June 28, 2013

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 2012 "Report to Congress on the Security Inspection Program for Commercial Power Reactors and Category I Fuel Cycle Facilities: Results and Status Update." Section 170D.e of Chapter 14 of 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 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 regulatory activities, among several, that the NRC performs to ensure the secure use and management of radioactive and nuclear materials by the commercial nuclear power industry and CAT I fuel cycle facilities.

During calendar year 2012, the NRC conducted 206 security inspections (of which 23 were FOF inspections) at commercial nuclear power reactors and CAT I fuel cycle facilities. These inspections identified 156 findings, 148 of which were of very low security significance and 8 were of greater than very low security significance. Enclosures 2 and 3 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 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 licensing and oversight processes, the NRC is committed to ensuring that licensees continue to provide high assurance that their facilities remain secure.

Enclosure 1 to this letter can be made publicly available; however, Enclosures 2 and 3 contain information that is not for public disclosure. Enclosure 3 must be handled and stored in accordance with Executive Order 13526, "Classified National Security Information." Access to Enclosure 3 should be limited to you and those of your staff who have the appropriate clearance and a need to know. Enclosure 2 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 Enclosure 2 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 Enclosure 2 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

Enclosures:
1. Publically Available Report
2. Safeguards Information Report
3. Confidential Report

cc: Senator David Vitter

Identical letters sent to:

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

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 Jeff Sessions

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 Paul Tonko

# 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 2012

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.e 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 eighth annual report, which covers calendar year 2012. 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, Revision 6, "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

# FIGURES



# TABLES

# ACRONYMS

| | |
|---|---|
| 10 CFR | Title 10 of the *Code of Federal Regulations* |
| CAT I | Category I |
| CSP | cyber security plan |
| 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 |
| HEUMF | highly enriched uranium manufacturing facility |
| IMC | inspector manual chapter |
| IPCE | integrated pilot comprehensive exercise |
| 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 |
| PIDAS | perimeter intrusion detection and assessment system |
| PPSDP | physical protection significance determination process |
| ROP | Reactor Oversight Process |
| SDP | significance determination process |
| SGI | Safeguards Information |
| SL | severity level |
| SNM | special nuclear material |
| SSNM | strategic special nuclear material |
| U.S.C. | United States Code |

PAGE INTENTIONALLY LEFT BLANK

# 1. INTRODUCTION

This report fulfills the requirements of Section 170D.e 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) 2012. 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 activities that the NRC performs to ensure the secure and safe use and management of radioactive and nuclear materials by the commercial nuclear power industry and CAT I fuel cycle facilities. 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 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 at least a formula quantity of SSNM, which is defined in Title 10 of the *Code of Federal Regulations* (10 CFR) 70.4, "Definitions," 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.

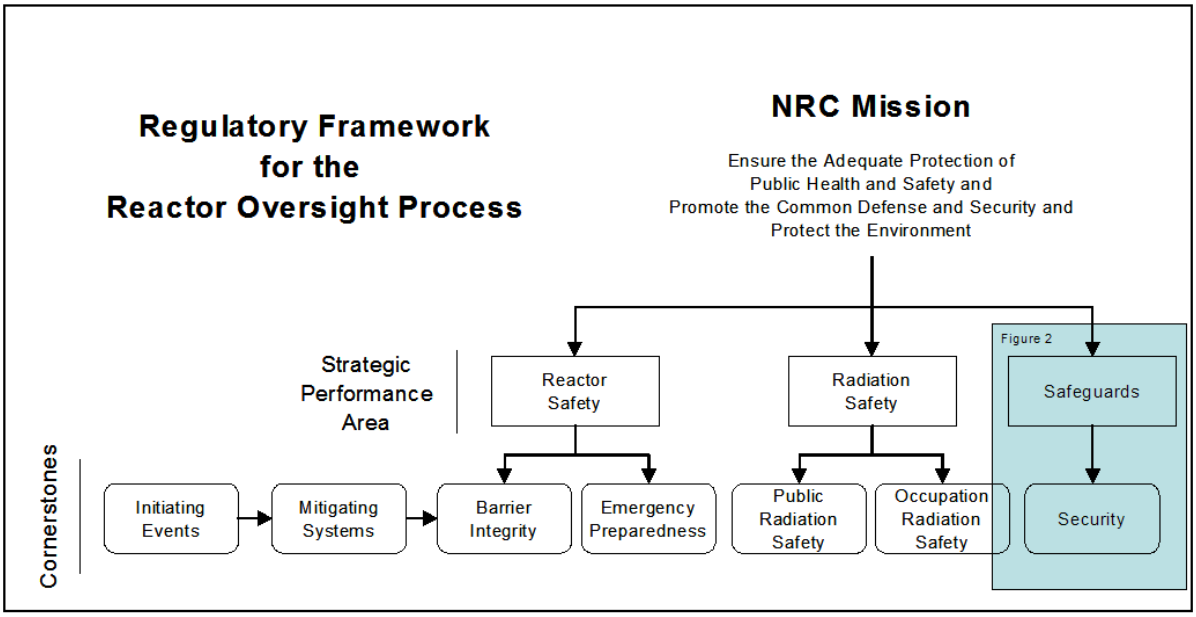


**Figure 1: Cornerstones of the Reactor Oversight Process**

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 NPP licensees comply with appropriate regulatory requirements and can provide high assurance of adequate protection against the design basis threat (DBT) of radiological sabotage.

