U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NUREG-1885, Rev. 7

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 2013

Office of Nuclear Security and Incident Response

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at NRC's Public Electronic Reading Room at http://www.nrc.gov/reading-rm.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and Title 10, "Energy," in the *Code of Federal Regulations* may also be purchased from one of these two sources.

1. The Superintendent of Documents
   U.S. Government Printing Office
   Mail Stop SSOP
   Washington, DC 20402–0001
   Internet: bookstore.gpo.gov
   Telephone: 202-512-1800
   Fax: 202-512-2250
2. The National Technical Information Service
   Springfield, VA 22161–0002
   www.ntis.gov
   1–800–553–6847 or, locally, 703–605–6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:

Address: U.S. Nuclear Regulatory Commission
Office of Administration
Publications Branch
Washington, DC 20555-0001
E-mail: DISTRIBUTION.RESOURCE@NRC.GOV
Facsimile: 301–415–2289

Some publications in the NUREG series that are posted at NRC's Web site address http://www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852–2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—

American National Standards Institute
11 West 42nd Street
New York, NY 10036–8002
www.ansi.org
212–642–4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor-prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG–XXXX) or agency contractors (NUREG/CR–XXXX), (2) proceedings of conferences (NUREG/CP–XXXX), (3) reports resulting from international agreements (NUREG/IA–XXXX), (4) brochures (NUREG/BR–XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG–0750).

DISCLAIMER: This report was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any employee, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product, or process disclosed in this publication, or represents that its use by such third party would not infringe privately owned rights.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NUREG-1885, Rev. 7

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 2013

Manuscript Completed: July 2014
Date Published: July 2014

Office of Nuclear Security and Incident Response

ABSTRACT

This report fulfills the requirements of Section 170D.e of Chapter 14 of the Atomic Energy Act of 1954 (42 U.S.C. §2201d.e) 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 ninth annual report, which covers calendar year 2013. 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 7, "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.

CONTENTS

FIGURES

TABLES

ACRONYMS

10 CFR	Title 10 of the *Code of Federal Regulations*
ADAMS	Agencywide Documents Access and Management System
AIT	Augmented Inspection Team
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
IIT	Incident Investigation Team
IMC	Inspection 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
OPPD	Omaha Public Power District
PDR	Public Document Room
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
TI	Temporary Instruction
U.S.C.	*United States Code*

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. §2201d.e), 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) 2013. 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 many 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 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 to 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 commercial nuclear 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, "Energy," 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.

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 commercial 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.

