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 2015

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 eleventh annual report, which covers calendar year 2015. 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 9, "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 nor 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

TABLE OF 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
CAT I	Category I
CY	calendar year
DBT	design-basis threat
FBI	Federal Bureau of Investigation
FOF	force-on-force
HEU	highly enriched uranium
IIT	incident investigation team
MC&A	material control and accounting
NPP	nuclear power plant
NRC	U.S. Nuclear Regulatory Commission
PDR	Public Document Room
PI	performance indicator
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	uranium
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 eleventh annual report covers calendar year (CY) 2015. 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 the agency's 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.

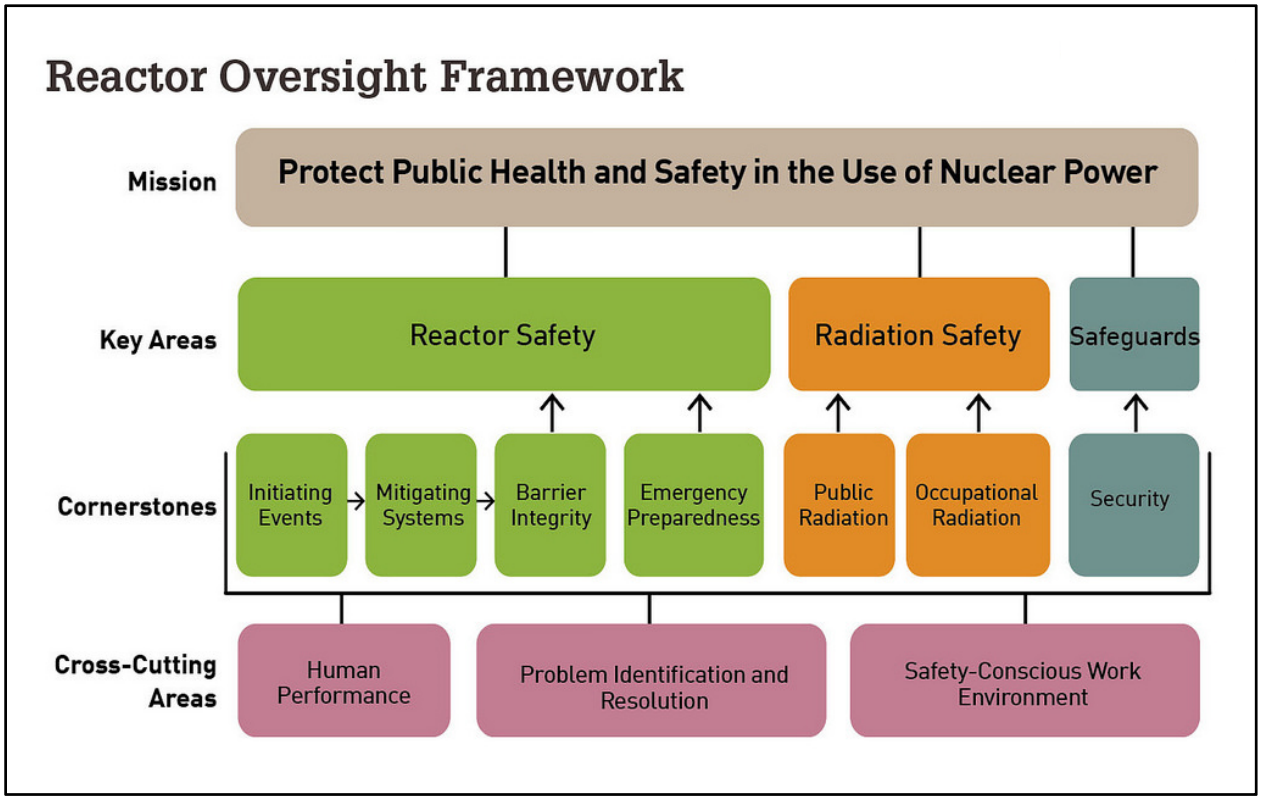
PAGE INTENTIONALLY LEFT BLANK

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



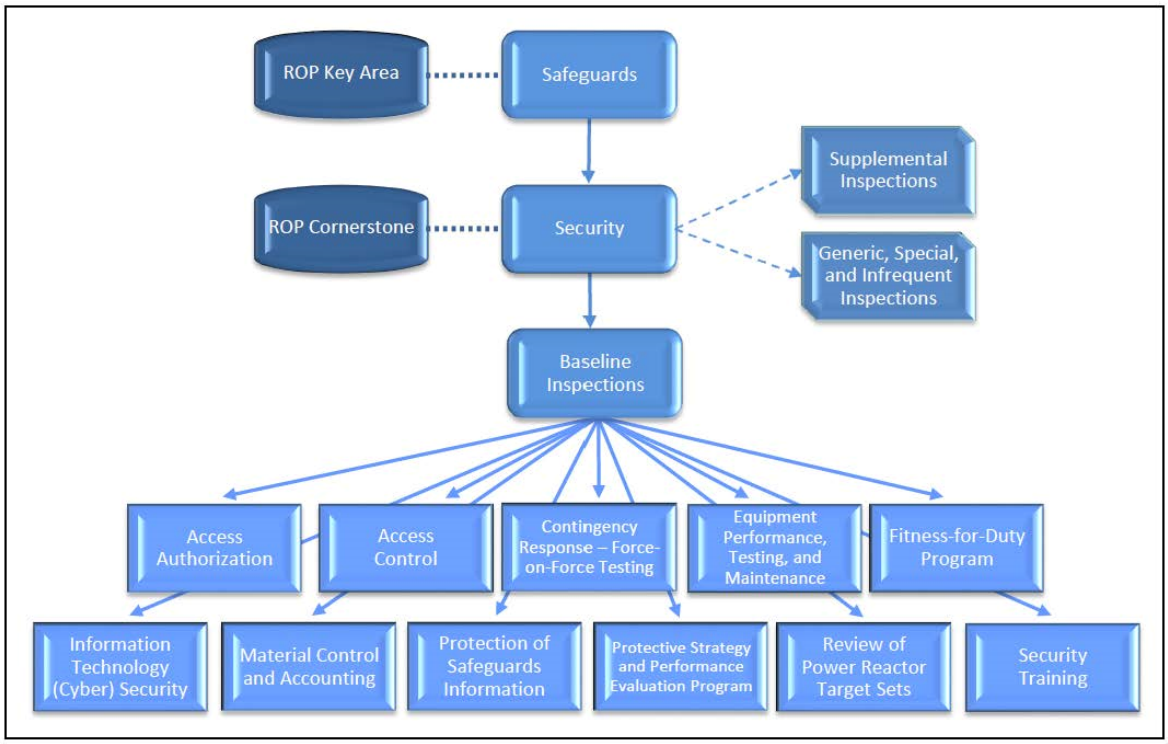
As part of its actions following the terrorist attacks of September 11, 2001, the NRC issued a number of orders requiring licensees to strengthen security programs in several areas. During 2009, the NRC completed a rulemaking that made generally applicable security requirements similar to these orders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

events, (6) protection of safeguards information (SGI), and (7) cyber security. The objective of the security cornerstone is to provide high assurance that a 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 programs and protective strategy can protect against the DBT of radiological sabotage consistent with the general performance objective of 10 CFR 73.55(b) and that the licensee's MC&A program includes processes for the control and accountability of special nuclear material, to include the identification and notification of theft or loss consistent with 10 CFR Part 74, "Material Control and Accounting of Special Nuclear Material"; (2) to determine a licensee's ability to identify, assess the significance of, and effectively correct security issues commensurate with the significance of the issue; (3) to verify the accuracy and completeness of PI data used in conjunction with inspection findings to assess the security performance of power reactor licensees; (4) to provide a mechanism for the NRC to remain cognizant of security status and conditions; and (5) 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 3 describes in detail.

