June 30, 2010

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 2009 "Report to Congress on the Security Inspection Program for Commercial Power Reactor and Category I Fuel Cycle Facilities: Results and Status Update." Section 651(e) of the Energy Policy Act of 2005 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. I am also providing additional 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 oversee the protection of 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 and nuclear materials by the commercial nuclear power industry. The Safeguards Information and Classified portions to this report will be transmitted under separate cover.

During calendar year 2009, the NRC conducted 179 security inspections (of which 24 were FOF inspections) at nuclear power reactors and CAT I fuel cycle facilities. These inspections identified 180 findings, of which 168 were of very low security significance and 12 were of low-to-moderate security significance. The Safeguards Information and Classified portions to this report discuss the results of the security inspections conducted at commercial nuclear power reactors and CAT I fuel cycle facilities. Whenever a finding is identified during a security inspection, the NRC ensures that the licensee implements adequate compensatory measures to correct the problem. Compensatory measures can include, for example, additional armed personnel and/or physical security measures to strengthen a licensee's response capabilities.

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.

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

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

Sincerely,

/RA/

Gregory B. Jaczko

Enclosure: As stated

cc: Senator James M. Inhofe

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

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

The Honorable Edward J. Markey
Chairman, Subcommittee on Energy and Environment
Committee on Energy and Commerce
United States House of Representatives
Washington, D.C. 20515
Dear Mr. Chairman:
cc: Representative Fred Upton

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
Dear Mr. Chairman:
cc: Senator David Vitter

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 2009

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 to Chapter 14, 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, "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 fifth annual report, which covers calendar year 2009. 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.

PAGE INTENTIONALLY LEFT BLANK

CONTENTS

Figures

Tables

PAGE INTENTIONALLY LEFT BLANK

ACRONYMS

10 CFR	Title 10 of the *Code of Federal Regulations*
BWNOG	Babcock & Wilcox Nuclear Operations Group, Inc.
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
HEU	highly enriched uranium
IPCE	Integrated Pilot Comprehensive Exercise
IR	inspection report
MC&A	material control and accounting
NEI	Nuclear Energy Institute
NFS	Nuclear Fuel Services
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
SL	severity level
SSNM	strategic special nuclear material

PAGE INTENTIONALLY LEFT BLANK

1. INTRODUCTION

This report fulfills the requirements of Section 170D to Chapter 14, 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, "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 fifth annual report covers calendar year 2009. 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 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.

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, 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 issues, and to require timely and effective corrective action of identified deficiencies by licensees of commercial nuclear power reactors and Category I fuel 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.

The U.S. Nuclear Regulatory Commission (NRC) is providing to Congress the fifth annual report on the results of the NRC's security inspection program. This report for calendar year (CY) 2009 conveys the results of inspections for the reporting period.

This report provides both an overview of the NRC's security inspection and force-on-force (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 security activities or initiatives of any class of licensee other than power reactors or Category I (CAT I) fuel cycle facilities. CAT I fuel cycle facilities are those that use or possess formula quantities of strategic special nuclear material (SSNM), which Title 10 of the *Code of Federal Regulations* (10 CFR), Section 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 weakness. Within each ROP cornerstone (see Figure 1), NRC inspectors implement detailed 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.