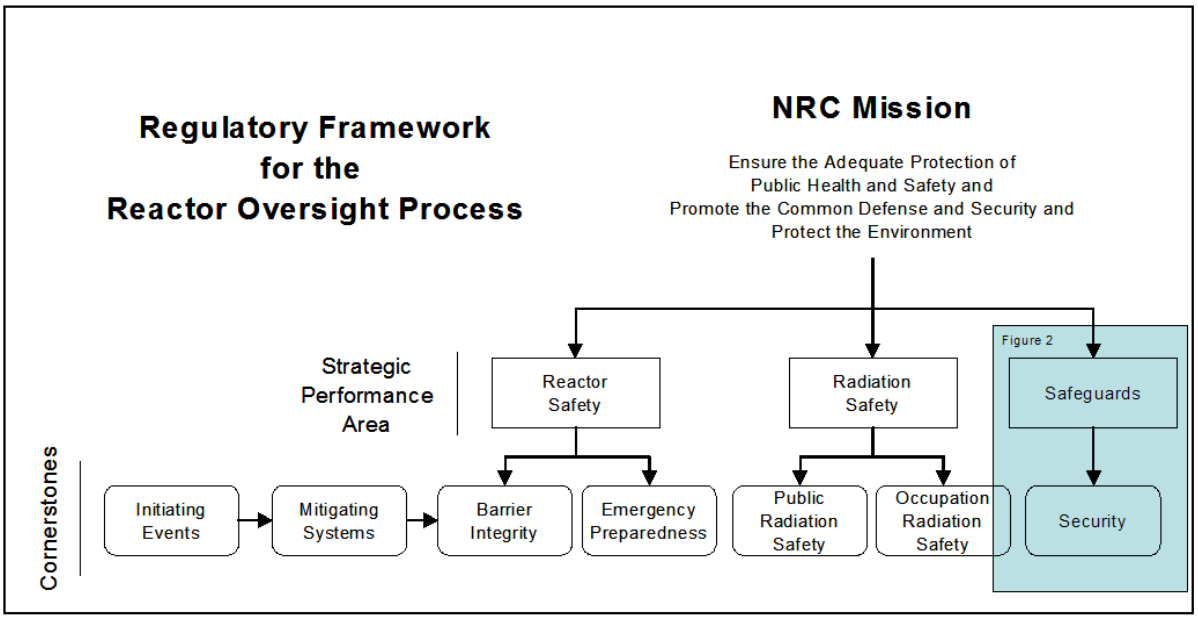

Figure 1: Cornerstones of the Reactor Oversight Process

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 are operating safely and securely within applicable regulatory requirements and can provide high assurance that the licensee's security system and MC&A program use a defense-in-depth approach and can protect against the design basis threat (DBT) of radiological sabotage from external and internal threats.

The objectives of the security 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 Section 4 describes in detail.

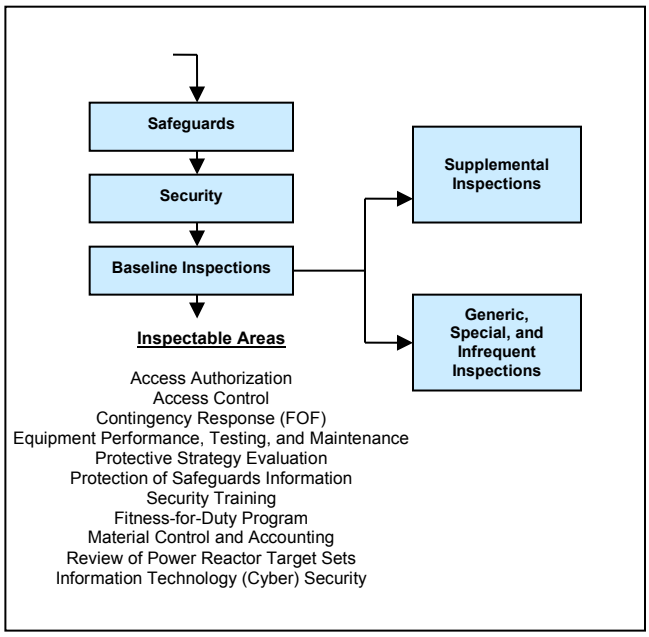

Figure 2: Inspectable Areas of the Security Cornerstone

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).

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

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

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 strike or walkout by its security force.