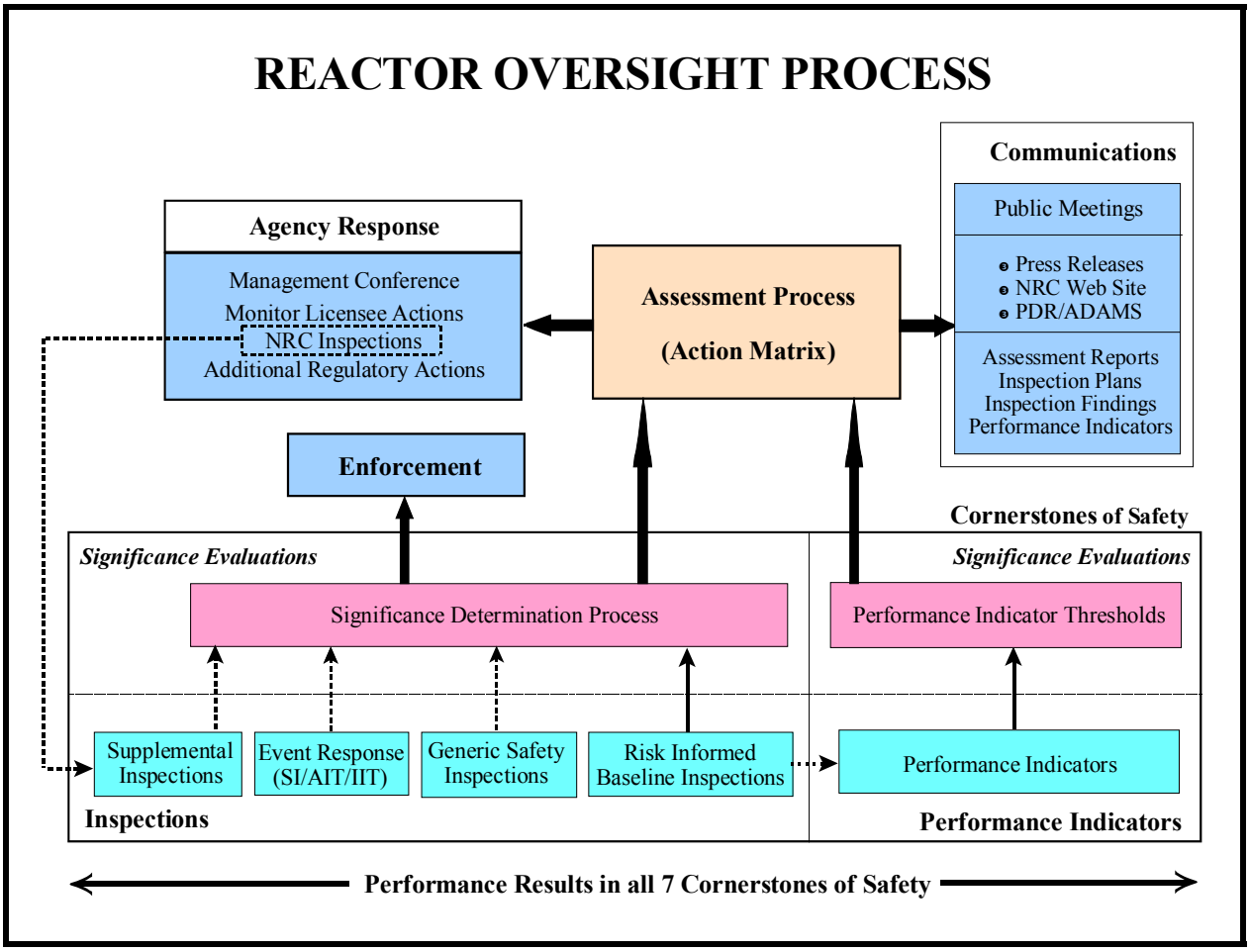
Figure 2: Inspectable Areas of the Security Cornerstone



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 event response 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]



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

[2] For additional information on the NRC's ROP, please refer to NUREG-1649, "Reactor Oversight Process" (Revision 5, February 2014), which can be found at: http://pbadupws.nrc.gov/docs/ML1405/ML14052A306.pdf.

In response to the terrorist attacks of September 11, 2001, the Commission directed the staff 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, 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. The NRC completed reintegration of the security cornerstone in August 2012. The staff continues to monitor the reintegration 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.

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 and determines the security significance of security program deficiencies using the Baseline Security Significance Determination Process.

During CY 2015, the NRC continued to monitor and evaluate the Baseline Security 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 Security Significance Determination Process 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 an 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 white, yellow, and red findings.

2.3 Findings and Violations

Inspection findings are associated with identified performance deficiencies and also typically relate to violations of NRC requirements. Violations associated with green findings are usually described in inspection reports as non-cited violations if the licensee has placed the issue 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 performs supplemental inspections to verify that the licensee's corrective actions were adequate.