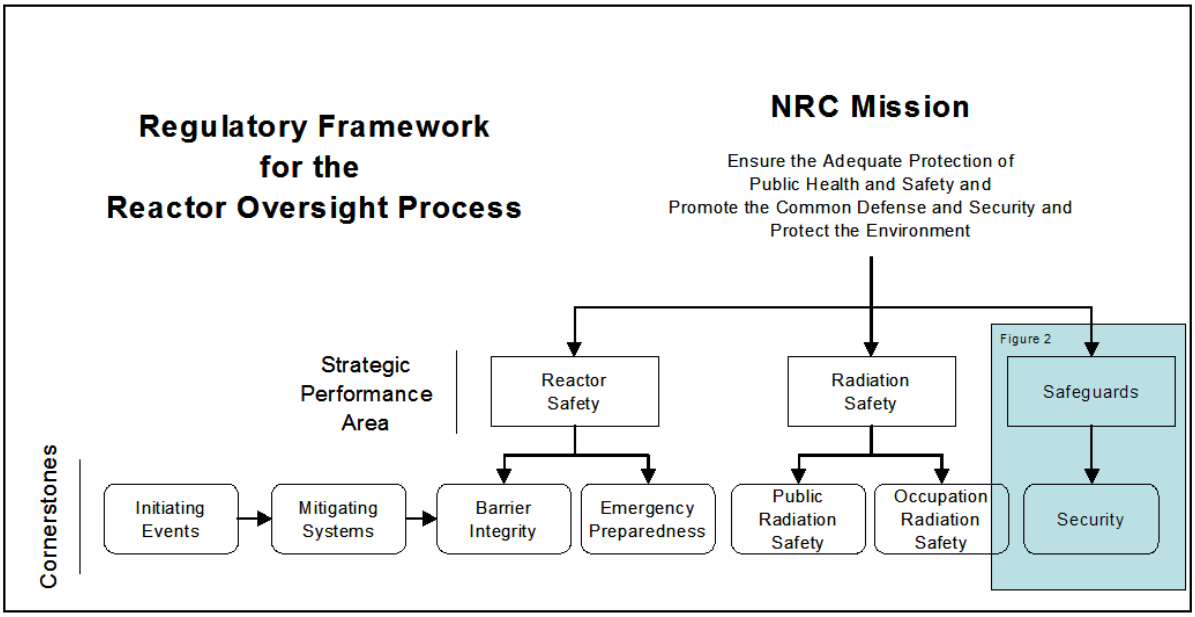

Figure 1: Cornerstones of the ROP

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 the orders and added new requirements based on insights and experience, including stakeholder feedback. Through those 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 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 seven inspectable areas to be reviewed periodically at each power reactor facility (see Figure 2). One of the inspectable areas (cyber security) is still under development and will be included in the inspection program at a later date.[1] The staff is coordinating with internal and external stakeholders in its current efforts to further develop this inspectable area, which will formalize and better define existing oversight activities. Another inspectable area, contingency response, is assessed through the conduct of FOF inspections, which the next section describes in detail.

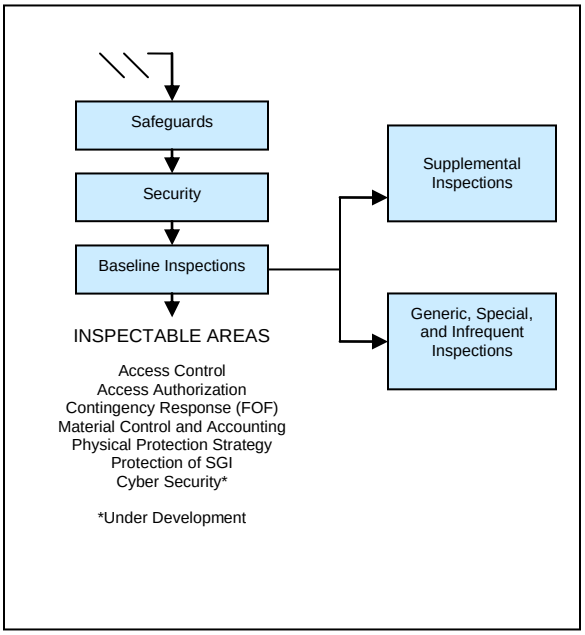

Figure 2: Inspectable areas of the security cornerstone

[1] Cyber Security actions were required by licensees by Order after 9/11 and subsequently codified through the issuance of 10 CFR 73.54. Previously, licensees addressed elements of cyber security in a section of their physical security plans. The new regulation required licensees to develop stand-alone cyber security plans, and they are in the process of implementing these plans. NRC inspection procedures and an oversight program are in the process of being developed.

If a licensee's performance degrades as indicated by quantity and significance of inspection findings and performance indicators, the Agency may conduct supplemental inspections in accordance with the security action matrix to ensure 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 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 the impact on critical 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 Finding and Violations

Inspection findings are associated with identified performance deficiencies and typically also relate to violations of NRC requirements. Violations associated with green findings are usually described in inspection reports (IRs) as noncited 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.

The NRC does not use the SDP to evaluate all inspection findings at CAT I fuel cycle facilities or those findings at commercial power reactor facilities that result in violations with willful aspects, or with potential or actual safety consequences, but instead addresses them through the traditional enforcement process. The 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.