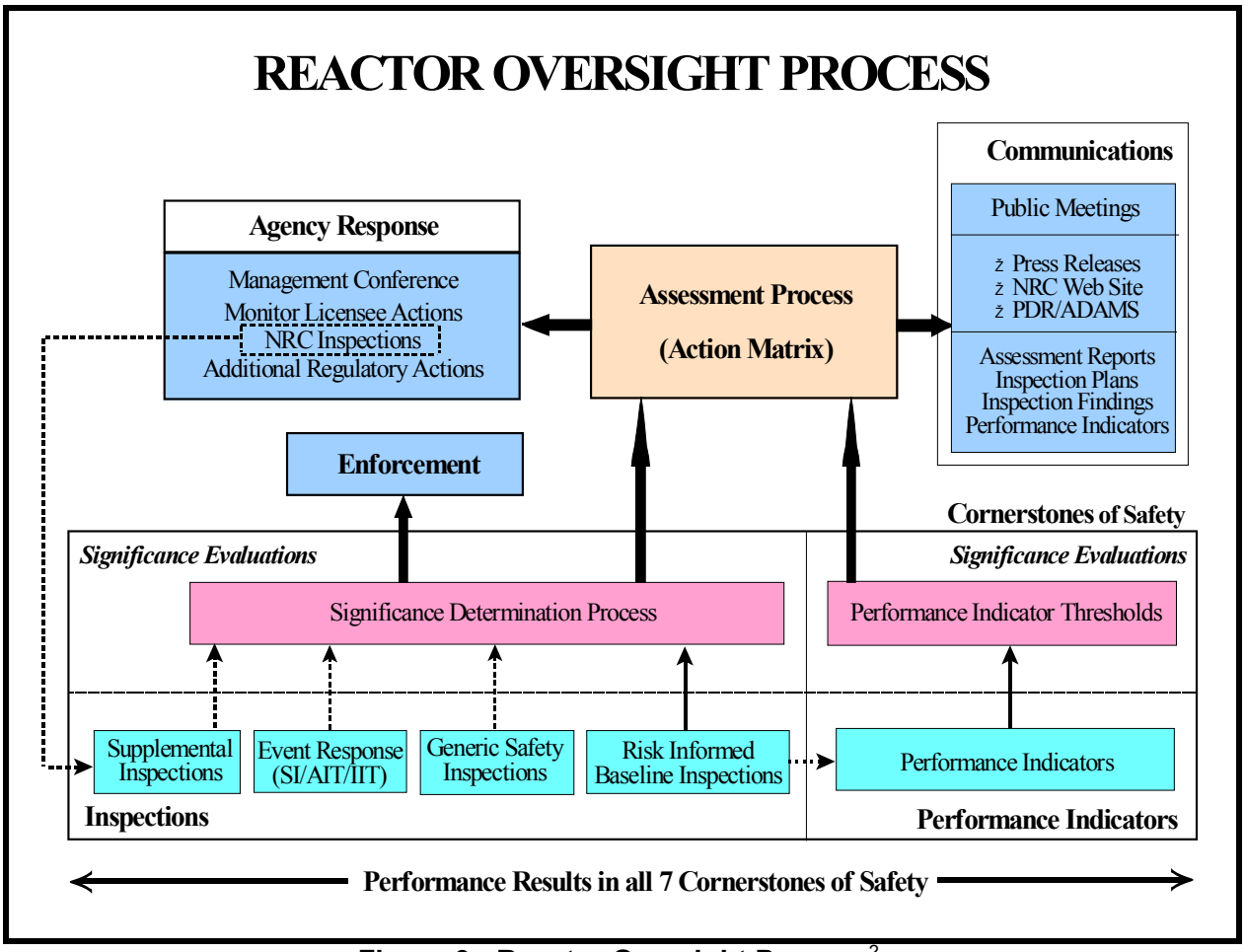

Figure 3: Reactor Oversight Process[2]

Furthermore, in CY 2013, four operating power reactor units were transitioned to decommissioning power reactors when their respective licensees submitted certifications to the NRC on permanent cessation of operations and permanent fuel removal. This prompted the Office of Nuclear Security and Incident Response to review and enhance the core inspection procedures used at reactors entering the decommissioning process. As a result, the NRC believes that adequate oversight and verification of the security posture for decommissioning power reactors will be maintained through the continued implementation of the core security inspection program. The core inspection program ensures that: (1) access authorization and access control requirements are met; (2) detection, assessment, and response capabilities are maintained; and (3) licensee-conducted security training drills and exercises are continued for effective implementation of the licensee's overall protective strategy. These power reactors

[2] For additional information on NRC's Reactor Oversight Process, please refer to NUREG-1649, "Reactor Oversight Process" (Revision 5, February 2014), available at https://adamsxt.nrc.gov/WorkplaceXT/getContent?id=release&vsId=%7B06DAA8C3-92B6-409B-9AE0-6E5E6D7855A6%7D&objectStoreName=Main.__.Library&objectType=document.

completed the baseline inspection program in CY 2013 and closed out the 5th triennial cycle of the ROP inspection program.

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.

In CY 2013, Office of Nuclear Security and Incident Response staff revised Part I, "Baseline Security Significance Determination Process for Power Reactors," of Appendix E, "Physical Protection Significance Determination Process for Power Reactors," to Inspection Manual Chapter (IMC) 0609, "Significance Determination Process." This update was necessary to account for adjustments to the security inspection program. The revisions to the IMC involved reducing redundancies and additional programmatic changes to increase efficiencies in the security inspection program.

The NRC also uses an SDP 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 might not be directly related to an FOF exercise outcome, but are identified during the FOF inspection.