The objectives of the security cornerstone's baseline inspection program are: (1) to gather sufficient, factual inspection information to determine whether a licensee is meeting the objective of the security cornerstone, which is to provide high assurance that the licensee's security system and MC&A program can protect against the DBT of radiological sabotage; (2) to determine the licensee's ability to identify, assess the significance of, and effectively correct security issues commensurate with the significance of the issue; (3) to determine whether licensees, in conjunction with established protocols with external agencies, are capable of deterring and protecting against the DBT of radiological sabotage; (4) to verify the accuracy and completeness of PI data used in conjunction with inspection findings to assess the security performance of power reactor licensees; (5) to provide a mechanism for the NRC to remain cognizant of security status and conditions; and (6) to identify those significant issues that may have generic applicability or cross-cutting applicability to the safe and secure operation of licensee facilities subject to the requirements of 10 CFR Part 73, "Physical protection of plants and materials."

The security cornerstone's baseline inspection program includes 11 inspectable areas to be reviewed periodically at each power reactor facility (see Figure 2). One of the inspectable areas—contingency response—is assessed through the conduct of FOF inspections, which the next section describes in detail.

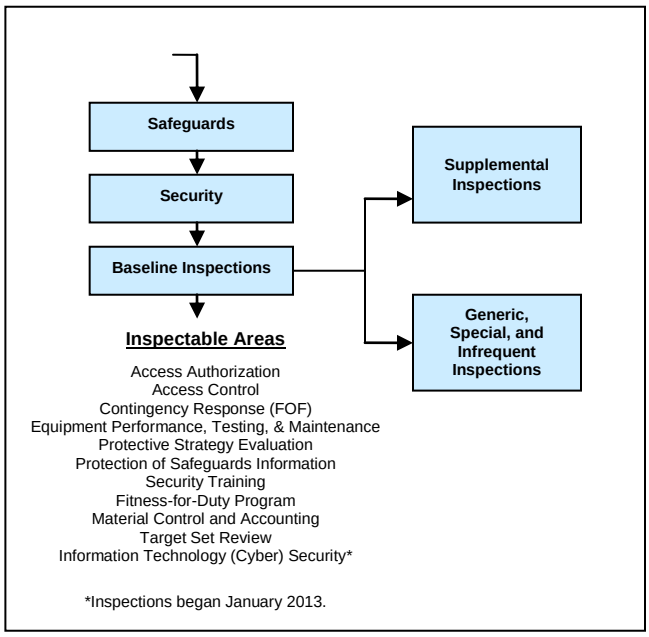


**Figure 2: Inspectable Areas of the Security Cornerstone**

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 ROP action matrix[1] to ensure that the licensee takes corrective actions to address and prevent recurrence of the performance weaknesses (see Figure 3).

[1] Additional information on the ROP action matrix is provided in Section 5.

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.

