3: Calendar Year 2011 Security Inspection Findings at Nuclear Power Plants (without Force-on-Force)....11
Table 4: Summary of Security Cornerstone Action Matrix 14

ACRONYMS

10 CFR	Title 10 of the *Code of Federal Regulations*
CAF	composite adversary force
CAT I	Category I
CY	calendar year
DBT	design basis threat
DHS	U.S. Department of Homeland Security
FBI	Federal Bureau of Investigation
FOF	force-on-force
FR	*Federal Register*
HEU	highly enriched uranium
IMC	Inspector Manual Chapter
IPCE	Integrated Pilot Comprehensive Exercise
IR	inspection report
MC&A	material control and accounting
NEI	Nuclear Energy Institute
NPP	nuclear power plant
NRC	U.S. Nuclear Regulatory Commission
PA	protected area
PI	performance indicator
PPSDP	physical protection significance determination process
ROP	Reactor Oversight Process
SDP	significance determination process
SGI	Safeguards Information
SA	security advisory
SL	severity level
SSNM	strategic special nuclear material

PAGE INTENTIONALLY LEFT BLANK

1. INTRODUCTION

This report fulfills the requirements of Section 170D of Chapter 14 of the Atomic Energy Act of 1954 (42 U.S.C. 2201 et seq.), as amended, which states, "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 annual report covers calendar year (CY) 2011. In addition to providing 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 and Category I (CAT I) fuel cycle facilities to keep Congress and the public informed of the NRC's efforts to protect public health and safety, the common defense and security, and the environment through the effective regulation of the Nation's commercial nuclear power facilities and strategic special nuclear material (SSNM).

Conducting FOF exercises and implementing the security inspection program are just two of a number of regulatory oversight activities that the NRC performs to ensure the secure and safe use and management of radioactive and nuclear materials by the commercial nuclear industry. In support of these activities, the NRC evaluates relevant intelligence information and vulnerability analyses to determine realistic and practical security requirements and mitigative strategies. The NRC also takes a risk-informed, graded approach to establish appropriate regulatory controls, to enhance its inspection efforts, to assess the significance of security issues, and to require timely and effective corrective action for identified deficiencies by licensees of commercial nuclear power reactors and CAT I fuel cycle facilities. The NRC also relies on interagency cooperation to develop an integrated approach to the security of nuclear facilities and contribute to the NRC's comprehensive evaluation of licensee security performance.

This report provides both an overview of the NRC's security inspection and FOF programs and summaries of the results of those inspections. It also describes the NRC's communications and outreach activities with the public and other stakeholders (including other Federal agencies). Unless otherwise noted, this report does not include the security activities or initiatives of any class of licensee other than power reactors or CAT I fuel cycle facilities. CAT I fuel cycle facilities are those that use or possess formula quantities of SSNM, which Title 10 of the *Code of Federal Regulations* (10 CFR) 70.4, "Definitions," defines 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 inspecting and assessing licensee performance at operating nuclear power plants (NPPs) in a manner that is risk-informed, objective, predictable, and understandable. ROP instructions and inspection procedures help ensure that licensee actions and regulatory responses are commensurate with the safety or security significance of the particular event, deficiency, or identified weakness. Within each ROP cornerstone (see Figure 1), NRC inspectors implement inspection procedures, and NPP licensees report performance indicator (PI) results to the NRC. The results of these inspections and PIs contribute to an overall assessment of licensee performance.