The NRC uses its traditional enforcement process to evaluate all inspection findings at CAT I fuel cycle facilities. The NRC also uses this process to evaluate those violations at commercial nuclear power reactors that resulted in actual safety or security consequences, may impact the ability of the NRC to perform its regulatory oversight function, or those involving willfulness. 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 licensees. 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 licensees' security programs that are not specifically inspected by the NRC's baseline inspection program. As of

the end of CY 2015, 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 a 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 performance; (4) multiple/repetitive degraded cornerstone; and (5) unacceptable performance. The licensee response column indicates that all action matrix inputs (PIs and inspection findings) are green and that the cornerstone objectives are fully met. Licensees that fall into the regulatory response column have action matrix inputs that result in one or two white inputs in any cornerstone and no more than two white inputs in any strategic performance area. The degraded performance column applies to licensees with action matrix inputs that result in three or more white inputs or one yellow input in any cornerstone or three white inputs in any strategic performance area. If a licensee falls into the multiple/repetitive degraded cornerstone, it has received action matrix inputs that result in a repetitive degraded cornerstone, multiple degraded cornerstones, multiple yellow inputs, or a red input. 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 associated with 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.

3. FORCE-ON-FORCE INSPECTION PROGRAM

3.1 Overview

FOF inspections, which are typically conducted over the course of 4 weeks, include both tabletop drills and exercises that simulate combat between a mock adversary force and a 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 a 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 in a way that is as realistic as possible.

In preparation for the FOF exercises, information from tabletop drills, which probe for potential deficiencies in a 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 reviewed and corrected by the licensee. When a complete target set is simulated to be destroyed, and it is determined that the licensee's protective strategy does not demonstrate high assurance to protect against radiological sabotage in accordance with the DBT, compensatory measures, outlined in the licensee security plans, are put in place.[3] 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 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.

---

[3] For additional information, see the NRC's "Protecting Our Nation" (NUREG/BR-0314, Revision 4, published August 2015) 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/ML1523/ML15232A263.pdf and http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/bg-force-on-force.pdf.

3.2 Program Activities in 2015

Program activities in CY 2015 marked the second year of a 3-year ROP and FOF inspection cycle and the second year implementing a revised FOF inspection procedure. Following the procedure revisions, NRC staff assessed the program to ensure revisions provided NRC inspectors with useful insights into licensees' abilities 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. The NRC anticipates that the increased involvement by licensee senior management will lead to continued overall improvement of licensees' protective strategies and processes, further reinforcing their physical protection programs against the DBT of radiological sabotage. The revisions to the FOF inspection program continue to focus on evaluating the licensees' protective strategies while maintaining regulatory stability and consistency in the inspection process.

The NRC issued a revised FOF SDP, in CY 2014, that incorporated enhancements which provided a process for assessing each type of exercise performance outcome and gave credit for strong overall security performance. Throughout CY 2015, 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[4], 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 the program was 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 evaluation results to the Commission in a SECY paper dated August 20, 2014.[5] 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

---

[4] 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.

[5] 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.

and licensee resources on the most 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 it is taking action on those through a follow-on working group, which will report its findings to the Commission on June 1, 2016.[6]

In September 2015, the staff submitted a memorandum to the Commission[7] requesting approval to revise the notification of licensees for upcoming NRC-conducted FOF exercises from the current period of 8–12 weeks prior to the inspection to 9–15 months prior to the inspection. The staff believed this change would minimize disruptions to the NRC and licensees without impacting the integrity of the inspection program and would better align the FOF inspection program with the ROP. The Commission approved the staff's request in a Staff Requirements Memorandum[8] and the change was implemented in January 2016.

The composite adversaries used for inspections continue to meet expectations for a credible, well-trained mock adversary force. FOF inspection 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 inspection 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 FOF 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.

3.3 Results of Force-on-Force Inspections

According to the FOF SDP, an effective exercise is an exercise in which the licensee demonstrated effective implementation of its protective strategy in accordance with plans approved by the NRC and related implementation procedures, regulatory requirements, or other Commission requirements, such as orders or confirmatory action letters affecting protective strategy for the conduct of the FOF exercise. An indeterminate exercise is an exercise in which 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 in conflict with the training of security personnel to implement the site protective strategy or significant exercise control failures were experienced including controller performance failures). A marginal exercise is an exercise in which the licensee's performance prevented the loss of a complete target set, however the site's response force did not neutralize the adversary(s) before the adversary(s) simulated the destruction of multiple target set elements. An ineffective exercise is an exercise in which the licensee did not demonstrate effective implementation of its

---

6 SECY Paper to the Commission from Victor M. McCree, Executive Director for Operations, dated June 1, 2016, "SECY 16 0073—Options and Recommendations for the Force on Force Inspection Program in Response to SRM-SECY-14-0088," which can be found at: https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML16109A200

7 Memorandum to the Commission from Michael Johnson, Acting Executive Director for Operations, dated September 11, 2015, "Proposed Revision to the Notification Process for Force-on-Force Inspections," which can be found at: https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML15231A232.

8 Memorandum to Victor McCree, Executive Director for Operations, from Annette L. Vietti-Cook, Secretary of the Commission, dated October 6, 2015, "Staff Requirements – COMSECY-15-0025 – Proposed Revision to the Notification Process for Force-on-Force Inspections," which can be found at: https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML15279A468.

protective strategy in accordance with plans approved by the NRC and related implementation procedures, regulatory requirements, or other Commission requirements, such as orders or confirmatory action letters affecting protective strategy for the conduct of the FOF exercise.

By the end of 2015, the NRC had completed the second year of the fourth 3-year cycle of FOF inspections. Between January 1, 2015, and December 31, 2015, the NRC conducted 22 FOF inspections (at 21 commercial power reactors and 1 CAT I fuel cycle facility) and identified 26 findings that related to areas of the security baseline inspection program. Table 1 summarizes the 22 FOF inspections conducted in CY 2015.

Table 1: Calendar Year 2015 Force-on-Force Inspection Program Summary

22	Total number of inspections conducted (two exercises per inspection)
39	Total number of effective exercises
4	Total number of indeterminate exercises
0	Total number of marginal exercises
1	Total number of ineffective exercises
0	Total number of canceled exercises
26	Total number of inspection findings
26	Total number of green findings
0	Total number of greater-than-green findings
0	Total number of SL IV violations
0	Total number of greater-than-SL IV violations

In CY 2015, one exercise was deemed ineffective, resulting from the licensees' inability to demonstrate an effective implementation of its protective strategy to defend designated target set components. None of the exercises conducted in CY 2015 were marginal. Of the total number of exercises conducted in CY 2015, four exercises were inconclusive and deemed indeterminate. These exercises were deemed indeterminate because site responders neutralized adversaries using practices unanticipated by the design of the protective strategy, site responders' demonstration of use-of-force was inconsistent with the licensees' protective strategy, exercise controllers failed to control drill artificialities, or because of anomalies with the control of the exercise and performance related to the sites' protective strategy implementation. No exercises were canceled or postponed in CY 2015 because of dangerous weather conditions or any other extenuating circumstance.

3.4 Discussion of Corrective Actions

In addition to corrective actions taken 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, 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 an adversary's mission. Corrective actions that are not necessary to address an identified vulnerability or a specific requirement (e.g., enhancements) are not required. However, once these changes are incorporated into a licensee's security plans, as required by 10 CFR Part 73, "Physical Protection of Plants and Materials," they become lasting regulatory requirements.

3.5 Future Planned Activities

CY 2016, the third year of the fourth 3-year cycle of FOF inspections, began with 21 inspections scheduled for the year. Of these, none are follow-up inspections to assess corrective actions to evaluate improvements that licensees implemented as a result of prior FOF inspections.

PAGE INTENTIONALLY LEFT BLANK

4. SECURITY BASELINE INSPECTION PROGRAM AT COMMERCIAL NUCLEAR POWER REACTORS

4.1 Overview

The security baseline inspection program is a primary component of the security cornerstone of the ROP. FOF inspections are just one piece of the NRC's overall security oversight process. In addition to FOF inspections, the security baseline inspection program includes the following inspectable areas: access control; access authorization; protective strategy evaluation; security training; equipment performance, testing, and maintenance; fitness-for-duty program; protection of SGI; review of power reactor target sets; MC&A; and information technology (cyber) security.[9]

4.2 Results of Inspections

Table 2 summarizes the results of the security baseline inspection program for operating commercial nuclear reactors, excluding FOF inspection results (discussed in Section 3) and CAT I fuel cycle facility security inspection results (discussed in Section 5). Table 2 indicates that 107 out of 108 baseline security findings issued in CY 2015 were of very low security significance (i.e., green or SL IV violations).