3. FORCE-ON-FORCE INSPECTION PROGRAM FOR NPPS

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 key safety systems and components, defined 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, interposes itself to prevent the adversaries 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, are 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 the DBT, compensatory measures will be put in place before the NRC inspection team leaves the site area.[2] However, in some instances, it may be appropriate, on a case-by-case basis, to allow the licensee time (e.g., 24–48 hours) to determine and completely implement its compensatory measures. Subsequently, the NRC inspection team or the senior resident inspector will review and assure such measures effectively address the noted deficiency.

An FOF inspection includes three FOF exercises over three nights. If an exercise is canceled because of severe weather or for other reasons, the 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 expand the schedule or return to conduct a subsequent exercise.

[2] See "Protecting Our Nation" and the Office of Public Affairs "Backgrounder" on FOF. These are available at http://www.nrc.gov/reading-rm/doc-collections/nuregs/brochures/br0314/.

3.2 Program Activities in 2009

In 2009, 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 2009, the staff started the development of an enhanced SDP for FOF exercises as applied to NPPs and issued a new standalone target-set review inspection procedure. The staff continued to revise the FOF guidance documentation and related inspection procedure. 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 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. 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 in the briefings accurately reflects established parameters. 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. Historically, no conflict of interest has been detected, and no conflict of interest was found this year.

3.3 Results of FOF Inspections

Between January 1, 2009, and December 31, 2009, the NRC conducted FOF inspections at 22 commercial NPPs and identified 29 findings.[3] The FOF inspections identified 26 findings related to areas of the security baseline program. Of these 26 findings, 23 were baseline-related findings. Three findings pertain to the conduct of FOF exercises at three separate sites. All three findings resulted from the failure to effectively protect designated target set components during NRC-evaluated FOF exercises.

As of the end of 2009, the NRC had completed the second year of the second 3-year cycle of NPP FOF inspections (22 sites). Table 1 summarizes the 23 FOF inspections conducted at NPPs in CY 2009, and Table 2 provides cumulative FOF inspection results since 2004.

[3] The NRC conducted a reinspection at one site in 2009.

Table 1: CY 2009 FOF Inspection Program Summary at NPPs

23	Total number of inspections conducted
3	Total number of times a complete target set damaged or destroyed
29	Total number of inspection findings
14	Total number of inspections with no findings
25	Total number of green findings
4	Total number of greater-than-green findings
0	Total number of SL IV violations
0	Total number of greater-than-SL IV violations

Table 2 summarizes the cumulative results of the FOF inspections conducted at NPPs since the first 3-year cycle began in November 2004. Table 2 shows that 78 of the 112 FOF inspections at NPPs since 2004 had no findings (70%). Figure 3 provides a visual summary of the FOF inspection findings at NPPs.

Table 2: Cumulative FOF Inspection Program Results at NPPs (November 2004 through December 2009)

112	Total number of inspections conducted
8	Total number of times a complete target set damaged or destroyed
49	Total number of inspection findings
78	Total number of inspections with no findings
40	Total number of green findings
7	Total number of greater-than-green findings[4]
2	Total number of SL IV violations
0	Total number of greater-than-SL IV violations

[4] Two greater-than-green findings occurred in CY 2007, one occurred in CY 2008, and four occurred in CY 2009.

