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 2014

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. §2210d.e), as amended, which states, "[n]ot 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 tenth annual report, which covers calendar year 2014. 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 8, "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

PAGE INTENTIONALLY LEFT BLANK

FIGURES

TABLES

PAGE INTENTIONALLY LEFT BLANK

ACRONYMS

10 CFR	Title 10 of the *Code of Federal Regulations*
ADAMS	Agencywide Documents Access and Management System
AIT	Augmented Inspection Team
CAPT	computer-aided planning tool
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
IPCE	Integrated Pilot Comprehensive Exercise
IRP	integrated response plan
MC&A	material control and accounting
NEI	Nuclear Energy Institute
NPP	nuclear power plant
NRC	U.S. Nuclear Regulatory Commission
PDR	Public Document Room
PI	performance indicator
PPSDP	physical protection significance determination process
ROP	Reactor Oversight Process
SDP	Significance Determination Process
SGI	safeguards information
SI	special inspection
SL	severity level
SSNM	strategic special nuclear material
TI	Temporary Instruction
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. §2210d.e), as amended, which states, "[n]ot 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 tenth annual report covers calendar year (CY) 2014. 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 SSNM in any combination in a quantity of 5,000 grams or more computed by the formula, grams=(grams contained U-235)+2.5(grams U-233+grams plutonium). This class of material is sometimes referred to as a Category I quantity of material.