Table 2: Calendar Year 2015 Security Inspection Summary for Commercial Nuclear Power Reactors (without Force-on-Force)

205	Total number of security inspections conducted
108	Total number of inspection findings
101	Total number of green findings
1	Total number of greater-than-green findings
6	Total number of SL IV violations
0	Total number of greater-than-SL IV violations

[9] Since 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 majority of cyber security findings identified in CY 2015. Consequently, the results of these very low security significance findings granted enforcement discretion are not reflected in Table 2.

PAGE INTENTIONALLY LEFT BLANK

5. CATEGORY I FUEL CYCLE FACILITY SECURITY OVERSIGHT PROGRAM

5.1 Overview

The NRC maintains regulatory oversight of safeguards and security programs at two CAT I fuel cycle facilities: BWXT 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. These 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 if 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 a 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.

5.2 Results of Category I Fuel Cycle Facility Inspections

Through its inspection program, the NRC has high assurance that CAT I fuel cycle facilities continue to meet the intent of the regulations. Table 3 summarizes the overall results of the security inspection program for CAT I fuel cycle facilities, excluding FOF inspection results discussed in Section 3.

Table 3: Calendar Year 2015 Security Inspection Summary for Category I Fuel Cycle Facilities (without Force-on-Force)

15	Total number of security inspections conducted
4	Total number of inspection findings
3	Total number of SL IV violations
1	Total number of greater-than-SL IV violations

6. SECURITY INSPECTION PROGRAM RESULTS FOR CALENDAR YEAR 2015

6.1 Overview

In CY 2015, the NRC conducted 242 security inspections at operating commercial power reactors and CAT I fuel cycle facilities, including FOF inspections. Those inspections resulted in a total of 138 findings.