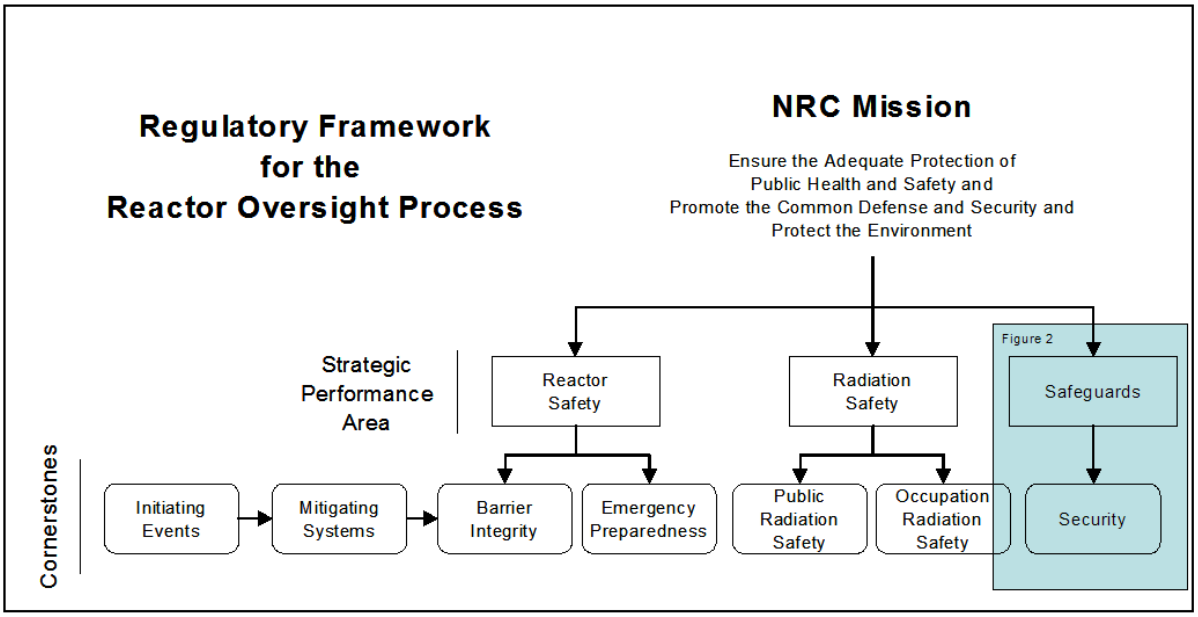

Figure 1: Cornerstones of the Reactor Oversight Process

As part of its actions following the terrorist attacks of September 11, 2001, the NRC issued a number of orders requiring licensees to strengthen security programs in several areas. During 2009, the NRC completed a rulemaking that made generally applicable security requirements similar to these orders and added new requirements based on insights and experience, including stakeholder feedback. Through the orders and the subsequent rulemaking, the NRC significantly enhanced its baseline security inspection program for commercial NPPs. 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 PIs, the NRC determines whether licensees comply with appropriate regulatory requirements and can provide high assurance of adequate protection against the design basis threat (DBT) of radiological sabotage.

The security cornerstone's baseline inspection program has 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 could result in a degradation of reactor safety or undue risk to public health and safety; and (4) to identify those significant issues that may have generic or crosscutting applicability. These objectives help ensure the secure use and management of radioactive materials.

The security cornerstone's baseline inspection program includes 10 inspectable areas to be reviewed periodically at each power reactor facility (see Figure 2). One of the inspectable area**s**—contingency response—is assessed through the conduct of FOF inspections, which the next section describes in detail.

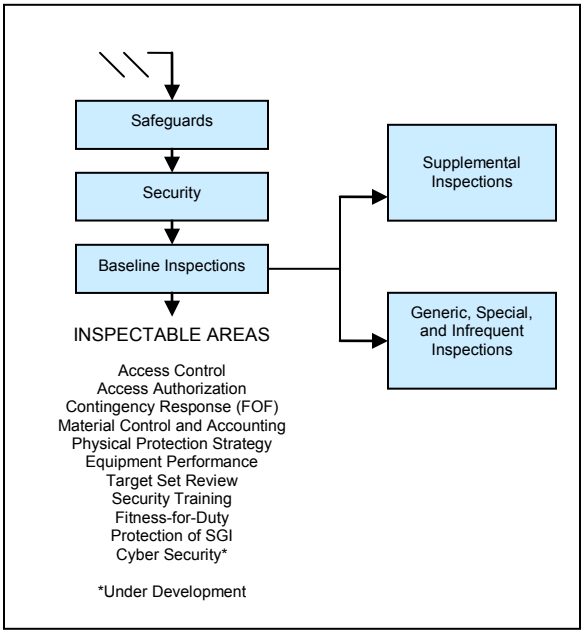

Figure 2: Inspectable Areas of the Security Cornerstone

If a licensee's performance degrades, as indicated by the quantity and significance of inspection findings and PIs, the NRC may conduct supplemental inspections in accordance with the security action matrix to ensure that the licensee takes corrective actions to address and prevent recurrence of the performance weaknesses.

In response to security or safeguards events or to conditions affecting multiple licensees, the NRC may conduct generic or special inspections, which are not part of the baseline or supplemental inspection program. Examples of these events or conditions include, but are not limited to, resolution of employee concerns, security matters requiring particular focus, and licensee plans for coping with a security force strike or walkout.