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

- red (inspection findings with high safety or security significance)
- yellow (inspection findings with substantial safety or security significance)
- white (inspection findings with low to moderate safety or security significance)
- green (inspection findings with very low safety or security significance)

The NRC conducts supplemental inspections in response to red, yellow, and white 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 in 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 from the licensee detailing reasons for the performance deficiency 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 nuclear 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 I violations are those that resulted in, or could have resulted in, serious safety or security consequences. SL II violations are those that resulted in, or could have resulted in, significant safety or security consequences. SL III violations are those that resulted in, or could have resulted in, moderate safety or security consequences. 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. 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.

3. EVOLVING SECURITY INSPECTION ACTIVITIES

3.1 Overview

Security, like safety, is achieved in layers of defense, with multiple approaches at work to provide high assurance that licensed activities do not cause unreasonable risk to public health and safety. This includes the development of new programs and regulations to address new and changing real-world threats, as well as future challenges. Recent changes to some of the NRC's security regulations will further strengthen our already rigorous program. In January 2013, the NRC began conducting inspections of power reactor licensees' cyber security plans and implementation. Additionally, in January 2013, the NRC initiated inspections of commercial nuclear power reactors to ensure that necessary procedures and processes are in place and to provide a reasonable confirmation that the requirements for responding to a potential aircraft threat are being met.

3.2 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 and an implementation schedule for NRC approval. Subsequently, the NRC reviewed and approved licensees' cyber security plans and the implementation schedules. After the NRC's approval, licensees began implementing the commitments in the cyber security plan to meet the new requirements.

In order to focus early licensee cyber security efforts on actions that addressed the most significant areas, cyber security plan implementation was divided into two phases. Interim implementation, which was completed by December 2012, addressed significant cyber threat vectors and the most risk-significant digital assets. Full cyber security program implementation will be completed at all power reactors by the end of CY 2017. The NRC began conducting cyber security inspections in January 2013 and completed 20 inspections by the end of CY 2013.

Most inspections revealed several very low security significance violations of cyber security plan requirements. No significant violations were identified. Because the cyber security requirements are new, and licensees have demonstrated a good-faith attempt to implement the requirements, the NRC has used enforcement discretion for these violations. As a result, these findings do not appear in the summary of findings in Section 5 of this report.
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.[3] 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 whether 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 that 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.

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 whether any program improvements are needed.[4]

3.3 Responding to Potential Aircraft Threats

Title 10 of the *Code of Federal Regulations* 50.54(hh)(1) establishes requirements for how operating nuclear power reactor licensees are to respond to a potential aircraft threat. The final rule for 10 CFR 50.54(hh)(1) was published on March 27, 2009, in the *Federal Register* (Vol. 74, No. 58, pp. 13926–13993 (74 FR 13926)) and went into effect March 31, 2010. The NRC issued Regulatory Guide 1.214 in July 2009. This document describes approaches acceptable to the NRC staff for conforming to operating nuclear power reactor requirements associated with airborne threats as stated in 10 CFR 50.54(hh)(1). In August 2012, the NRC issued Temporary Instruction (TI) 2515/186, "Inspection of Procedures and Processes for Responding to Potential Aircraft Threats." The objective of this inspection activity is to verify that the procedures and processes necessary to effectively respond to aircraft threats are in place and provide a reasonable confirmation that the requirements of 10 CFR 50.54(hh)(1) are being met. Specifically, the TI is used to confirm that each licensee has developed, implemented and maintained procedures that describe how it will address the following areas if notified of a potential aircraft threat: (1) verification of the authenticity of threat notifications; (2) maintenance of continuous communication with threat notification sources; (3) contacting all onsite personnel and applicable offsite response organizations; (4) onsite actions necessary to enhance the capability of the facility to mitigate the consequences of an aircraft impact; and (5) measures to reduce visual discrimination of the site relative to its surroundings or individual buildings within the protected area. Fifty inspections were completed during the CY 2013 timeframe, with the remaining sites anticipated to be completed by June 30, 2014. No significant issues have been identified.

[3] 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.

[4] 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.

4. FORCE-ON-FORCE INSPECTION PROGRAM

4.1 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, 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 the licensee's protective strategy capabilities relative to the DBTs of radiological sabotage and theft or diversion of SSNM.

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 exercises. 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, preliminary compensatory measures will be put in place before the NRC inspection team leaves the site area.[5] However, it might be appropriate, on a case-by-case basis, to allow the licensee time (e.g., 24 to 48 hours) to determine and completely implement 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

[5] For additional information, see the NRC's "Protecting Our Nation" (NUREG/BR-0314, Revision 3, published October 2013) and the Office of Public Affairs fact sheet on Force-on-Force Security Inspections. These documents are available at http://pbadupws.nrc.gov/docs/ML1327/ML13270A213.pdf and http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/bg-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.