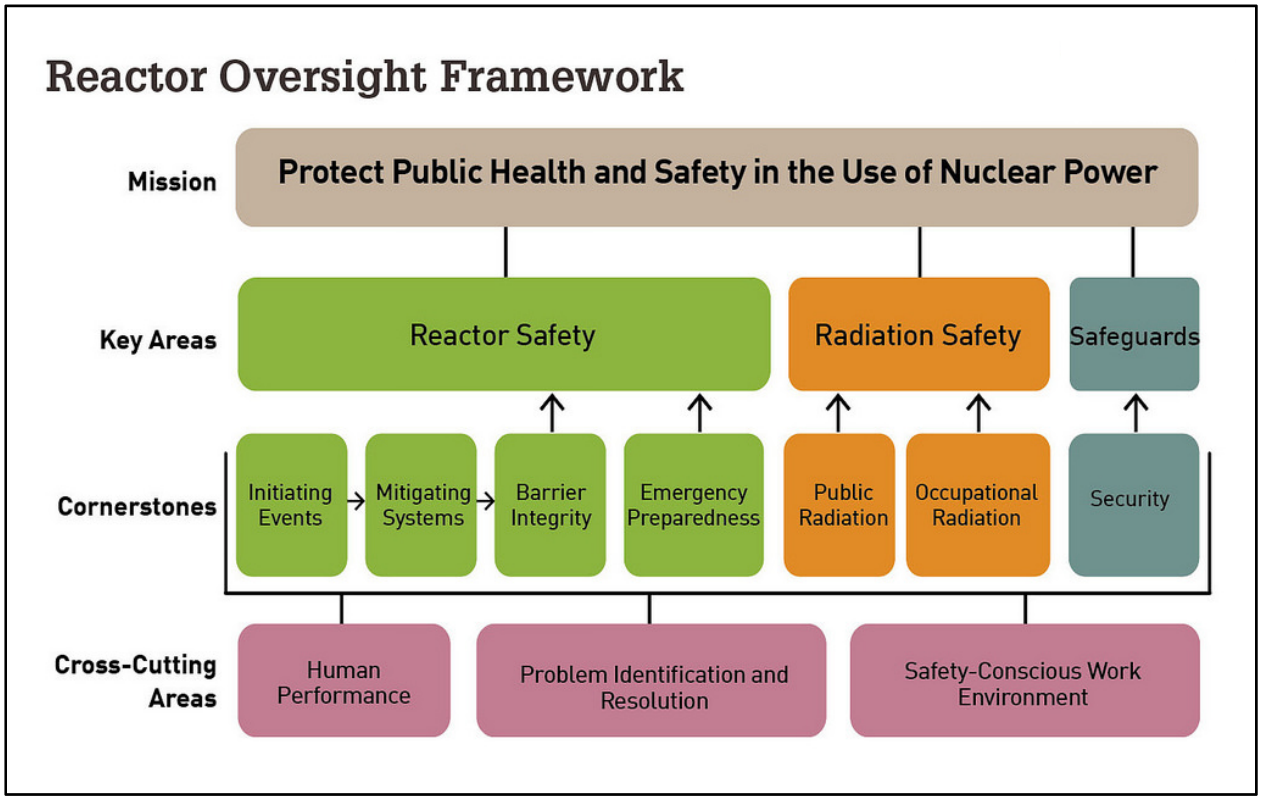
PAGE INTENTIONALLY LEFT BLANK

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 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: Reactor Oversight Framework



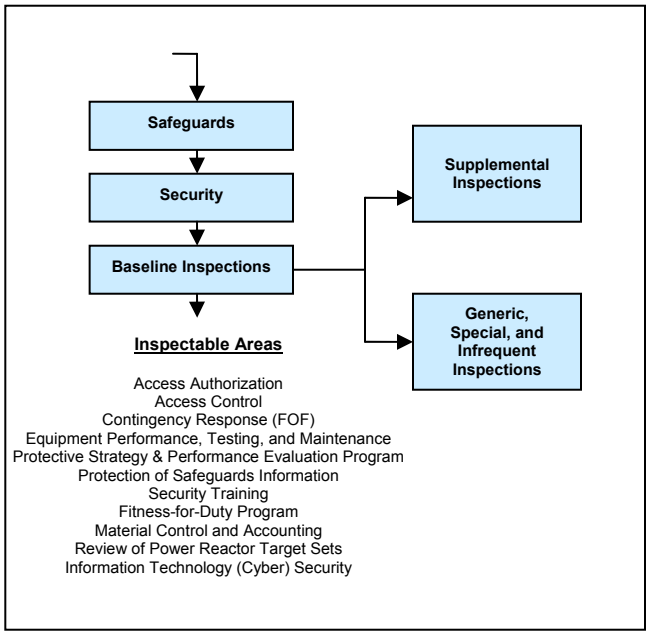
As part of its actions following the terrorist attacks of September 11, 2001, the NRC issued a number of orders requiring licensees to strengthen security programs in several areas. During 2009 the NRC completed a rulemaking that made generally applicable security requirements similar to these orders 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 nuclear power reactors. 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: (1) access authorization; (2) access control; (3) physical protection systems; (4) material control and accounting (MC&A); and (5) response to

contingency events. The objective of the security cornerstone is to provide high assurance that the licensee's security system and MC&A program use a defense-in-depth approach and can protect against (1) the design basis threat (DBT) of radiological sabotage from external and internal threats, and (2) the theft or loss of radiological materials.

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 commercial nuclear power reactor (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