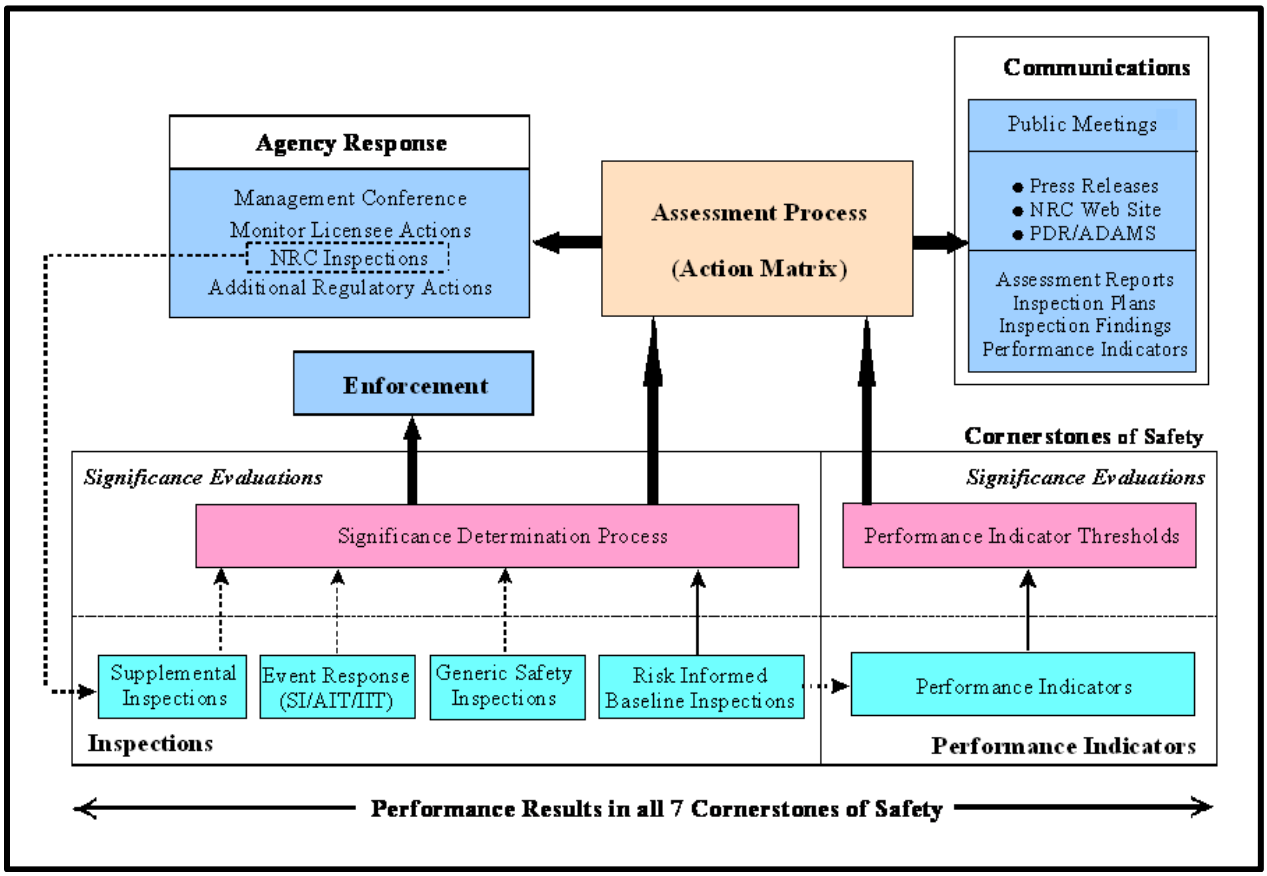


**Figure 3: Reactor Oversight Process**

## 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 significance determination process (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 in which 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 (inspection findings with very low safety or security significance)
- white (inspection findings with low to moderate safety or security significance)
- yellow (inspection findings with substantial safety or security significance)
- red (inspection findings with high safety or 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 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 typically is 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. SL IV violations are those that are less serious, but are of more than minor concern, that resulted in no or relatively inappreciable potential safety or security consequences. SL III violations are those that resulted in, or could have resulted in, moderate safety or security consequences. SL II violations are those that resulted in, or could have resulted in, significant safety or security consequences. SL I violations are those that resulted in, or could have resulted in, serious safety or security consequences. For particularly significant violations, the Commission reserves the use of its discretion to assess civil penalties in accordance with Section 234 of the Atomic Energy Act of 1954, as amended.

## 2.4 Cyber Security

Shortly after the terrorist attacks of September 11, 2001, the NRC ordered its NPP licensees to enhance their overall security. The order included requirements for addressing certain cyber security threats and vulnerabilities. A year later, the NRC issued another order that, for the first time, added cyber attacks to the adversary threat types that plants must defend against. Subsequently, these orders were codified through the issuance of 10 CFR 73.54, "Protection of digital computer and communication systems and networks," commonly referred to as the "Cyber Security Rule." This rule requires that licensees protect digital computer systems and networks associated with safety-related and important-to-safety functions, security functions, and emergency preparedness functions.

Previously, licensees addressed elements of cyber security in a section of their physical security plans. The new regulation required licensees to develop a more comprehensive cyber security program and to incorporate it as part of their physical security program. Additionally, licensees were required to submit a cyber security plan (CSP) and an implementation schedule for NRC approval. Subsequently, the NRC reviewed and approved licensees' CSPs and the implementation schedules. After the NRC's approval, licensees began implementing the commitments in the CSP to meet the new requirements.

In parallel with the review and approval of the CSPs, the NRC began developing a Cyber Security Oversight Program, with plans to incorporate this new program into its current ROP in early CY 2013. In order to establish its oversight process, the NRC staff developed a Cyber Security Inspector Training Program. The NRC conducted its first 2-week inspector training course in January 2011, and the second course was conducted in October 2012. As of October 2012, the NRC had trained approximately 60 personnel (inspectors and cyber security specialists). Additionally, in 2012, the staff developed an inspection program and a process for evaluating the significance of cyber security inspection findings. The development of the inspection program was accomplished collaboratively, to include the following stakeholders: NRC staff, the industry, Federal partners and representatives from the U.S. Department of Homeland Security (DHS), the Federal Energy Regulatory Commission, and the National Institute of Standards and Technology. In a way consistent with how the NRC developed other inspection elements within the ROP, the NRC piloted the cyber security inspection process by conducting one pilot evaluation at Watts Bar Nuclear Plant, Unit 2, and a second pilot evaluation at Clinton Power Station, Unit 1. Together, the evaluations resulted in successful completion of the pilot process.

With the development of the Cyber Security Oversight Program, completion of the cyber security training for inspectors, and successful pilot inspections, the NRC began inspections of the licensee implementation of CSPs in January 2013.

The NRC developed and issued a cyber security roadmap to evaluate the need for cyber security requirements for fuel cycle facilities, nonpower reactors, independent spent fuel storage installations, and byproduct materials licensees.[2] A cyber security working group was established in 2011 to review current fuel cycle facilities cyber security programs to determine how this group of licensees protects its digital assets from cyber attacks and to determine if the NRC needed to take additional action to have these facilities strengthen their programs. The working group specifically looked at digital systems performing, supporting, or associated with critical functions, such as safety, important-to-safety, security, emergency preparedness, information security, and MC&A. The working group designed a four step assessment process for examining cyber security programs at fuel cycle facilities that included: (1) requesting fuel cycle facilities respond to an NRC questionnaire; (2) performing site visits to a representative cross-section of the fuel cycle licensees; (3) analyzing licensees' documentation of their cyber security programs and observing how the programs were implemented; and (4) issuing a final report documenting observations. The staff is currently developing a recommended path forward for fuel cycle facilities.

[2] For more information on the NRC's cyber security roadmap, please refer to http://www.nrc.gov/reading-rm/doc-collections/commission/secys/2012/2012-0088scy.pdf.

The implementation of this roadmap will ensure that appropriate levels of cyber security actions are implemented in a timely and efficient manner at all NRC-licensed facilities and will identify if any program improvements are needed.[3]

[3] For more information on the NRC's Cyber Security Initiative for Fuel Cycle Facilities, please refer to http://www.nrc.gov/security/domestic/phys-protect/reg-initiatives/fuel-cycle-cyber-security.html.

# 3. FORCE-ON-FORCE INSPECTION PROGRAM

## 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. At a CAT I fuel cycle facility, a similar process is used to assess the effectiveness of those licensee's protective strategy capabilities relative to the DBTs of radiological sabotage and theft or diversion of SNM.

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.[4] However, it might 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 these measures and ensure that they effectively address the noted deficiency.

An FOF inspection usually consists of three FOF exercises. In an instance in which a licensee conducts two successful exercises that demonstrate an effective strategy, upon request by the licensee, the NRC may allow a third "training" exercise that is not evaluated under the inspection procedure. 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

[4] 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.

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.

## 3.2 Program Activities in 2012

In 2012, the FOF inspection program continued to focus on 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.

In CY 2009, staff from the Office of Nuclear Security and Incident Response conducted a review of the FOF Inspection Program and began to consider ways to enhance the assessment of the FOF Inspection Program results and SDP. The FOF exercises historically had been conducted as a more or less pass/fail assessment. The NRC staff had identified the potential for this type of assessment to result in a false-positive or false-negative assessment of the protective strategy. A false-positive assessment would be an inspection with "marginal" licensee protective strategy performance during the three exercises (e.g., adversaries destroy a significant portion of the target set components or in some cases adversaries are neutralized at the last target set component), but no complete target set was destroyed. In this case, the pass/fail determination would result in a pass with no requirement for corrective action. The staff had concerns that this "marginal" performance may truly indicate a poor overall protective strategy. A false-negative assessment would be an inspection with two exercises demonstrating a strong licensee protective strategy performance and strong overall security programs, but one exercise that resulted in the destruction of a complete target set (e.g., armed response officers not provided with accurate information on adversary movement and fail to go to the correct location to neutralize adversary). In some cases, the inspection team may have determined that the one poor exercise performance was an "anomaly", due to control issues or other artificialities. In a case of this type, the poor performance could be viewed as a false-negative assessment of the overall protective strategy.

Enhancements to the FOF assessment and SDP tool provided a process for assessing "marginal" performance and gave credit for strong overall security performance that the former system did not allow to reduce the likelihood of false-positive and false-negative results. The NRC staff conducted public meetings and closed industry meetings to present the final proposal to enhance the FOF SDP, which was under consideration for future FOF exercises at NPPs. After this multiyear effort to enhance the FOF SDP, which began in CY 2009 and involved interaction with both internal and external stakeholders, staff completed work on the FOF SDP in July 2012. Data on the impact of any change to the significance of a finding and comments from stakeholders were reviewed and incorporated, as appropriate, into revisions of the FOF SDP. The revised FOF SDP was finalized and issued on July 27, 2012.

In 2009, the NRC issued a standalone target set review inspection procedure, which was revised on August 16, 2011, and which the agency used to conduct 19 target set reviews in CY 2012. 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 adversaries used for inspections continued to meet expectations for a credible, well-trained mock adversary force. FOF team members provide the necessary monitoring of information to assist the adversary force in defining and developing mission plans used during FOF exercises. Additionally, FOF team members review adversary team briefings to ensure that the information provided accurately reflects established parameters. U.S. Special Operations Command members also provide support to the NRC inspection team in tactics planning. Because the adversaries are 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, 2012, and December 31, 2012, the NRC conducted 23 FOF inspections[5] (at 22 commercial NPPs and 1 CAT I fuel cycle facility) and identified 23 findings 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 2012, the NRC had completed the second year of the third 3-year cycle of FOF inspections. Table 1 summarizes the 23 FOF inspections conducted in CY 2012.

**Table 1: Calendar Year 2012 Force-on-Force Inspection Program Summary**

| | |
|---|---|
| 23 | Total number of inspections conducted |
| 11 | Total number of inspections with findings |
| 12 | Total number of inspections with no findings |
| 1 | Total number of complete target sets simulated to be damaged or destroyed |
| 23 | Total number of inspection findings |
| 19 | Total number of green findings |
| 1 | Total number of greater than green findings |
| 3 | Total number of SL IV findings |
| 0 | Total number of greater than SL IV findings |

Of the total number of exercises conducted in CY 2012, 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 deemed indeterminate because of site controller training and controller performance failures. Furthermore, two additional exercises were canceled due to potential safety concerns associated with dangerous weather conditions and other extenuating circumstances. In both of these instances, the NRC management considered that fewer than three exercises satisfied the inspection requirements because the licensees had 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

[5] The NRC conducted a re-inspection at one site in CY 2012, which is included in the 23 FOF inspections.

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 might 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 might 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 might 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 licensee's plans as required by 10 CFR Part 73, "Physical protection of plants and materials," they become lasting regulatory requirements.

## 3.5 Future Planned Activities

CY 2013, the third year of the third 3-year cycle of FOF inspections, began with 24 inspections scheduled for the year. Of these, two are follow-up inspections to assess corrective actions and evaluate other improvements that licensees implemented as a result of CY 2012 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; Protective Strategy Evaluation; Security Training; Equipment Performance, Testing, and Maintenance; Fitness for Duty Program; Protection of Safeguards Information (SGI); Review of Power Reactor Target Sets; and MC&A. Furthermore, the NRC initiated its Cyber Security Inspection Program based on the Cyber Security Rule, 10 CFR 73.54, "Protection of digital computer and communication systems and networks," in January 2013.

## 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 the 23 inspections (discussed in Section 3) and the CAT I fuel cycle facility security inspection results. Table 2 shows that 90 of the 173 security baseline inspections at NPPs had no findings (52 percent). Figure 3 provides a graphic summary of the CY 2012 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 and Classified versions of this report.

**Table 2: Calendar Year 2012 Security Inspections at Nuclear Power Plants (without Force-on-Force)**

| | |
|---|---|
| 173 | Total number of baseline inspections conducted |
| 83 | Total number of baseline inspections with findings |
| 90 | Total number of baseline inspections with no findings |
| 3 | Total number of special and augmented inspections |

**Table 3: Calendar Year 2012 Security Inspection Findings at Nuclear Power Plants (without Force-on-Force)**

| | |
|---|---|
| 130 | Total number of inspection findings |
| 121 | Total number of green findings |
| 5 | Total number of greater than green findings |
| 3 | Total number of SL IV findings |
| 1 | Total number of greater than SL IV findings |

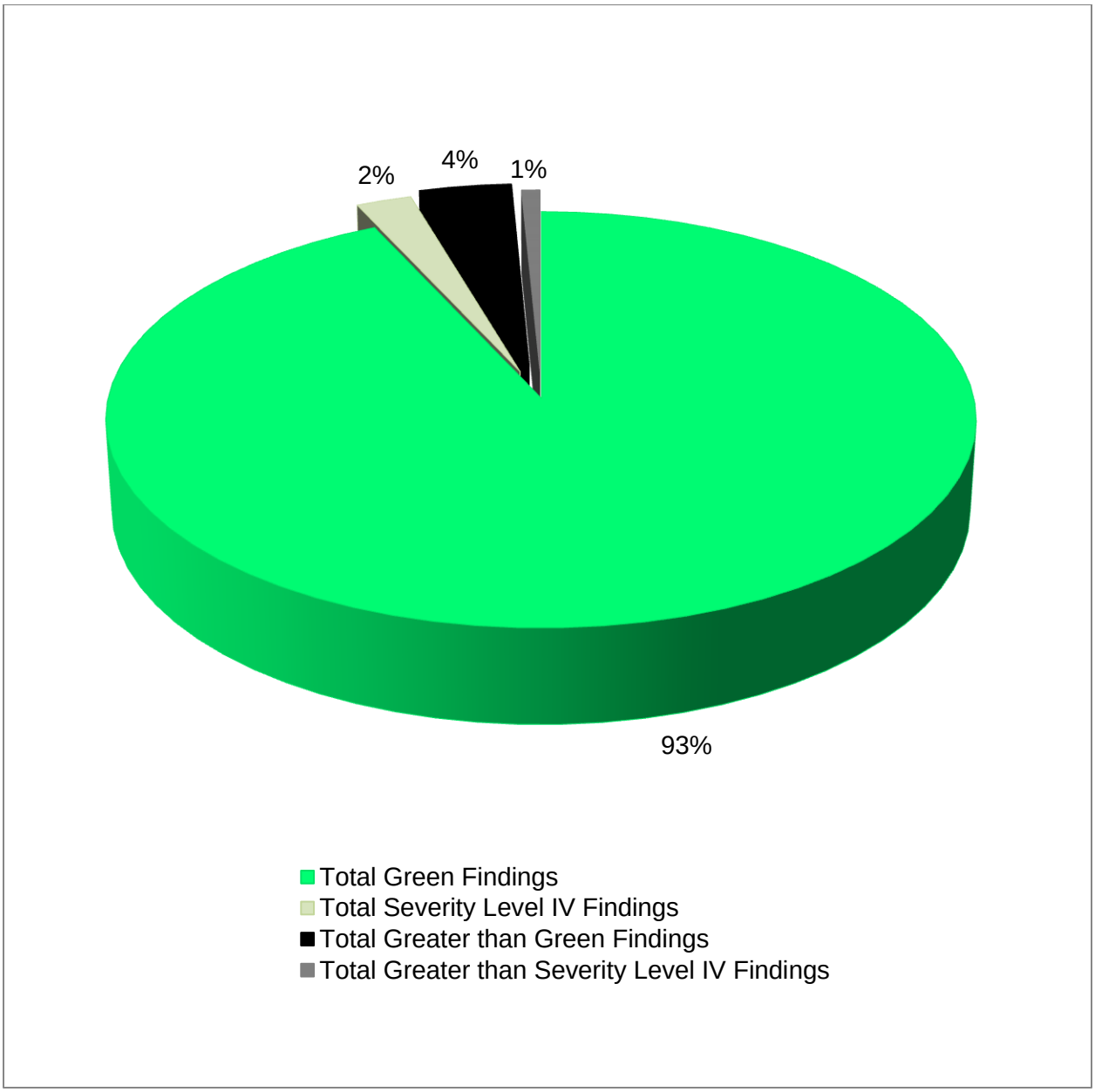


**Figure 4: Summary of Calendar Year 2012 Baseline Security Inspection Findings at Nuclear Power Plants**

# 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 PIs would be considered when determining appropriate agency response. Since 2004, the security cornerstone has been treated in a way 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 was completed in August 2012.

As noted above, the staff revised agency procedures to reflect an integrated approach to performance assessment across all seven ROP cornerstones. As such, the NRC began including security-related inputs (inspection findings and PIs) under a combined agency assessment program and has discontinued a separate security performance assessment process. Licensees receive one assessment letter that will document an assessment across all seven ROP cornerstones. Security-related information is not included in the assessment letters and is sent to licensees in separate correspondence that is not publicly available.

Similarly, the NRC modified the ROP public Web site to include all seven ROP cornerstones when the quarterly updates to Action Matrix inputs are posted. The Web site displays security inputs that are determined to be of very low security significance (i.e., of green significance); however, instead of including the actual color, a security input of white, yellow, or red significance will be a different color (blue) to reflect greater than green significance. Not specifying the actual color of greater than green security inputs is consistent with current Commission policy. Similarly, specific information about all security performance deficiencies will continue not to be publicly available, consistent with current Commission policy.

## 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 2012, 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. To review the listing of plants and their current PIs, please refer to the ROP Performance Indicators Summary Web page located at http://www.nrc.gov/NRR/OVERSIGHT/ASSESS/pi_summary.html.

## 5.3 Reactor Oversight Process Action Matrix

The ROP Action Matrix identifies the range of NRC and licensee actions and the appropriate level of communication for different levels of licensee performance. The ROP Action Matrix describes a graded approach for addressing performance issues and was developed with the philosophy that within a certain level of safety performance (e.g., the licensee response band), licensees would address their performance issues without additional NRC engagement beyond the baseline inspection program. NRC actions beyond the baseline inspection program will normally occur only if assessment input thresholds are exceeded. The ROP Action Matrix collects information from inspections and PIs to enable the agency to arrive at objective conclusions about the licensee's performance. Based on this assessment information, the NRC determines the appropriate level of agency response, including supplemental inspection and pertinent regulatory actions ranging from management meetings up to and including orders for plant shutdown.

The ROP action matrix has five response columns: licensee response, regulatory response, degraded cornerstone, repetitive degraded cornerstone, and unacceptable performance. The licensee response column 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 one white input in any cornerstone or no more than two white inputs in any strategic performance area, and the cornerstone objective was met with minimal degradation in performance. The degraded cornerstone column categorizes a performance level indicated by two white inputs or one yellow input in any cornerstone or three white inputs in any strategic performance area, while meeting the cornerstone objective with moderate degradation in performance. If a licensee falls into the repetitive degraded cornerstone column, it has received multiple yellow inputs, multiple degraded cornerstones, or at least one red input, while meeting the cornerstone objective with longstanding issues or significant degradation in performance. The most significant column in the ROP action matrix is the unacceptable performance column. Unacceptable performance represents situations in which the NRC lacks reasonable assurance that the licensee can or will conduct its activities to ensure protection of public health and safety. Licensee performance is unacceptable, and continued plant operation is not permitted within this column.

The Action Matrix Summary, posted on the NRC public Web page, reflects overall plant performance and is updated regularly to reflect inputs from the most recent PIs and inspection findings. Although the Security Cornerstone is included in the ROP assessment program, the Commission has decided that specific information related to findings and PIs pertaining to the Security Cornerstone will not be publicly available to ensure that security information is not provided to a possible adversary. Other than the fact that a finding or PI is green or greater than green, security-related information will not be displayed on the public Web page. To review the listing of plants and their current Action Matrix Column, please refer to the ROP Action Matrix Summary and Current Regulatory Oversight Web page located at http://www.nrc.gov/NRR/OVERSIGHT/ASSESS/actionmatrix_summary.html.

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. Although Fort Calhoun Station was moved into the IMC 0350 oversight process, ROP baseline security inspections continue as scheduled. For additional information on the Fort Calhoun Station's change in regulatory oversight, please see the NRC's letter dated December 13, 2011, available in the Agencywide Documents Access and Management System at https://adamsxt.nrc.gov/WorkplaceXT/getContent?id=release&vsId=%7B537F305A-F7D1-401C-8496-F921CFAB5FD2%7D&objectStoreName=Main. .Library&objectType=document.

The IMC 0350 oversight process is implemented at facilities in an extended shutdown condition because of significant performance concerns in order to: (1) establish criteria for the oversight of licensee performance for licensees that are in a shutdown condition as a result of significant performance problems or operational event(s); (2) ensure that when the plant is in a shutdown condition as a result of performance problems and/or an operational event, the NRC communicates a unified and consistent position in a clear and predictable manner to the licensee, public, and other stakeholders; (3) establish a record of the major regulatory and licensee actions taken and technical issues resolved leading to approval for restart and to the eventual return of the plant to the ROP; (4) verify that licensee corrective actions are sufficient prior to restart; and (5) provide assurance that following restart, the plant will be operated in a manner that provides adequate protection of public health and safety.

PAGE INTENTIONALLY LEFT BLANK

# 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 acts of radiological sabotage and theft or diversion of SNM. 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.

In a way 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.

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 and classified versions of this report include 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 NRC places the cover letters to NPP security-related inspection reports in the public domain. The information contained in the letters does not identify actual or potential vulnerabilities at the inspected plant. The NRC has been releasing its cover letters to the public for security-related inspection reports since May 2006.

The NRC continues to hold public meetings specifically on nuclear security issues.[6] For example, the agency presents a variety of security topics at its Regulatory Information Conference, held each spring in Rockville, Maryland.[7] Security topics at the Regulatory Information Conference range from security-related rulemaking efforts to activities associated with security inspection and oversight of NRC licensed facilities to the latest Cyber Security and Emergency Preparedness and Response activities undertaken by the agency.

The NRC also communicates with the public, licensees, and other stakeholders by disseminating generic communications 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 other key stakeholders and develops generic communications, such as security advisories, as a means of effectively communicating security-related issues. In CY 2012, the NRC issued 17 security advisories covering a variety of topics. There was one security-related regulatory issue summary and one information notice issued in CY 2012 (see Section 7.2 for a complete list).

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.

---

6 For more information on the NRC's public meeting schedule, please refer to http://www.nrc.gov/public-involve/public-meetings/index.cfm.

7 For more information on the Regulatory Information Conference, please refer to http://www.nrc.gov/public-involve/conference-symposia/ric/.

## 7.2 Calendar Year 2012 List of Generic Communications by Title[8]

Security Advisories

| | |
|---|---|
| SA-12-01, SA-12-02, SA-12-03, SA-12-04 | "National Special Security Event for the 2012 Presidential State of the Union Address" |
| SA-12-05 | "Security of Instrument Calibrators and Other Devices with Radioactive Material in Quantities of Concern Located Outside of the Power Reactor Protected Area" |
| SA-12-06 | "Security of Radioactive Sources in Quantities of Concern Located at Facilities Outside of a Fuel Cycle Facility Protected Area/Controlled Access Area" |
| SA-12-07, SA-12-08, SA-12-09 | "National Special Security Event for the 2012 NATO Summit to be Held in Chicago, Illinois" |
| SA-12-10 | "Protection of Safeguards Information (SGI): Performance and Specific Requirements for SGI and SGI-M" |
| SA-12-11, SA-12-12, SA-12-13 | "National Special Security Event for the 2012 Republican National Convention to be Held in Tampa, Florida" |
| SA-12-14, SA-12-15, SA-12-16 | "National Special Security Event for the 2012 Democratic National Convention to be Held in Charlotte, North Carolina and Concord, North Carolina" |
| SA-12-17 | "Security Breach at the Y12 Department of Energy Nuclear Facility" |

Regulatory Issue Summaries

| | |
|---|---|
| RIS-12-03 | "Reintegration of Security into the Reactor Oversight Process Assessment Program" |

Information Notices

| | |
|---|---|
| IN-2012-18 | "Failure to Properly Augment Emergency Response Organizations" |

[8] All publicly available security advisories, regulatory issue summaries, and information notices can be found electronically on NRC's Generic Communications web page at http://www.nrc.gov/reading-rm/doc-collections/gen-comm/.

## 7.3 Security Breach at the Department of Energy's Y-12 National Security Complex

On July 28, 2012, without authorization, three protesters successfully breached the perimeter intrusion detection and assessment system (PIDAS) at the U.S. Department of Energy's Y-12 National Security Complex nuclear facility. The protesters, who call themselves the "Transform Now Plowshares," traveled approximately 600 meters on foot through site property within the owner-controlled area. Once they reached the first PIDAS security barrier, a chain link fence, they began breaching activities with bolt cutters. They then pried the fence open and crawled through the opening. During this time, the protesters constantly alarmed the intrusion detection systems until they exited the PIDAS. While security forces assessed the alarming condition, the assessment was not performed in accordance with established facility security standards. The protesters continued to use the same breaching method on the remaining chain link fence security barriers until they reached the Highly Enriched Uranium Manufacturing Facility (HEUMF).

Once inside all PIDAS security barriers, the protestors defaced an exterior wall of the HEUMF with paint and fake blood. Additionally, the protestors used a hammer to inflict superficial damage to an exterior portion of a wall. According to DOE, at no time was there a risk to the integrity of the HEUMF.

After breaching the PIDAS, the protesters were detained by site security and turned over to local law enforcement. During the investigation, it was discovered that the protesters had a variety of tools and items for use during the breach. These tools and items included flashlights, binoculars, red "danger" tape, backpacks, bolt cutters, hammers, spray paint, and paraphernalia related to their organization and cause.

Although the Y-12 facility is not regulated by the NRC, the NRC issued a security advisory to assist facility managers and other security personnel responsible for protecting NRC-licensed facilities and radioactive materials in implementing detection and assessment. Recipients were encouraged to review this information related to the Y-12 nuclear facility breach for applicability to their facilities and to consider actions, as appropriate, that could prevent similar problems. However, suggestions contained in the security advisory were not NRC requirements; therefore, no specific action or written response was required.

The advisory reminded NRC-licensed facilities that applicable requirements for intrusion detection and assessment are found in NRC regulations, applicable orders, site security plans, or site contingency plans. The advisory emphasized that these requirements are to be met at all times, allowing security forces the capability to detect and assess unauthorized persons and facilitate an effective and appropriate response. Lastly, the advisory suggested that licensees review their procedures and current practices for prompt detection and assessment to ensure that they comply with applicable requirements and remain vigilant against unauthorized entry into the PA or facility boundary.

## 7.4 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. From 2007–2012, the NRC participated in the Integrated Pilot Comprehensive Exercise (IPCE) initiative, which was a voluntary collaborative effort between the Federal Bureau of Investigation (FBI), DHS, the NRC, the Nuclear Energy Institute (NEI), and the nuclear power industry. The IPCE provided Federal, State, and local law enforcement tactical teams with the opportunity to plan and exercise their responses to simulated security incidents inside three NPP sites: Limerick Generating Station, Donald C. Cook Nuclear Plant, and the Indian Point Nuclear Generating Station.

In 2012, the NRC, FBI, DHS, NEI, and the nuclear power industry decided to transition IPCE from a pilot phase to a more durable, repeatable process focusing on core integrated response activities, such as data collection, planning, and plan validation. This new approach was adopted to integrate several complementary integrated response activities into a single initiative to gain efficiencies in effort, time, and resources. Two sites, Surry Power Station and Davis-Besse Nuclear Power Station, volunteered to spearhead the new approach. The integrated response planning activities at Surry were completed in December 2012, and the activities at Davis-Besse are planned to occur in 2013. The NRC, FBI, DHS, NEI, and nuclear power industry continue to work towards establishing a schedule of recurring activities at all NPP sites.