4.2 Program Activities in 2013

In 2013, 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 ensured that the nuclear industry improved the standards of training and qualifications for exercise controllers.

After a multiyear effort to enhance the FOF SDP, which began in September 2008 and involved internal and external stakeholder interactions, the staff completed the revision to the FOF SDP in July 2012. During 2012, following the implementation of the revised FOF SDP, the staff identified additional areas in which to enhance the FOF SDP. These enhancements to the FOF assessment and SDP tool provided a process for assessing each type of exercise performance outcome and give credit for strong overall security performance. Data on the impact of any change to the significance of a finding and comments from stakeholders were reviewed and incorporated, as appropriate, in revisions of the FOF SDP. These revisions were completed with interactions from internal and external stakeholder input in late 2013. The revised FOF SDP was finalized and issued on January 1, 2014. 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.

In 2009, the NRC issued a standalone target set review inspection procedure, which was revised on March 27, 2013, and which the agency used to conduct 27 target set reviews in CY 2013. Furthermore, on August 30, 2013, the most current target set inspection procedure was approved with an effective date of January 1, 2014. The NRC staff continues to revise the FOF and target set guidance documentation and related inspection procedures.

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 adversary force is composed of individuals with a nuclear security background, the NRC recognizes the potential for conflicts of interest and continually assesses this possibility. No conflict of interest has been detected.

4.3 Results of Force-on-Force Inspections

Between January 1, 2013, and December 31, 2013, the NRC conducted 23 FOF inspections[6] (at 22 commercial NPPs and 1 CAT I fuel cycle facility) and identified 24 findings that related to areas of the security baseline inspection program. Two of the findings resulted from the failure to effectively protect designated target set components during NRC-evaluated FOF exercises.

[6] Of the 23 FOF inspections conducted by the NRC in CY 2013, none were re-inspections.

By the end of 2013, the NRC had completed the third 3-year cycle of FOF inspections. Table 1 summarizes the 23 FOF inspections conducted in CY 2013.

Table 1: Calendar Year 2013 Force-on-Force Inspection Program Summary

23	Total number of inspections conducted
14	Total number of inspections with findings
9	Total number of inspections with no findings
1	Total number of complete target sets simulated to be damaged or destroyed
24	Total number of inspection findings
24	Total number of green findings
0	Total number of greater than green findings
0	Total number of SL IV findings
0	Total number of greater than SL IV findings

Of the total number of exercises conducted in CY 2013, 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, of the total number of exercises conducted in CY 2013, two exercises were canceled due to potential safety concerns associated with dangerous weather conditions and a licensee's work-hour restriction limitations. 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.

4.4 Discussion of Corrective Actions

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

Licensees commonly improve or add physical security structures and technologies based on lessons learned from FOF exercises. For example, if a licensee determines that the adversary force 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 security plans as required by 10 CFR Part 73, "Physical protection of plants and materials," they become lasting regulatory requirements.

4.5 Future Planned Activities

CY 2014, the first year of the fourth 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 prior FOF inspections.

5. SECURITY INSPECTION PROGRAM

5.1 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; MC&A; and Information Technology (Cyber) Security. Additionally, in CY 2013 security inspections for two TIs began: TI 2515/186, "Inspection of Procedures and Processes for Responding to Potential Aircraft Threats," and TI 2201/004, "Inspection of Implementation of Interim Cyber Security Milestones 1–7." The results of both TIs are included in the CY 2013 security inspection findings.[7]

5.2 Results of Inspections

Tables 2 and 3 summarize the overall results of the security 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 182 of the 255 security inspections at NPPs had no findings (71 percent). Figure 4 provides a graphic summary of the CY 2013 security 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 version of this report.