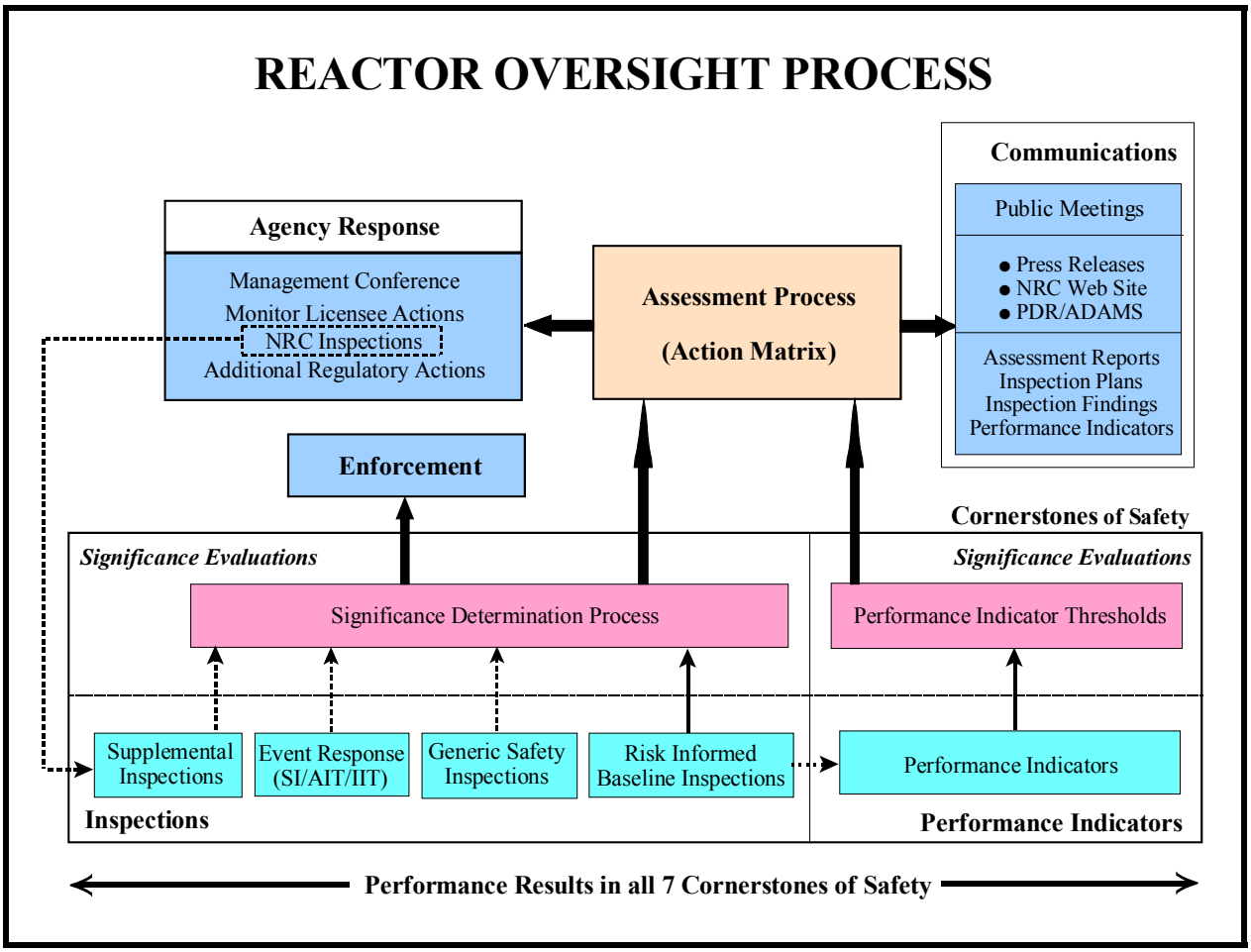


The security assessment process collects information from NRC security inspections and PIs provided by NPP licensees to enable the NRC to reach objective conclusions about a licensee's security performance. Based on this assessment information, the NRC determines the appropriate level of agency response. 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 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]



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

[1] Additional information on the ROP action matrix is provided in Section 2.5.

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

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, ensures 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 continues 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.

The NRC modified the ROP public Web page in 2012 to include all seven ROP cornerstones. As a result, the quarterly updates to action matrix inputs incorporate security. The Web page displays security inputs that are determined to be of very low security significance (i.e., 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.

Additionally, over the last two years, five operating power reactors were transitioned to decommissioning status 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. The NRC provides oversight of licensee security programs at decommissioning power reactors through a security inspection program that verifies compliance with applicable regulatory requirements. The security inspection program examines licensee activities in order to assess performance and to assure that the licensee's overall security program is meeting the objective of the security cornerstone, which is to provide high assurance that a power reactor licensee's security system and MC&A program can protect against the DBT of radiological sabotage consistent with 10 CFR Part 73, "Physical Protection of Plants and Materials," and the theft or loss of special nuclear material consistent with 10 CFR Part 74, "Material Control and Accounting of Special Nuclear Material." The Office of Nuclear Security and Incident Response enhanced the core inspection procedures used at reactors entering the decommissioning process to ensure adequate oversight and verification of the security posture at these facilities. 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. In May 2014 the Commission approved the staff's recommendation to continue the current

practice of security inspections for decommissioning power reactors, which do not include NRC-conducted FOF inspections. NRC-conducted FOF inspections during decommissioning are not warranted because the current security inspection program provides adequate oversight and verification of the security posture given a reduction in both risk and the number of target sets at decommissioning power reactors. The NRC believes that adequate oversight of security at decommissioning power reactors will be maintained through the continued implementation of the core security inspection program.

2.2 Significance Determination Process

The Significance Determination Process (SDP) for NPPs uses risk insights, where appropriate, to help NRC inspectors and 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.

During CY 2014 the NRC continued to monitor and evaluate the Baseline Significance Determination Process to ensure it continues to offer predictable and repeatable results that allow the NRC to determine the appropriate level of agency response to identified weaknesses and deficiencies in licensee security programs.

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 could 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 reactors that have willful aspects, actual safety consequences, or an impact on the regulatory process. 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.

2.4 Performance Indicator

The NRC evaluates plant performance by analyzing two distinct inputs: inspection findings resulting from the NRC's inspection program and PIs reported by the licensee. Licensees voluntarily report PI 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 commercial nuclear 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 2014, all licensees reported that their 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.

2.5 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: (1) licensee response; (2) regulatory response; (3) degraded cornerstone; (4) repetitive degraded cornerstone; and (5) 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 supplied 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.

PAGE INTENTIONALLY LEFT BLANK

3. EVOLVING SECURITY INSPECTION ACTIVITIES

3.1 Overview

Security, like safety, is achieved in layers, with multiple approaches at work to provide high assurance that licensed activities do not cause unreasonable risk to public health and safety, the common defense and security, and the environment. 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 licensees' cyber security plans and their implementation of these plans. Additionally, in January 2013 the NRC initiated inspections of commercial nuclear power reactors to ensure licensees developed, implemented, and maintain procedures for responding to potential aircraft threats.

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, security, 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 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 is expected to be completed at all commercial nuclear power reactors by the end of CY 2017. The NRC began cyber security inspections in January 2013 and completed 22 inspections by the end of CY 2014.

Most inspections revealed several very low security significance violations of cyber security plan requirements. Industry is increasing its ability to identify problems and working with the NRC on remediation solutions. 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, non-power reactors, independent spent fuel storage installations, and byproduct materials licensees.[3] 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]

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, security, emergency preparedness, information security, and MC&A of special nuclear material. 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) visiting 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 NRC is beginning a rulemaking for fuel cycle facility cyber security.

The Commission has voted to approve a final rule, 10 CFR 73.77, "Cyber Security Event Notifications," that will require timely notification of cyber security events that cause or could cause adverse impacts to safety-related and important-to-safety, security, and emergency preparedness functions. The staff is awaiting Commission instruction before finalizing the rule. This rule will contribute to the NRC's analysis of the reliability and effectiveness of licensees' cyber security programs.

3.3 Responding to Potential Aircraft Threats

Regulations in 10 CFR 50.54(hh)(1) establish 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. In July 2009 the NRC issued Regulatory Guide 1.214, "Response Procedures for Potential or Actual Aircraft Attacks"[5], which was revised in March 2014. This document describes approaches acceptable to 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 potential aircraft threats are in place and to confirm 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

[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.

[5] RG 1.214 contains "Official Use Only – Security-Related Information" and is not publicly available.

potential aircraft threat: (1) verification of the authenticity of threat notifications; (2) maintenance of continuous communication with threat notification sources; (3) contact with 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.

As of May 2014, all TI 2515/186 inspections have been completed. No significant issues were identified.

PAGE INTENTIONALLY LEFT BLANK

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 offers 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.[6] 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, an 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 consists of two FOF exercises. If an exercise is canceled because of severe weather or for other reasons, NRC management may consider allowing fewer than two exercises to satisfy inspection requirements, but only when a licensee has successfully demonstrated an effective strategy in at least one exercise 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.

[6] For additional information, see the NRC's "Protecting Our Nation" (NUREG/BR-0314, Revision 3, published October 2013) and the Office of Public Affairs *Backgrounder* on "Force-on-Force Security Inspections" (July 2014). 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.

4.2 Program Activities in 2014

Program activities in CY 2014 marked the beginning of a 3-year ROP and FOF inspection cycle; during this year a newly revised FOF inspection procedure was implemented. Following the procedure revisions, NRC staff continually assessed the program to ensure revisions provided NRC inspectors with useful insights into the licensee's ability to implement a protective strategy that defends against the DBT of radiological sabotage. An additional benefit of the revisions to the inspection procedure was the increased emphasis the industry placed on its critique process for assessing the effectiveness of the protective strategy during FOF exercises and inspection activities. Specifically, NRC inspectors generally observed increased involvement by licensee senior management in implementing the corrective actions of security activities identified during NRC FOF inspections. It is anticipated that the increased involvement by licensee senior management will lead to continued overall improvement of the licensees' protective strategies and processes, further reinforcing their physical protection programs against the DBT of radiological sabotage. The revisions to the FOF inspection program implemented in CY 2014 continue to focus on evaluating the licensees' protective strategies while maintaining regulatory stability and consistency in the inspection process.

In CY 2014, the NRC issued a revised FOF SDP that incorporated enhancements which provided a process for assessing each type of exercise performance outcome and gives credit for strong overall security performance. Throughout 2014 the NRC continued to evaluate and assess the FOF SDP to ensure it continues to provide predictable and repeatable results that allow the NRC to determine the appropriate level of agency response for weaknesses and deficiencies identified during FOF exercises. Additionally, 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 a February 2014 Staff Requirements Memorandum[7] the Commission directed the staff to conduct a lessons-learned review of the NRC's FOF inspection program to evaluate whether any adjustments were necessary to ensure efforts in the NRC's FOF inspection program were accomplishing intended objectives effectively and whether the NRC's and licensees' efforts were focused on the most important issues to ensure security and safety at the sites. The lessons-learned review consisted of data collection and analysis regarding the history and implementation of the FOF program, including a literature review, benchmarking of the NRC program against similar programs conducted by other Federal agencies, the assessment of international best practices, and the solicitation and review of stakeholder input. Upon completion of the lessons-learned review, the Executive Director for Operations provided the results of the evaluation to the Commission in a SECY Paper dated August 20, 2014.[8] The assessment determined that the NRC's FOF program is consistent with applicable statutory and regulatory requirements, including the Atomic Energy Act of 1954, as amended; is generally consistent with similar programs conducted by the U.S. Department of Energy and the U.S. Department of Defense; and properly focuses NRC and licensee resources on the most

[7] Memorandum to Mark A. Satorius, Executive Director for Operations, from Annette L. Vietti-Cook, Secretary of the Commission, dated February 11, 2014, "COMGEA/COMWCO-14-0001—Proposed Initiative to Conduct a Lessons-Learned Review of the NRC's Force-on-Force Inspection Program," which can be found at: https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML14043A063.

[8] SECY Paper to the Commission from Mark A. Satorius, Executive Director for Operations, dated August 20, 2014, "SECY-14-0088—Proposed Options to Address Lessons-Learned Review of the NRC's Force-on-Force Inspection Program in Response to Staff Requirements Memorandum – COMGEA/COMWCO-14-0001," which can be found at: https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML14139A231.

important issues to ensure security and safety of the sites. Furthermore, the review concluded that the current program has the necessary processes in place to evaluate and incorporate lessons-learned on an ongoing basis. The staff identified several enhancements to improve the realism and effectiveness of NRC-conducted FOF exercises and is taking action on those through a follow-on working group, which will report its findings to the Commission in CY 2016.[9]

Target set inspections ensure licensees will provide, with high assurance, a security response to protect the appropriate equipment, structures, and components so that actions by adversaries defined in the DBT would not be successful in causing radiological sabotage. The issuance of 10 CFR 73.55(f), effective May 26, 2009, codified the necessity for complete and accurate target sets, requiring licensee's full compliance by March 31, 2010. Target set inspections are essential in assessing the execution of a licensee's protective strategy by identifying which equipment, structures, and components to simulate attacking during the on-site conduct of FOF exercise and inspection activities. In 2009, the NRC issued a standalone target set review inspection procedure, which was revised in CY 2014.

In CY 2014 the target set inspection program completed its final ROP cycle as a headquarters-based inspection program and initiated its transition to a regional-based program. Regional offices have been the traditional administrator for baseline inspection activities at commercial nuclear power reactors under their responsibility. Because the oversight of target sets is now clearly defined in NRC requirements as a baseline inspection activity, the NRC determined CY 2015 was the appropriate timeframe to transfer target set inspections to the regions. NRC staff continues to revise the FOF and target set guidance documentation and related inspection procedures and target set inspections continue to be completed on a triennial basis by qualified regional inspectors.

The composite adversaries used for inspections continue 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 support 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, 2014, and December 31, 2014, the NRC conducted 23 FOF inspections[10] (all at commercial power reactors) and identified 22 findings that related to areas of the security baseline inspection program. One of the findings resulted from the failure to protect designated target set components effectively during NRC-evaluated FOF exercises.

[9] Memorandum to Mark A. Satorius, Executive Director for Operations, from Rochelle C. Bavol, Acting Secretary of the Commission, dated December 19, 2014, "SECY-14-0088—Proposed Options to Address Lessons Learned Review of the NRC's Force-on-Force Inspection Program in Response to Staff Requirements—COMGEA/COMWCO-14-0001," which can be found at: https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML14353A433.

[10] The NRC conducted re-inspections at four sites in 2014 which are included in the 23 FOF inspections.

By the end of 2014, the NRC had completed the first year of the fourth 3-year cycle of FOF inspections. Table 1 summarizes the 23 FOF inspections conducted in CY 2014.

Table 1: Calendar Year 2014 Force-on-Force Inspection Program Summary

23	Total number of inspections conducted
13	Total number of inspections with findings
10	Total number of inspections with no findings
1	Total number of complete target sets simulated to be damaged or destroyed
22	Total number of inspection findings
20	Total number of green findings
2	Total number of greater than green findings
0	Total number of SL IV violations
0	Total number of greater than SL IV violations

Of the total number of exercises conducted in CY 2014, one exercise was inconclusive and deemed indeterminate. An indeterminate exercise is an exercise where the results were significantly skewed by an anomaly or anomalies, resulting in the inability to determine the outcome of the exercise (e.g., site responders neutralize the adversaries using procedures or practices unanticipated by the design of the site protective strategy or training of security personnel to implement the site protective strategy or significant exercise control failures to include controller performance failures). This exercise was deemed indeterminate because the licensee failed to identify in their protective strategy the location of a responder that had been planned and practiced, resulting in the neutralization of adversaries. No exercises were canceled or postponed in CY 2014 because of dangerous weather conditions or any other site limitations.

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: (1) procedural or policy changes, (2) physical security or technology improvements and upgrades, and (3) 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. These corrective actions are not required. However, 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 2015, the second year of the fourth 3-year cycle of FOF inspections, began with 22 inspections scheduled for the year. Of these, none are follow-up inspection to assess corrective actions to evaluate improvements that licensees implemented as a result of prior FOF inspections.

PAGE INTENTIONALLY LEFT BLANK

5. SECURITY BASELINE INSPECTION PROGRAM AT COMMERCIAL NUCLEAR POWER REACTORS

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 from both TIs are included in the CY 2014 security inspection numbers.[11]

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 115 of the 195 security inspections at NPPs had no findings (59 percent). Figure 4 provides a graphic summary of the CY 2014 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 2014 Security Inspections at Commercial Nuclear Power Reactors (without Force-on-Force)

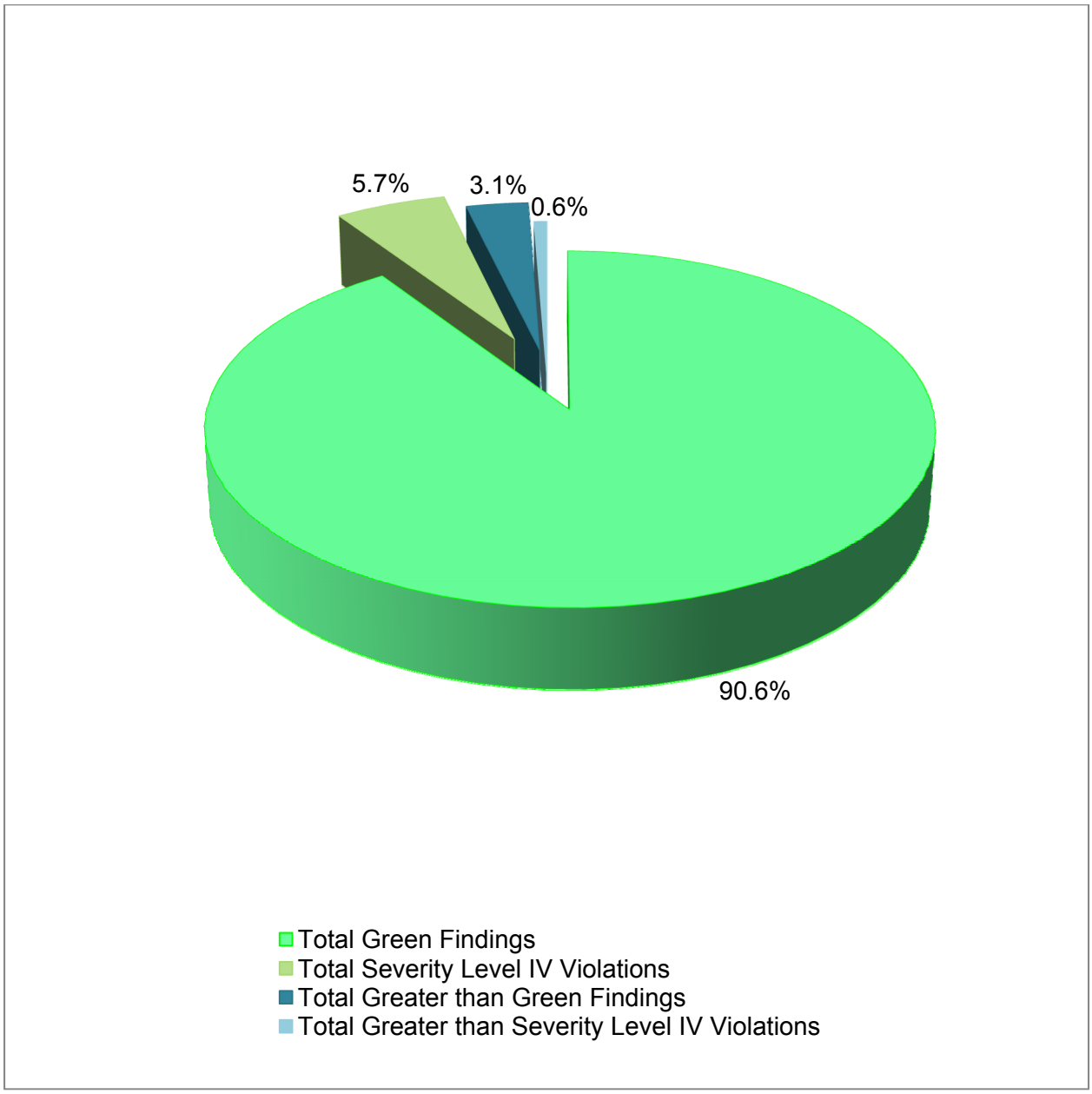
195	Total number of security inspections conducted
80	Total number of security inspections with findings
115	Total number of security inspections with no findings
4	Total number of special or augmented inspections