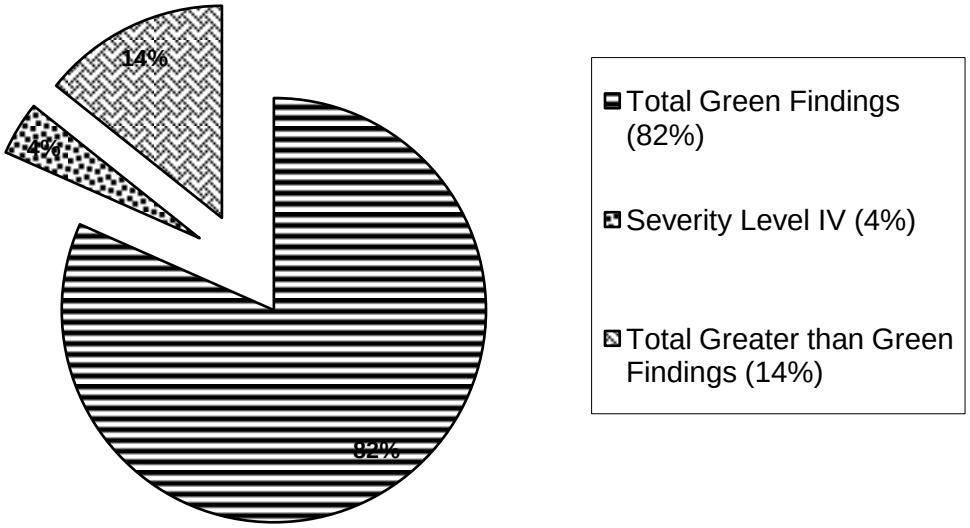

Figure 3: Summary of cumulative FOF inspection findings at NPPs

Of the total number of exercises conducted since November 2004, four 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 insufficient exercise control or excessive administrative holds. Another two exercises were canceled because of potential safety concerns associated with dangerous weather conditions or a plant safety issue. In the latter two cases, the NRC management considered that fewer than three exercises satisfied the inspection requirements because the licensee successfully demonstrated an effective strategy in the other two exercises, with no significant issues identified.

3.4 Discussion of Corrective Actions

In addition to corrective actions due to findings, licensees voluntarily 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 taken in each of these categories.

Licensees will 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. As 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 where a licensee decided that additional security personnel would increase its opportunity to interdict its adversary and thus enhance its ability to prevent the completion of the adversary's mission.

3.5 Future Planned Activities

CY 2010, the third year of the second 3-year cycle of FOF inspections, began with 25 inspections scheduled for the year. Of these, three are followup inspections to assess corrective actions and evaluate other improvements that licensees implemented as a result of previous FOF inspections. 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 protective strategy, protection of SGI, and MC&A. The staff is currently developing the cyber security inspection program based on the "Cyber Security Rule," 10 CFR 73.54, on a pace consistent with licensees' implementation schedules.

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 from 23 inspections (discussed in Section 3) and CAT I security inspection results from 13 inspections (discussed in the SGI and classified versions of this report). Table 3 shows that 69 of the 142 security baseline inspections at NPPS had no findings (49%). Figure 4 provides a graphic summary of the CY 2009 security baseline inspection findings. This information gives an overview of licensee performance within the security cornerstone.

Table 3: CY 2009 Security Inspections (without FOF)

142	Total number of inspections conducted (includes special and augmented inspections)
73	Total number of inspections with findings
69	Total number of inspections with no findings
2	Total number of special and augmented inspections

Table 4: CY 2009 Security Inspection Findings (without FOF)

135	Total number of inspection findings
130	Total number of green findings
3	Total number of greater-than-green findings
2	Total number of SL IV violations
0	Total number of greater-than-SL IV violations