2.2 Significance Determination Process

The significance determination process (SDP) for NPPs uses risk insights, where appropriate, to help NRC inspectors and the NRC staff determine the significance of inspection findings. These findings include both programmatic and process deficiencies. The NRC evaluates security-related findings using the baseline physical protection SDP (PPSDP). The PPSDP determines the security significance of security program deficiencies.

The NRC also uses a PPSDP to evaluate FOF performance findings. The significance of findings associated with FOF adversary actions depends on their impact on significant equipment (referred to as a "target set") and a determination of whether these actions could have an adverse impact on public health and safety. The NRC also uses the baseline PPSDP to evaluate other security-related findings identified during FOF activities. 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, it will consider the exercise indeterminate, and it may conduct an additional exercise, if appropriate.

The NRC assigns the following colors to inspection findings evaluated with the SDP:

- green (very low security significance)
- white (low-to-moderate security significance)
- yellow (substantial security significance)
- red (high security significance)

The NRC conducts supplemental inspections in response to white, yellow, and red findings.

2.3 Findings and Violations

Inspection findings are associated with identified performance deficiencies and also typically relate to violations of NRC requirements. Violations associated with green findings are usually described in inspection reports (IRs) as non-cited violations if the licensee has placed the issue into its corrective action program. A violation associated with a finding having greater-than-green significance is typically cited as a notice of violation requiring a written response detailing reasons for the violation and immediate and long-term corrective actions. Additionally, the NRC verifies that the licensee's corrective actions were adequate through supplemental inspections.

The NRC uses its traditional enforcement process to evaluate all inspection findings at CAT I fuel cycle facilities and those violations at commercial power reactor facilities that have willful aspects, actual safety consequences, or an impact on the regulatory process. The NRC staff categorizes these violations in terms of four levels of severity to show their relative importance or significance. It assigns Severity Level (SL) I to the most significant violations. In general, violations designated as SL I or II involve actual or high potential consequences for public health and safety or the common defense and security. SL III violations are cause for significant regulatory concern. SL IV violations are less serious, but are of more-than-minor concern. SL IV violations involve noncompliance with NRC requirements that are not considered significant, based on security risk. For particularly significant violations, the Commission

reserves the use of discretion to assess civil penalties in accordance with Section 234 of the Atomic Energy Act of 1954, as amended.

2.4 Cyber Security

The NRC is developing an oversight program for cyber security and plans to incorporate this program into the ROP starting in early CY 2013. The NRC required licensee cyber security actions by order after September 11, 2001, and subsequently codified them through the issuance of 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks." This regulation is commonly referred to as the "Cyber Security Rule." Previously, licensees addressed elements of cyber security in a section of their physical security plans. The new regulation requires licensees to develop standalone cyber security plans. Licensees submitted those plans by the schedule shown in the Cyber Security Rule. Subsequently, the NRC reviewed and approved those plans, and licensees are in the process of implementing them.

The staff is developing an inspection procedure and a process for evaluating the significance of inspection findings. The staff has developed a cyber security inspector training program. The first two-week inspector training course was conducted in January 2011 and the next course is tentatively scheduled for October 2012. After the class in October, the NRC will have trained approximately 60 personnel (inspectors and cyber security specialists). The inspection program development was accomplished collaboratively with stakeholders to include NRC staff and Regional inspectors, the industry, Federal partners and representatives from the Department of Homeland Security, the Federal Energy Regulatory Commission, and the National Institute of Standards and Technology. Consistent with how NRC developed other inspection elements within the Reactor Oversight Process, NRC will pilot the cyber security inspection process. NRC conducted one pilot evaluation at Watts Bar Unit 2 and will conduct a second pilot evaluation at Clinton in August 2012. Upon successful completion of the pilot process, NRC will begin inspections of the licensee implementation of cyber security plans in January 2013.

3. FORCE-ON-FORCE INSPECTION PROGRAM FOR NUCLEAR POWER PLANTS

3.1 Overview

An FOF inspection, which is typically conducted over the course of 4 weeks, includes both tabletop drills and exercises that simulate combat between a mock adversary force and the licensee's security force. At an NPP, the adversary force attempts to reach and simulate damage to significant systems and components (referred to as "target sets") that protect the reactor's core or the spent fuel pool, which could potentially cause a radioactive release to the environment. The licensee's security force, in turn, attempts to interdict the adversary to prevent the adversary from reaching target sets and thus causing such a release.