Table 3: Calendar Year 2014 Security Inspection Findings at Commercial Nuclear Power Reactors (without Force-on-Force)

159	Total number of inspection findings
144	Total number of green findings
5	Total number of greater than green findings
9	Total number of SL IV violations
1	Total number of greater than SL IV violations

[11] 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 the cyber security findings in CY 2014. 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 2014 Security Inspection Findings at Commercial Nuclear Power Reactors (without Force-on-Force)



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 nuclear power 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 enhanced their security postures significantly 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 identify 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.

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

7. STAKEHOLDER COMMUNICATIONS

7.1 Communications with the Public, Licensees, and Other Stakeholders

The 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.[12] For example, the agency presents a variety of security topics at its Regulatory Information Conference, held each spring in Rockville, Maryland.[13] 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, 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 2014, the NRC issued eight Security Advisories, one Regulatory Issue Summary related to security, three Information Assessment Team Advisories, and no Information Notices (see Section 7.2 for a complete list).

After each FOF inspection, 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 on a quarterly basis through the FOF Working Group meetings, which includes security representatives from NRC-licensed facilities.

7.2 Calendar Year 2014 List of Generic Communications by Title[14]

Security Advisories

SA 14-01, SA 14-02, SA 14-03, SA 14-04	"National Special Security Event for the 2014 Presidential State of the Union Address"
SA 14-05, SA 14-06, SA 14-07, SA 14-08	"National Special Security Event for the U.S. – Africa Leaders' Summit"

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

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

[14] 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/.

Regulatory Issue Summaries

RIS 14-02	"NRC Regulatory Issue Summary 2014-02 Withdrawal of NRC Generic Letter 95-08, "10 CFR 50.54(p) Process for Changes to Security Plans without Prior NRC Approval""

Information Assessment Team Advisories

IATA-14-01	"Situational Awareness—Cyber Security Event at NRC Licensed Facility"
IATA-14-02	"Situational Awareness—Returning Foreign Fighters Pose Potential Terrorist Threat"
IATA-14-03	"Updated Suspicious Flight Activity Voluntary Reporting Procedures—Unmanned Aircraft Systems"

Information Notices

N/A

7.3 Communications with Local, State, and Federal Agencies

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

The NRC continues to support the 2004 Homeland Security Council initiative to enhance integrated response planning for NPP sites. 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 commercial 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.

In 2012, the NRC, FBI, DHS, NEI, and the commercial 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.

Currently, there are four core elements, that make up integrated response activities, also known as the Integrated Response Program: (1) site-specific integrated response plans (IRPs), which identify resources and roles and responsibilities of the response organizations for FBI review and approval; (2) computer-aided planning tool (CAPT) development, which is a navigational and response planning tool for the tactical response team; (3) tabletop exercises, which validate

the IRP; and (4) limited exercises, which focus on mission understanding, communications, and self-guided navigation by law enforcement responders within power blocks.

The FBI has approved 48 site-specific IRPs to date, with the remaining 14 IRPs currently being drafted. Additionally, the staff continues to collaborate with the FBI on the development of the CAPTs. Specifically, the staff assisted the FBI with the development and delivery of 21 CAPTs, to date. The development of CAPTs for the remaining commercial power reactors is moving forward at the rate of six sites per year.

With regard to the tabletop exercise and limited exercise, the staff is exploring possible options to encourage the implementation of the tabletop exercise and limited exercise elements on a voluntary basis by the industry. More specifically, the staff is examining aspects of the physical security regulatory program components that may be viable to work in concert with the tabletop exercises and limited exercises to use NRC and licensee resources effectively and efficiently. Pending the outcome of the ongoing evaluation, the staff will provide a description of the path forward during the next semi-annual update of the Integrated Response Program. Until the NRC, its Federal partners, and industry align on a path forward for the tabletop exercises and limited exercises, the planned tabletop exercises and limited exercises discussed in the last semi-annual update are on hold.