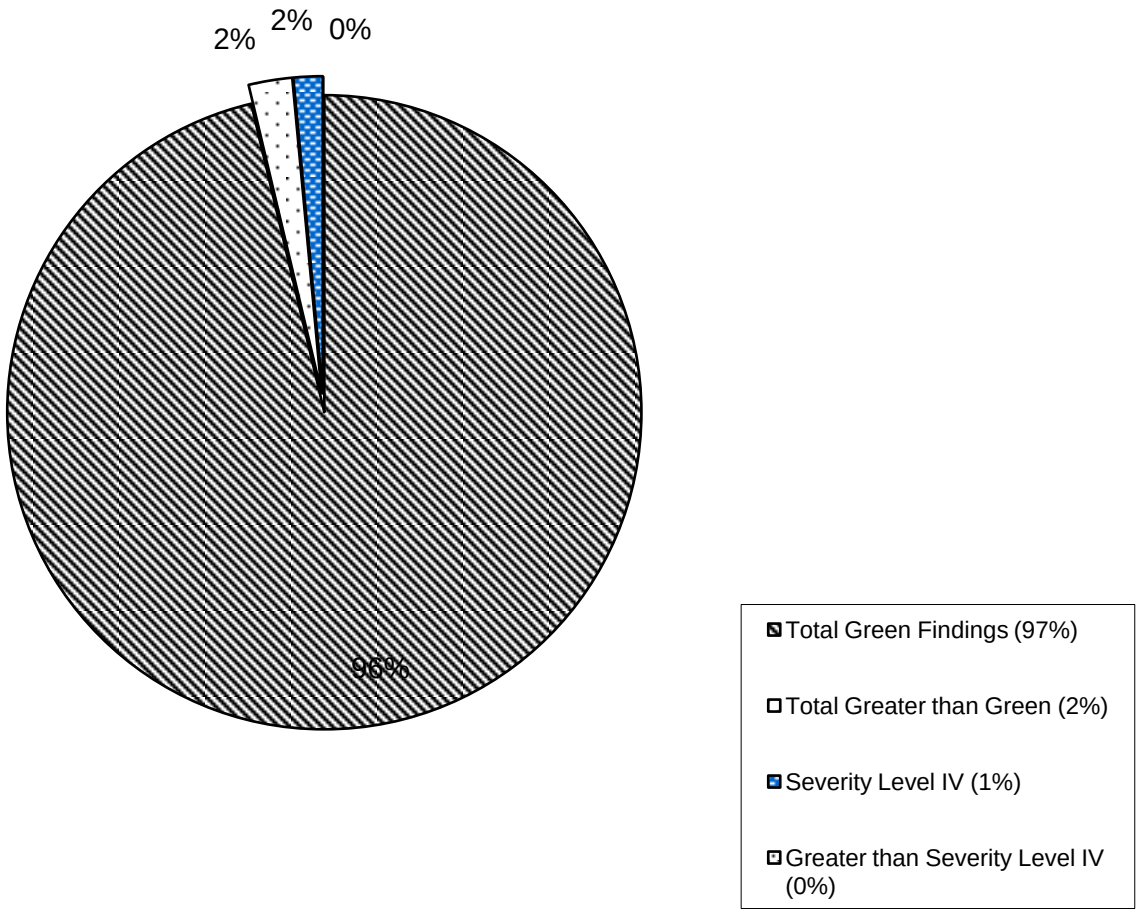

Figure 4: Summary of CY 2009 security inspection findings at NPPs

5. OVERALL REACTOR SECURITY ASSESSMENT

5.1 Overview

The previous two sections describe 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.

5.2 Performance Indicator

Licensees voluntarily report data on the PA detection and assessment equipment. To determine their significance, these data are compared to an established set of thresholds, represented by the colors green, white, yellow, and red (in order of increasing significance). 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 2009, 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 5 summarizes the number of NPPs by their performance, as indicated by security cornerstone action matrix columns.

Most licensees fell 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 2009, 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 action matrix is the unacceptable performance column. Licensees in this column have an overall unacceptable performance and margin for security. In CY 2009, no licensees fell into the degraded cornerstone category, and no licensees fell into either the repetitive degraded cornerstone or the unacceptable performance categories.

Table 5 Summary of Security Action Matrix[5]

Number of Sites	Response Band
58	Licensee Response
6	Regulatory Response
0	Degraded Cornerstone
0	Repetitive Degraded Cornerstone
0	Unacceptable Performance

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

6. CATEGORY I 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. (BWNOG) located in Lynchburg, Virginia, and Nuclear Fuel Services (NFS), located in Erwin, Tennessee. Previously, separate and independent companies operated these two sites. On December 31, 2008, the owners of NFS sold the company to BWNOG, which now operates both sites. However, the names of the two sites remain unchanged. 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 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 posture since September 11, 2001.

The primary objectives of the CAT I security oversight program are to determine whether 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 Rockville, Maryland, and Atlanta, Georgia, conduct inspections using detailed 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 inspection program to make findings, determine their significance, document the 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 two material control and accounting (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, which is implemented by NRC Headquarters inspectors with Regional assistance. In addition, NRC resident inspectors assigned to each CAT I 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, or sabotage of CAT I 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 facilities continue to meet the intent of the regulations. The Classified annex of this report include the results of the CAT I security inspections.

7. STAKEHOLDER COMMUNICATIONS

7.1 Communications with the Public and Industry

In 2006, the Commission reviewed several options to make certain security oversight information available to the public. The Commission decided to place the cover letters to NPP security-related inspection reports (IRs) in the public domain. However, the information contained in the letters does not identify actual or potential vulnerabilities at the inspected plant. The NRC releases to the public its cover letters for security-related IRs issued after May 8, 2006.

As an additional effort to inform and involve stakeholders in the regulatory process, the NRC continues to hold public meetings specifically on nuclear security issues.[6] For example, it presents security topics at the NRC's Regulatory Information Conference, held each spring in Rockville, Maryland, and has held a number of meetings on regulatory guidance for the implementation of the Power Reactor Security Requirements rulemaking, published in the *Federal Register* on March 27, 2009. The draft regulatory guides were published for comment by stakeholders in the spring of 2008. Subsequent to the submission of the final rule to the Commission for consideration, the staff conducted more than 30 meetings, over an 8-month period, with the public and industry stakeholders to review and understand comments submitted on the draft regulatory guidance in support of the rulemaking. The guidance, covering topics including physical security, access authorization, safety/security interface, training and qualification of security personnel, contingency planning, and FOF program enhancements, was published July 2009.

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 potential generic issues. When applicable, the NRC staff supplements periodic security meetings held with the industry and develops generic communications or security advisories as a means of effectively communicating security-related issues to the industry. In CY 2009, the NRC issued nine security advisories, three regulatory issue summaries, and six information notices covering a variety of topics (see the list in the next section). 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 Agency disseminates lessons learned to the industry through the FOF Working Group, which includes security representatives from NRC-licensed facilities.

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

7.2 Calendar Year 2009 List of Generic Communications by Title

Security Advisories (SAs)

SA-09-01, SA-09-02, SA-09-03, SA-09-04	The Presidential Address to a Joint Session of Congress
SA-09-05	Recent Inspection Issues Regarding Intrusion Detection Requirements at Protected Area Boundaries
SA-09-06	Special Security Issue Titled “Laundry”
SA-09-07, SA-09-08, SA-09-09	National Special Security Event for the Pittsburgh (G-20) Summit

Regulatory Issue Summaries (RIS)

RIS-09-10	Communications Between the NRC and Reactor Licensees During Emergencies and Significant Incidents
RIS-09-13	Emergency Response Data System Upgrade from Modem to Virtual Private Network Appliance
RIS-09-15	National Source Tracking System Annual Inventory Reconciliation

Information Notices (IN)

IN 2009-01	National Response Framework
IN 2009-08	NRC Rapid Change Notification of Licensees Following a Physical Attack Against a Facility
IN 2009-19	Hostile Action-Based Emergency Preparedness Drills
IN 2009-24	Sources of Information Related to Potential Cyber Security Vulnerabilities
IN 2009-25	Small Arms Firing Range Safety Issues
IN 2009-28	Summary of Fitness-For-Duty Program Performance Reports for Calendar Year 2008

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's security cornerstone action matrix also includes informing various levels of interested local, State, and Federal organizations of plants with declining performance. In addition, U.S. Department of Homeland Security (DHS) offices in several States routinely receive copies of security IRs associated with the NPPs located in their States.

The NRC continues to support the Homeland Security Council initiative to enhance integrated response planning for power reactor facilities. One significant example of that support is the Integrated Pilot Comprehensive Exercise (IPCE), which is a voluntary, collaborative effort led by the Federal Bureau of Investigation (FBI) in collaboration with DHS, the NRC, and the Nuclear Energy Institute (NEI). IPCE represents the first initiative designed to incorporate Federal, State, and local law enforcement tactical response planning and operations into the concept of integrated response by providing law enforcement tactical teams with opportunities to prepare for, and respond to, simulated security incidents inside commercial NPP sites.

The first IPCE occurred at the Limerick NPP in 2008, and involved senior representatives and planners from Exelon Corporation, the Limerick Township (Pennsylvania) Police, Pennsylvania State Police, FBI Headquarters and Philadelphia Field Office, DHS, the NRC, and NEI. This effort culminated in tabletop and full-scale exercises in November and December 2008, respectively. The IPCE participants produced an after-action report that included lessons learned from the Limerick IPCE. On January 25, 2010, after an extensive vetting and security classification review, DHS disseminated the final Limerick IPCE after-action report to those entities with an official need to know.

The NRC, FBI, DHS, and NEI held interagency meetings in January and February 2009, to discuss the future of this initiative. Those organizations agreed in principle to conduct a second IPCE, and D.C. Cook NPP volunteered to be the host site. The D.C. Cook IPCE will be conducted during fiscal year 2010 and will incorporate lessons learned from the Limerick IPCE. Anticipated participants include D.C. Cook, Berrien County Sheriff's Department, Michigan State Police, Nile Police Department, Medic One (Tactical Medical Personnel), FBI Headquarters and Detroit Field Office, the NRC, DHS, and NEI.