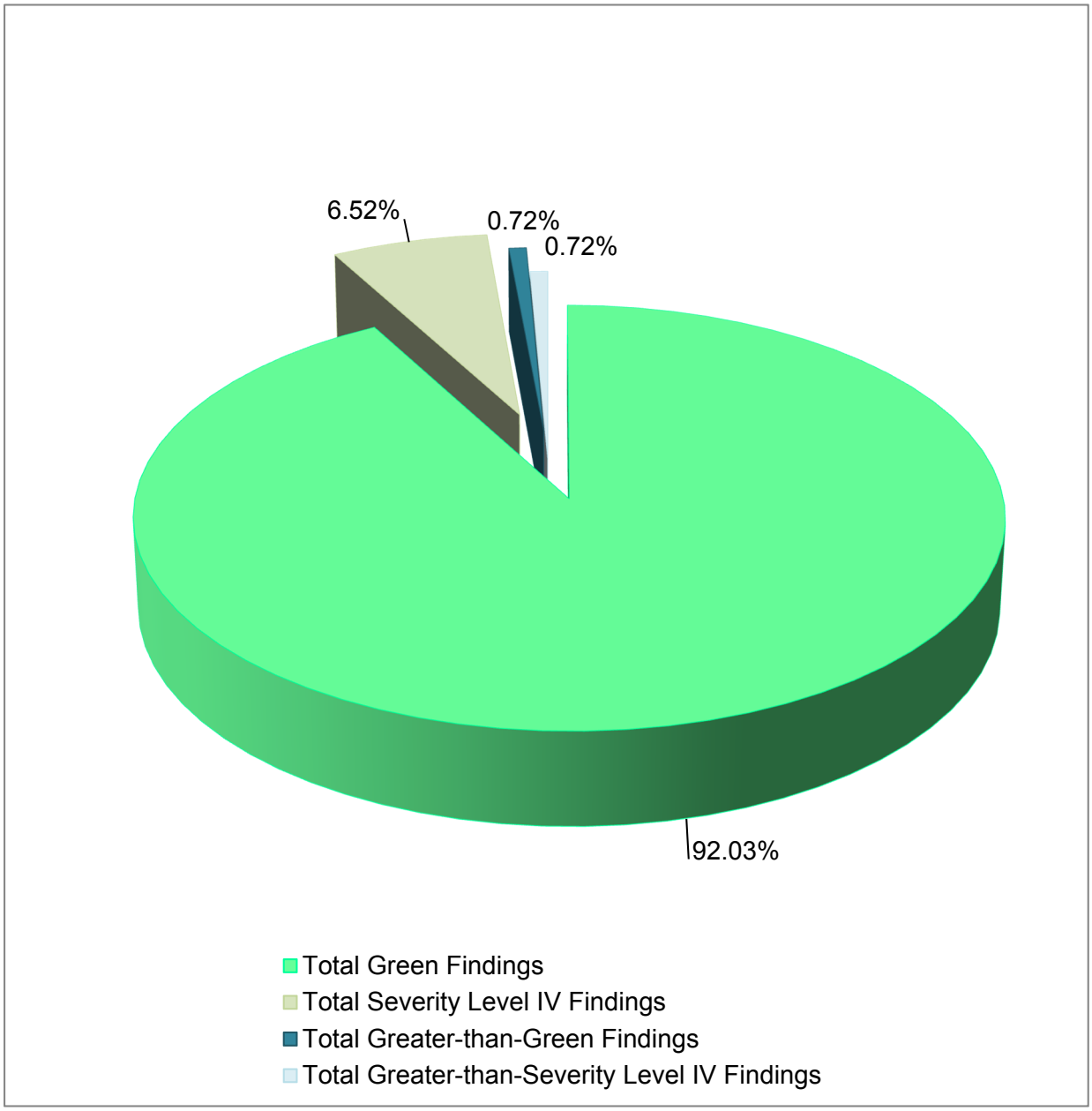
6.2 Results of Inspections

Table 4 summarizes the overall results of the NRC's security inspection program at operating commercial power reactors and CAT I fuel cycle facilities, including FOF inspections. Table 4 indicates that 136 out of 138 security inspection findings issued in CY 2015 were of very low security significance (i.e., green or SL IV violations). Figure 5 provides a graphic summary of the CY 2015 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 4: Calendar Year 2015 Security Inspection Program Summary

242	Total number of security inspections conducted
138	Total number of inspection findings
127	Total number of green findings
1	Total number of greater-than-green findings
9	Total number of SL IV violations
1	Total number of greater-than-SL IV violations

Figure 4: Summary of Security Inspection Program Results for Calendar Year 2015



7. EVOLVING SECURITY INSPECTION ACTIVITIES

7.1 Overview

Security is achieved through defense-in-depth, with multiple approaches utilized 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.

7.2 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 licensees to protect digital computer systems and networks associated with safety-related and important-to-safety, security, and emergency preparedness functions.

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 their cyber security plans to meet the new requirements.

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 all interim implementation inspections by the end of CY 2015.

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 Sections 4 or 6 of this report.

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 final rulemaking package was published on November 2, 2015, became effective on December 2, 2015, and has a compliance date of May 2, 2016. This rule

will contribute to the NRC's analysis of the reliability and effectiveness of licensees' cyber security programs.

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.[10] 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.[11]

A cyber security working group was established in 2011 to review 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. Based on site visits and reviews of licensees' cyber security programs, the working group, in December 2014, provided three recommendations to the Commission on how to strengthen cyber security at fuel cycle facilities regulated by the NRC. In March 2015, the Commission voted and approved the initiation of an expedited cyber security rulemaking for fuel cycle facilities.[12] The NRC started working on the rulemaking in mid-2015 and will continue working on it into CY 2016.

7.3 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 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 was 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 met.

Inspections associated with TI 2515/186 were completed by May 2014. No significant issues were identified. The NRC issued a final report on June 17, 2015, documenting results and recommendations associated with the TI.[13] Identified issues were discussed during a public meeting held on July 15, 2015.[14] The ROP will be utilized to ensure that any issues are appropriately addressed through the licensees' corrective action program. The objectives of TI 2515/186 have been accomplished and the TI was deleted in June 2015.

---

10 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.

11 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.

12 For more information on the Commission's direction to staff, please refer to Memorandum to Mark A. Satorius, Executive Director for Operations, from Annette L. Vietti-Cook, Secretary of the Commission, dated March 24, 2015, "Staff Requirements – SECY-14-0147 - Cyber Security For Fuel Cycle Facilities," which can be found at: https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML15083A175.