Table 2: Calendar Year 2013 Security Inspections at Nuclear Power Plants (without Force-on-Force)

255	Total number of security inspections conducted
73	Total number of security inspections with findings
182	Total number of security inspections with no findings
6	Total number of special and augmented inspections

Table 3: Calendar Year 2013 Security Inspection Findings at Nuclear Power Plants (without Force-on-Force)

125	Total number of inspection findings
114	Total number of green findings
4	Total number of greater than green findings
5	Total number of SL IV findings
2	Total number of greater than SL IV findings

[7] As stated in Section 3.2, because the cyber security requirements are new and licensees have demonstrated a good-faith attempt to implement the requirements, the NRC has used enforcement discretion for these findings. Subsequently, the results of these very low security significance findings are not reflected in Table 3 or Figure 4.

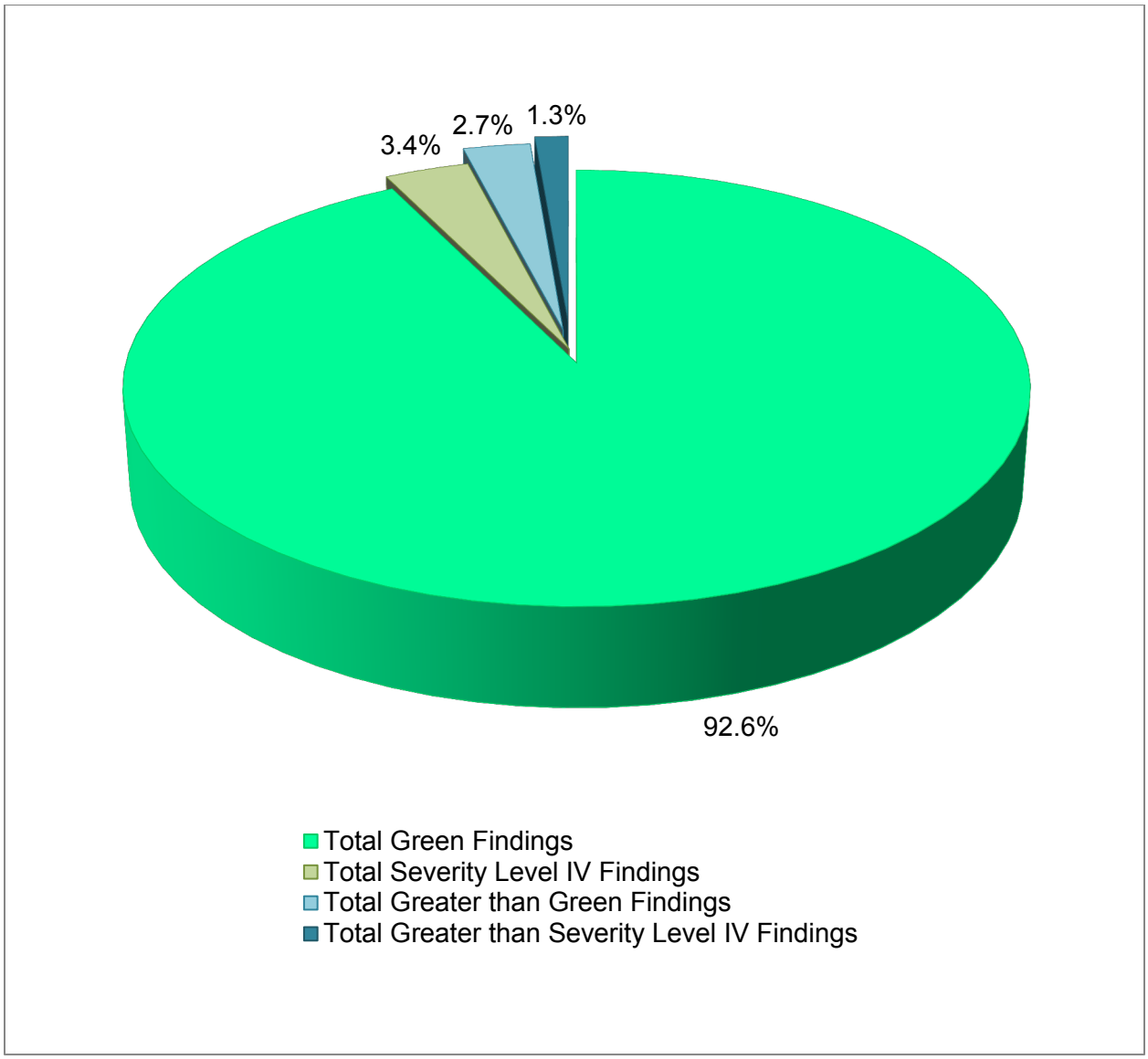

Figure 4: Summary of Calendar Year 2013 Security Inspection Findings at Nuclear Power Plants

6. OVERALL REACTOR SECURITY ASSESSMENT

6.1 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.