In conducting FOF inspections, the NRC notifies the licensees in advance, for operational and personnel safety reasons as well as 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, the licensee must arrange for a group of individuals to control and monitor each exercise. A key goal of the NRC is to balance personnel and plant safety with the maintenance of actual plant security during an exercise that is as realistic as possible.

In preparation for the FOF exercises, information from tabletop drills, which probe for potential deficiencies in the licensee's protective strategy, is factored into a number of adversary force attack scenarios. FOF inspections consider security baseline inspection results and security plan reviews. Any significant deficiencies in the protective strategy identified during FOF exercises are promptly reviewed and corrected. When a complete target set is simulated to be destroyed, and it is determined that the licensee's protective strategy does not demonstrate high assurance to protect against radiological sabotage in accordance with the DBT, compensatory measures will be put in place before the NRC inspection team leaves the site area.[1] However, it may be appropriate, on a case-by-case basis, to allow the licensee time (e.g., 24–48 hours) to determine and implement completely its compensatory measures. Compensatory measures will remain in place until a permanent solution resolving the deficiencies in the protective strategy can be evaluated and implemented. Subsequently, the NRC inspection team or the NRC senior resident inspector will review and ensure that such measures effectively address the noted deficiency.

An FOF inspection usually includes three FOF exercises over 3 nights. If an exercise is canceled because of severe weather or for other reasons, NRC management may consider allowing fewer than three exercises to satisfy inspection requirements, but 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 extend the inspection or return to conduct a subsequent exercise.

---

[1] See the NRC's "Protecting Our Nation" (NUREG/BR-0314, Revision 2, issued June 2011) and the Office of Public Affairs fact sheet on FOF Security Exercises. These are available at http://www.nrc.gov/reading-rm/doc-collections/nuregs/brochures/br0314/r2/br0314r2.pdf and http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/force-on-force.pdf.

3.2 Program Activities in 2011

In 2011, the FOF inspection program continued to focus on effectively evaluating licensee protective strategies while maintaining regulatory stability and consistency in the evaluation process. Also, the NRC staff assured that the nuclear industry improved the standards of training and qualifications for exercise controllers. Furthermore, the NRC staff conducted public meetings and closed industry meetings to present the proposed enhancements to the FOF SDP under consideration for future FOF exercises at NPPs. The NRC staff plans to finalize those proposed enhancements in CY 2012. In 2009, the NRC issued a standalone, target set review inspection procedure, which was revised on August 16, 2011, that the agency used to conduct 22 target set reviews in CY 2011. The NRC staff continues to revise the FOF and target set guidance documentation and related inspection procedures. The NRC remains committed to improving the realism and effectiveness of the FOF inspection program and will continue to pursue methods to improve exercise simulations and 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. FOF team members provide the 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 accurately reflects established parameters. U.S. Department of Defense contractors also provide support to the CAF in tactics planning. Because the CAF is composed of individuals with a nuclear security background, the NRC recognizes the potential for conflicts of interest and continually assesses this possibility. No conflict of interest has been detected.

3.3 Results of Force-on-Force Inspections

Between January 1, 2011, and December 31, 2011, the NRC conducted 24 FOF inspections (all at commercial NPPs) and identified 15 findings[2] that related to areas of the security baseline inspection program. None of the findings resulted from the failure to effectively protect designated target set components during NRC-evaluated FOF exercises.

By the end of 2011, the NRC had completed the first year of the third 3-year cycle of NPP FOF inspections. Table 1 summarizes the 24 FOF inspections conducted at NPPs in CY 2011.

[2] The NRC conducted re-inspections at two sites in 2011 which are included in the 24 FOF inspections.

Table 1: Calendar Year 2011 Force-on-Force Inspection Program Summary for Nuclear Power Plants

24	Total number of inspections conducted
8	Total number of inspections with findings
16	Total number of inspections with no findings
0	Total number of times a complete target set was simulated to be damaged or destroyed
15	Total number of inspection findings
12	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

Of the total number of exercises conducted in CY 2011, two exercises were inconclusive and deemed indeterminate. An indeterminate exercise is one in which 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 because of drill artificialities and exercise control issues. Furthermore, one exercise was canceled because of potential safety concerns associated with dangerous weather conditions. In this instance, the NRC management considered that fewer than three exercises satisfied the inspection requirements because the licensee successfully demonstrated an effective strategy in the two more challenging exercises, with no significant issues identified.

3.4 Discussion of Corrective Actions

In addition to corrective actions as a result of inspection findings, licensees implement corrective actions in response to observations and lessons learned from FOF inspections, even after demonstrating that their protective strategy can effectively protect against the DBT. Corrective actions typically fall into one of three categories: procedural or policy changes, physical security or technology improvements and upgrades, and personnel or security force enhancements. FOF inspectors have observed corrective actions applied in each of these categories.

Licensees commonly improve 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 the desired delay throughout the simulated attack, it may add extra delay barriers, such as fences or locks on doors or gates. In another example, if a licensee determines that earlier detection and assessment are desirable (even after demonstrating an effective protective strategy in FOF exercises), it may choose to add sensors, cameras, or lighting to the owner-controlled area (the area of the facility beyond the boundary of the protected perimeter) to enhance its security posture. Finally, licensees may commit to additional security personnel as a result of lessons learned from FOF exercises. Inspectors have observed situations in which a licensee decided that additional security personnel would increase its opportunity to interdict an adversary and thus enhance its ability to prevent the completion of the adversary's mission. Once these changes are incorporated into the plans required by 10 CFR 73.55, they become lasting regulatory requirements.

3.5 Future Planned Activities

CY 2012, the second year of the third 3-year cycle of FOF inspections, began with 24 inspections scheduled for the year. Of these, one is a follow-up inspection to assess corrective actions and evaluate other improvements that licensees implemented as a result of a CY 2010 FOF inspection. Although significant enhancements have already been made, the NRC will continue to seek ways to increase the realism of 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. 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 control, access authorization, physical protection strategy, security training, equipment performance, fitness-for-duty, protection of Safeguards Information (SGI), target set review, and MC&A. The NRC staff is currently developing the cyber security inspection program based on the cyber security rule, 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks," on a pace consistent with licensees' implementation schedules.

4.2 Results of Inspections

Tables 2 and 3 summarize the overall results of the security baseline inspection program for NPPs, excluding FOF inspection results from 24 inspections (discussed in Section 3) and CAT I fuel cycle facility security inspection results from 8 inspections (discussed in the SGI attachment to this report). Table 2 shows that 110 of the 193 security baseline inspections at NPPs had no findings (57 percent). Figure 3 provides a graphic summary of the CY 2011 security baseline inspection findings. This information gives an overview of licensee performance within the security cornerstone. Detailed discussions on each finding can be found in the SGI attachment to this report.

Table 2: Calendar Year 2011 Security Inspections at Nuclear Power Plants (without Force-on-Force)

193	Total number of inspections conducted
83	Total number of inspections with findings
110	Total number of inspections with no findings
6	Total number of special and augmented inspections

Table 3: Calendar Year 2011 Security Inspection Findings at Nuclear Power Plants (without Force-on-Force)

136	Total number of inspection findings
125	Total number of green findings
9	Total number of greater-than-green findings
2	Total number of SL IV violations
0	Total number of greater-than-SL IV violations

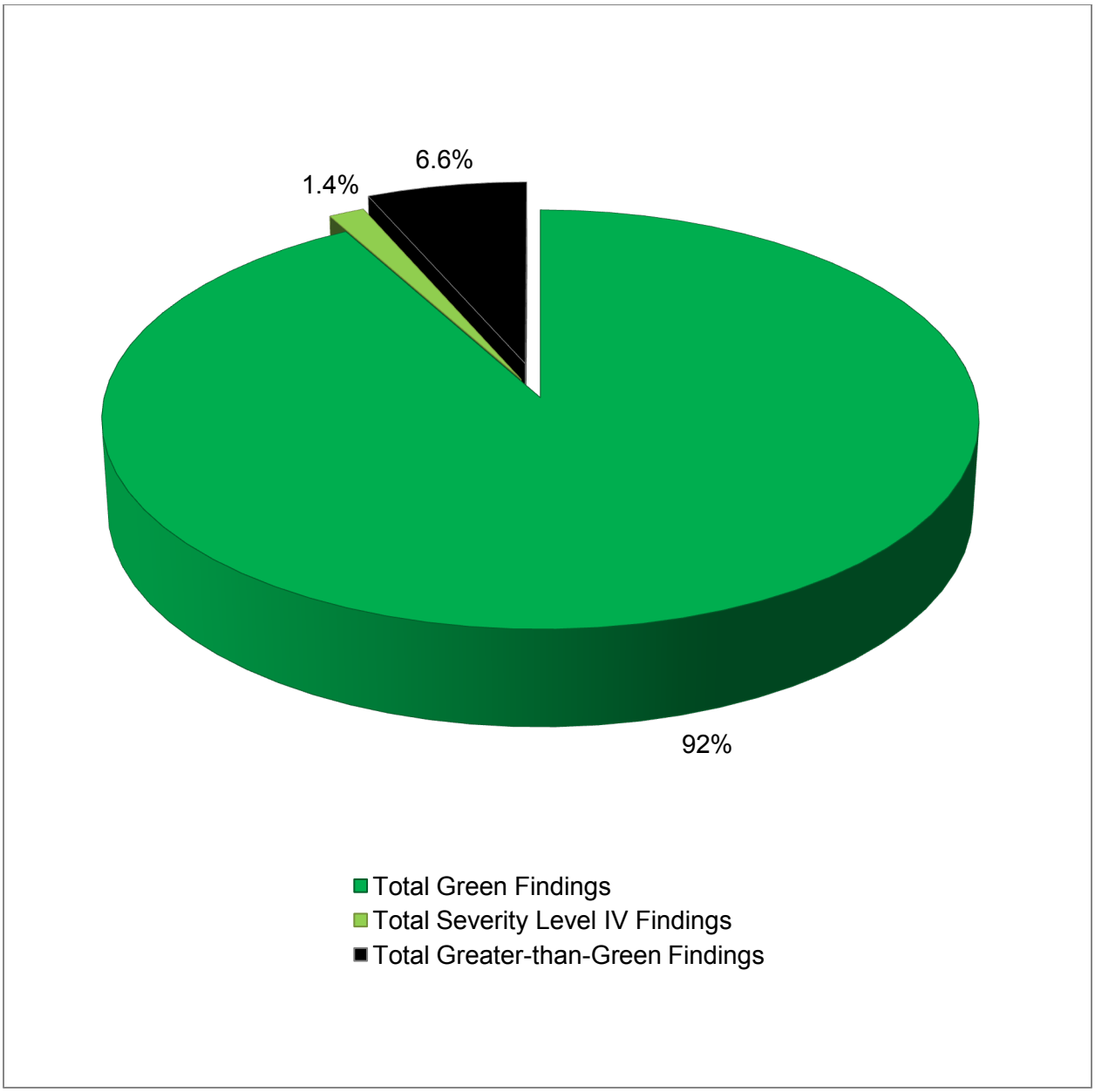

Figure 3: Summary of Calendar Year 2011 Baseline Security Inspection Findings at Nuclear Power Plants

5. OVERALL REACTOR SECURITY ASSESSMENT

5.1 Overview

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

Per Commission direction, in response to the terrorist attacks of September 11, 2001, staff was directed to develop a separate but parallel ROP process for physical protection to address how security-related inspection findings and performance indicators would be considered when determining appropriate agency response. Since 2004, the security cornerstone has been treated similar to, but essentially separate from, the rest of the ROP cornerstones due to the sensitivity of the information involved.

In July 2011, the Commission approved a staff recommendation to reintegrate the security cornerstone into the ROP action matrix. The staff found that using a separate action matrix inhibits the staff's ability to fully leverage supplemental inspection procedures and resources to detect the potential existence of more systemic, organizational issues that can manifest themselves across multiple cornerstones of the ROP. Assessing safety and security performance in a combined action matrix, as originally designed, will ensure that the NRC provides the most appropriate regulatory response to degraded licensee performance, without the need for deviations from the action matrix that may have been required under the separate assessment processes. Security-related information that is currently withheld from public disclosure will continue to be withheld under the combined assessment process. Reintegration of the security cornerstone is scheduled to occur on July 1, 2012.

5.2 Performance Indicator

Licensees voluntarily report data about the protected area (PA) detection and assessment equipment that is implemented within their physical security program. To determine PI significance, data are compared to an established set of thresholds, represented by the colors green, white, yellow, and red (in order of increasing significance); however, the security PI only comprises the green and white thresholds. The PI measures the aspects of the licensees' security programs that are not specifically inspected by the NRC's baseline inspection program. As of the end of CY 2011, all licensees reported that the security PI was categorized as green. This means that PA detection and assessment equipment is operating at a performance level that does not warrant additional NRC inspection.

5.3 Security Cornerstone Action Matrix

Similar to the ROP Action Matrix, the security cornerstone action matrix has five response columns: licensee response, regulatory response, degraded cornerstone, repetitive degraded cornerstone, and unacceptable performance. Table 4 summarizes the number of NPPs whose performance falls into each column of the security cornerstone action matrix.

Most licensees fell into the licensee response column, which indicates that all assessment inputs (PIs and inspection findings) were green and that 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. As of the end of CY 2011, six sites fell into this column.

The degraded cornerstone column categorizes a performance level indicated by multiple white inputs or one yellow input, while meeting the cornerstone objective with moderate degradation in security performance. If a licensee falls into the repetitive degraded cornerstone column, it has 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 cornerstone action matrix is the unacceptable performance column. Licensees in this column have an overall unacceptable performance and margin for security. At the end of CY 2011, no licensees fell into the degraded cornerstone, repetitive degraded cornerstone, or the unacceptable performance categories.

On December 13, 2011, the NRC moved Fort Calhoun Station out of the ROP and is currently conducting safety and security oversight under Inspection Manual Chapter (IMC) 0350, "Oversight of Reactor Facilities in a Shutdown Condition Due to Significant Performance and/or Operational Concerns." Located approximately 19 miles north of Omaha, Nebraska, Fort Calhoun Station was initially shut down in April 2011, for a scheduled refueling outage. The outage was extended because the Missouri River flooding affected the site from June through September 2011, and because of some longstanding technical issues. During the shutdown, additional safety and security issues were identified that required additional NRC oversight. For additional information on the Fort Calhoun Station change in regulatory oversight, please see the letter dated December 13, 2011 (Agencywide Documents Access and Management System Accession No. ML113470721).

The IMC 0350 oversight process is implemented at facilities in an extended shutdown with significant performance concerns to: establish a regulatory oversight framework as a result of significant performance problems or where a significant operational event has occurred; ensure the NRC communicates a unified and consistent regulatory position in a clear and predictable manner; establish a record of actions taken and technical issues resolved; verify corrective actions are sufficient for restart; and to provide assurance that following restart the plant will be operated in a manner that provides adequate protection of public health and safety.

Table 4: Summary of Security Cornerstone Action Matrix

Number of Sites[a]	Response Band
57	Licensee Response
6	Regulatory Response
0	Degraded Cornerstone
0	Repetitive Degraded Cornerstone
0	Unacceptable Performance
1	IMC 0350 Process[b]

[a] For the purpose of the security inspection program, Salem Nuclear Generating Station and Hope Creek Generating Station are counted as one site, as they share a common security program. This brings the total number of reactor sites to 64.

[b] The IMC 0350 Process column is included for illustrative purposes only and is not necessarily representative of the worst level of licensee performance. Plants in the IMC 0350 oversight process are considered outside the auspices of the ROP Action Matrix.

6. CATEGORY I FUEL CYCLE FACILITY SECURITY OVERSIGHT PROGRAM

6.1 Overview

The NRC maintains regulatory oversight of safeguards and security programs at two CAT I fuel cycle facilities: Babcock & Wilcox Nuclear Operations Group, Inc., located in Lynchburg, Virginia, and Nuclear Fuel Services, located in Erwin, Tennessee. These facilities manufacture fuel for Government reactors and also down-blend highly enriched uranium (HEU) into low-enriched uranium for use in commercial reactors. Each CAT I fuel cycle facility stores and processes SSNM, which must be protected with high assurance against unauthorized access, theft, and diversion. The facilities have significantly enhanced their security postures since September 11, 2001.

The primary objectives of the CAT I fuel cycle facility security oversight program are to: (1) determine whether the fuel cycle facilities are operating safely and securely, in accordance with regulatory requirements and Commission orders; (2) detect indications of declining safeguards performance; (3) investigate specific safeguards events and weaknesses; and (4) identify generic security issues. NRC Headquarters and regional security inspectors based at the NRC offices in Rockville, Maryland, and Atlanta, Georgia, conduct inspections using established inspection procedures. In the aggregate, the results of these inspections contribute to an overall assessment of licensee performance.

Similar to the reactor baseline inspection program, the NRC uses the CAT I fuel cycle facility inspection program to make findings, determine their significance, document the results, and assess licensees' corrective actions. The core inspection program requires three HEU-related physical security areas (inspection procedure suites) to be reviewed annually at each CAT I fuel cycle 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 two MC&A inspections annually and a transportation security inspection once every 3 years. NRC inspectors also review the U.S. Department of Energy's audits of licensees' programs to protect classified material and information.