13 Memorandum to Christopher M. Regan from Aron Lewin dated June 17, 2015, "Final Report Documenting Results and Recommendations Associated With Temporary Instruction 2515/186, "Inspection of Procedures and Processes for Responding to Potential Aircraft Threats,"" which can be found at: https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML15163A252.

14 Memorandum to Nathan Sanfilippo from Andrew Waugh dated August 12, 2015, "Summary of the Reactor Oversight Process Working Group Public Meeting Held on July 15, 2015," which can be found at: https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML15211A130.

7.4 Decommissioning Power Reactors

Over the last 3 years, five operating power reactors were transitioned to decommissioning status when the 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 ensure that a licensee's overall security program is meeting the general performance objective of the applicable NRC regulation, 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 a 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 does 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.

7.5 Category 1 and Category 2 Materials

On March 19, 2013, the NRC published the final rule for 10 CFR Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material." The objective of this rule was to establish generically applicable security requirements for the protection of Category 1 and Category 2 quantities of radioactive materials possessed by certain NRC and Agreement State licensees. These security requirements are similar to the requirements imposed on these licensees through the NRC's previously issued increased controls security orders; however, this rulemaking expanded the scope of applicability of those orders to include such production and utilization facilities as power reactors, fuel cycle facilities, and independent spent fuel storage installations. The NRC issued TI 2800/041, "10 CFR Part 37 Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material at Facilities with a 10 CFR Part 73 Physical Protection Program," in July 2015 to address Part 37 inspections at power reactors, fuel cycle facilities, and independent spent fuel storage installations. Part 37 inspections commenced in October 2015. Thus far, there have been no significant issues identified regarding the protection of Category 1 and Category 2 quantities of material at these 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 conducted at nuclear reactors since May 2006. Furthermore, as of April 2015, the Commission decided that, to meet the agency's goal for increased transparency and openness, the NRC would treat CAT I fuel cycle facility cover letters similar to those of reactor licenses and began releasing the cover letters for security-related inspection reports.

The NRC continues to hold public meetings specifically about nuclear-security issues.[15] For example, the agency presents a variety of security topics at its Regulatory Information Conference, held each spring in Rockville, Maryland.[16] 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 2015, the NRC issued 11 security advisories, 3 regulatory issue summaries related to security, 2 information notices related to security, and no information assessment team advisories (see Section 8.2 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.

8.2 Calendar Year 2015 List of Generic Communications by Title[17]

Security Advisories

SA 15-01, SA 15-02, SA 15-03	"National Special Security Event for the 2015 Presidential State of the Union Address"
SA 15-04, SA 15-05, SA 15-06	"National Special Security Event for the 2015 Papal Visit to Washington, DC"

[15] For more information on the NRC's public meeting schedule, please refer to http://meetings.nrc.gov/pmns/mtg.

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

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

Security Advisories

SA 15-07, SA 15-08	"National Special Security Event for the 2015 World Meeting of Families"
SA 15-09, SA 15-10	"National Special Security Event for the United Nations General Assembly and Papal Visit to New York, NY"
SA 15-11	"Situational Awareness-Security Concerns Related to Geocaching and Other Similar Geolocating Game Activity Near Critical Infrastructure Facilities"

Regulatory Issue Summaries

RIS 15-03	"Identifying and Reporting Security Incidents Under 10 CFR Part 37"
RIS 15-08	"Oversight of Counterfeit, Fraudulent, and Suspect Items in the Nuclear Industry"
RIS 15-15	"Information Regarding a Specific Exemption in the Requirements for the Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material"

Information Notices

IN 15-06	"Message from OPM to Security Clearance Holders"
IN 15-07	"Temporary Suspension of e-QIP System to Affect Pending Background Investigations"

Information Assessment Team Advisories

N/A

8.3 Communications with Federal, State, and Local Agencies

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

The NRC and Federal Bureau of Investigation (FBI) continue to support initiatives to enhance integrated response planning for NPPs.

The FBI has completed and approved all site-specific integrated response plans, which identify Federal, State, and local law enforcement agencies with tactical teams and their roles and responsibilities. To date, contingency response tools for 23 NPPs have been completed. The computer-aided planning tools familiarize law enforcement with the site and allow for the law enforcement teams to plan and execute onsite missions in support of a site's public health and safety priorities.