In accordance with Commission direction, in response to the terrorist attacks of September 11, 2001, staff was directed to develop a separate but parallel ROP assessment process for physical protection to address how security-related inspection findings and PIs would be considered when determining appropriate agency response. After 2004, the security cornerstone was treated in a way similar to, but essentially separate from, the rest of the ROP cornerstones because of the sensitivity of the information involved.

In July 2011, the Commission approved a staff recommendation to reintegrate the security cornerstone into the ROP assessment process and action matrix. The staff found that using a separate action matrix inhibited 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 might 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. The staff continues to monitor the reintegration of the security cornerstone into the assessment program to ensure reliable regulatory response outcomes are achieved, effective communications with internal and external stakeholders are provided, and regulatory outcomes continue to be appropriate.

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 conveys 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 page in 2012 to include all seven ROP cornerstones when the quarterly updates to Action Matrix inputs are posted. The Web page 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 information protection policy. Similarly, specific information about all security performance deficiencies will continue to be withheld from public disclosure to be consistent with current Commission information protection policy.

6.2 Performance Indicator

Licensees voluntarily report data about the protected area detection and assessment equipment that is implemented within their physical security program. NRC inspectors verify the accuracy and completeness of PI data used in conjunction with inspection findings to assess the security performance of power reactor licensees. 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, only green and white thresholds are established for the security PI. 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 2013, all licensees reported that the security PI was green. This means that protected area 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.

6.3 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 responding to performance issues and was developed with the philosophy that within a certain level of safety performance (i.e., the licensee response band), licensees would identify and correct 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 combines 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, if needed, additional regulatory actions ranging from management meetings to 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 applies to licensees with two white inputs or one yellow input in any cornerstone or three white inputs in any strategic performance area; licensees in this column meet the cornerstone objectives 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 in a manner that ensures 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 began conducting safety and security oversight under IMC 0350, "Oversight of Reactor Facilities in a Shutdown Condition Due to Significant Performance and/or Operational Concerns."[8] 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 (1) Missouri River flooding affected the site from June through September 2011, and (2) the licensee was addressing 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.

The IMC 0350 oversight process was implemented at Fort Calhoun Station to: (1) establish criteria for the oversight of licensee performance; (2) ensure that 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.

On December 2, 2013, Omaha Public Power District (OPPD) provided the NRC with its restart readiness letter entitled, "Integrated Report to Support Restart of Fort Calhoun Station and Post-Restart Commitments for Sustained Improvement."[9] The letter outlined the actions OPPD took to address the restart checklist items and provided commitments to implement post-restart actions that would continue to further improve plant performance. In December 2013, the NRC determined that Fort Calhoun Station was ready to restart after being shut down for nearly 3 years to address a number of significant performance deficiencies. The NRC restart readiness assessment was based on the NRC having thoroughly reviewed all of the extensive actions OPPD had taken and committed to take prior to restarting the plant. To support its approval of restart, the NRC applied more than 23,000 hours of extensive NRC inspections and detailed evaluations to independently review more than 450 restart action items, major improvements made by OPPD to the plant's supporting organizational infrastructure and programs, and numerous equipment modifications to improve reliability. Substantial inspection

---

[8] For additional information on the Fort Calhoun Station's change in regulatory oversight, please see the NRC's letter dated December 13, 2011, available at https://adamsxt.nrc.gov/WorkplaceXT/getContent?id=release&vsId=%7B537F305A-F7D1-401C-8496-F921CFAB5FD2%7D&objectStoreName=Main.__.Library&objectType=document.

[9] http://pbadupws.nrc.gov/docs/ML1333/ML13336A785.pdf

resources focused on licensee activities within the security cornerstone were expended during this period.