The core inspection program is complemented by the FOF inspection program. In addition, NRC resident inspectors assigned to each CAT I fuel cycle facility provide an onsite NRC presence for direct observation and verification of the 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 or diversion and radiological sabotage of SSNM.

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

6.2 Results of Inspections

Through its inspection program, the NRC has high assurance that CAT I fuel cycle facilities continue to meet the intent of the regulations. The SGI attachment to this report includes the results of the security inspections at CAT I fuel cycle facilities.

7. STAKEHOLDER COMMUNICATIONS

7.1 Communications with the Public, Licensees, and Other Stakeholders

The Commission places the cover letters to NPP security-related IRs in the public domain. The information contained in the letters does not identify actual or potential vulnerabilities at the inspected plant. The NRC releases its cover letters to the public for security-related IRs issued after May 8, 2006.

The NRC continues to hold public meetings specifically on nuclear security issues.[3] For example, the agency presents security topics at its Regulatory Information Conference, held each spring in Rockville, Maryland, and it held a number of meetings on regulatory guidance for the implementation of the power reactor security requirements rulemaking, published in the *Federal Register* (FR) on March 27, 2009 (74 FR 13926). The draft regulatory guides were published for comment by stakeholders in spring 2008 (73 FR 19443). Subsequent to the submission of the final rule to the Commission for consideration, the NRC staff conducted more than 30 meetings with the public and industry stakeholders over an 8-month period. The NRC held these meetings to review and understand comments submitted on the draft regulatory guidance in support of the rulemaking. The guidance, published in July 2009, covers topics that include physical security, access authorization, the safety and security interface, training and qualification of security personnel, contingency planning, and FOF program enhancements.

The NRC also communicates with the industry to disseminate generic issues and key lessons learned from security activities and inspections. The NRC analyzes findings and observations from the security inspection program to determine potential generic issues. When applicable, the NRC staff supplements periodic security meetings held with the industry and develops generic communications or security advisories (SAs) as a means of effectively communicating security-related issues to the industry. In CY 2011, the NRC issued nine SAs covering a variety of topics (see the list in Section 7.2). There were no security-related regulatory issue summaries or information notices issued in CY 2011. After each FOF inspection, the NRC staff gathers lessons learned in a variety of categories. To further the mutual goal of safe and realistic performance evaluations, the NRC disseminates lessons learned to the industry through the FOF Working Group, which includes security representatives from NRC-licensed facilities.

[3] For more information on public meetings on security, see http://www.nrc.gov/security/security-safeguards.html.

7.2 Calendar Year 2011 List of Generic Communications by Title

Security Advisories

SA-11-01	"Uncontrolled Access to Radioactive Material in Quantity of Concern"
SA-11-02, SA-11-03, SA-11-04, SA-11-05	"National Special Security Event for the 2011 Presidential State of the Union Address"
SA-11-06	"Recently Identified Equipment-Related Security Issues at NRC-Licensed Facilities"
SA-11-07	"Multiple Vulnerabilities Discovered and Exploit Packages are Being Developed for Industrial Control Systems"
SA-11-08	"National Special Security Event for the 2011 Asia-Pacific Economic Cooperation Summit To Be Held In Honolulu, Hawaii"
SA-11-09	"Information Security Programs"

Regulatory Issue Summaries

None

Information Notices

None

7.3 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 their 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 continues to support the 2004 Homeland Security Council initiative to enhance integrated response planning for NPP sites. One significant example is the Integrated Pilot Comprehensive Exercise (IPCE) initiative, which is a voluntary, collaborative effort between the Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), the NRC, the Nuclear Energy Institute (NEI), and the nuclear power industry. The IPCE is designed to provide Federal, State, and local law enforcement tactical teams with the opportunity to plan and exercise their responses to simulated security incidents inside NPP sites. Since 2008, the NRC has partnered with FBI, DHS, the nuclear industry, and Federal, State, and local tactical

law enforcement to conduct IPCEs at the Limerick Generating Station, Donald C. Cook Nuclear Plant, and the Indian Point Nuclear Generating Station.

The NRC is currently working with FBI, DHS, NEI, and the nuclear power industry to transition IPCE from a pilot phase to a more durable, repeatable process. Based on lessons learned from the IPCE and other integrated response initiatives, the anticipated approach will focus on core integrated response activities, such as data collection, planning, and plan validation.

Attachment:
Report to Congress on the Security Inspection Program for Commercial Power Reactors and Category I Fuel Cycle Facilities: Results and Status Update **(Safeguards Information)**