On December 17, 2013, the NRC sent Fort Calhoun Station a letter entitled "Fort Calhoun Station Closure of Confirmatory Action Letter." [10] The letter outlined the closure of the Confirmatory Action Letter, coordination of the restart decision with other Federal agencies, and continuation of IMC 0350 oversight of Fort Calhoun Station activities after restart. Plant oversight under IMC 0350 will continue until the agency determines that the plant's performance warrants returning it to the ROP (i.e., IMC 0305). In addition, the NRC will continue to hold periodic public meetings with OPPD in the local community to provide a status of the licensee's performance improvements.

[10] http://pbadupws.nrc.gov/docs/ML1335/ML13351A423.pdf

7. CATEGORY I FUEL CYCLE FACILITY SECURITY OVERSIGHT PROGRAM

7.1 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 formula quantities of SSNM. 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 formula quantities of SSNM.

The NRC may conduct plant-specific supplemental or reactive inspections similar to those of the ROP 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.

7.2 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 version of this report includes the results of the security inspections at CAT I fuel cycle facilities.

8. STAKEHOLDER COMMUNICATIONS

8.1 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 about nuclear-security issues.[11] For example, the agency presents a variety of security topics at its Regulatory Information Conference, held each spring in Rockville, Maryland.[12] 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 2013, the NRC issued eight Security Advisories covering a variety of topics. Four Regulatory Issue Summaries were issued in CY 2013 related to security and no Information Notices (see Section 8.2 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.

8.2 Calendar Year 2013 List of Generic Communications by Title[13]

Security Advisories

SA 13-01, SA 13-02, SA 13-03, SA 13-04	"National Special Security Event for the 2013 Presidential Inauguration"
SA 13-05, SA 13-06, SA 13-07, SA 13-08	"National Special Security Event for the 2013 Presidential State of the Union Address"

Regulatory Issue Summaries

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

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

[13] 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/.

RIS 13-02	"Impact of Sequestration on NRC Activities and NRC Stakeholders"
RIS 13-16	"Interactions Between the NRC and NRC Stakeholders During a Lapse of Agency Appropriations"
RIS 13-17	"Resuming Normal Interactions Between the NRC and NRC Stakeholders Following an Agency Shutdown"
RIS 13-19	"Removal of Safeguards Information Designation from Attachment 2 to Order EA-02-261, 'Order for Compensatory Measures Related to Access Authorization'"

Information Notices

N/A

8.3 Communications with Local, State, and Federal Agencies

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

The NRC continues to support the 2004 Homeland Security Council initiative to enhance integrated response planning for NPP sites. From 2007 through 2012, the NRC participated in the Integrated Pilot Comprehensive Exercise (IPCE) initiative, which was a voluntary collaborative effort among the Federal Bureau of Investigation (FBI), U.S. Department of Homeland Security (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 Energy Center.

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 were completed in August 2013. The NRC, FBI, DHS, NEI, and commercial nuclear power industry are currently working towards implementation of an industrywide integrated response program at all NPP sites.

NRC FORM 335
(12-2010)
NRCMD 3.7

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER
(Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)

NUREG-1885, Rev. 7

2. TITLE AND SUBTITLE

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

3. DATE REPORT PUBLISHED

MONTH	YEAR
July	2014

4. FIN OR GRANT NUMBER

5. AUTHOR(S)

Niry Simonian, NSIR

6. TYPE OF REPORT

Annual

7. PERIOD COVERED (Inclusive Dates)

01/01/2013-12/31/2013

8. PERFORMING ORGANIZATION - NAME AND ADDRESS (If NRC, provide Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)

Division of Security Operations
Office of Nuclear Security and Incident Response
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555-0001

9. SPONSORING ORGANIZATION - NAME AND ADDRESS (If NRC, type "Same as above", if contractor, provide NRC Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address.)

Same as above

10. SUPPLEMENTARY NOTES

11. ABSTRACT (200 words or less)

This report fulfills the requirements of Section 170D.e of Chapter 14 of the Atomic Energy Act of 1954 (42 U.S.C. §2201d.e) 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 ninth annual report, which covers calendar year 2013. 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.

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)

Security Inspection Program
Security Response Evaluation Program
Force-on-Force Inspections
Commercial Power Reactors
Category I Fuel Cycle Facilities
Congressional Report
Report to Congress

13. AVAILABILITY STATEMENT

unlimited

14. SECURITY CLASSIFICATION

(This Page)
unclassified

(This Report)
unclassified

15. NUMBER OF PAGES

16. PRICE

Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS