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 2016

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 twelfth annual report, which covers calendar year 2016. 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, and the common defense and security through the effective regulation of the Nation's commercial nuclear power facilities and strategic special nuclear material.

Paperwork Reduction Act Statement

NUREG-1885, Revision 10, "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

CONTENTS

ABSTRACT iii
FIGURES vii
TABLES vii
ACRONYMS ix
1. INTRODUCTION 1
2. REACTOR SECURITY OVERSIGHT PROCESS 3
2.1 Overview 3
2.2 Significance Determination Process 6
2.3 Findings and Violations 7
2.4 Performance Indicator 7
2.5 Reactor Oversight Process Action Matrix 8
3. FORCE-ON-FORCE INSPECTION PROGRAM 9
3.1 Overview 9
3.2 Program Activities in 2016 10
3.3 Results of Force-on-Force Inspections 11
3.4 Discussion of Corrective Actions 12
3.5 Future Planned Activities 13
4. SECURITY BASELINE INSPECTION PROGRAM AT COMMERCIAL NUCLEAR POWER REACTORS 15
4.1 Overview 15
4.2 Results of Inspections 15
5. CATEGORY I FUEL CYCLE FACILITY SECURITY OVERSIGHT PROGRAM 17
5.1 Overview 17
5.2 Results of Category I Fuel Cycle Facility Inspections 18
6. SECURITY INSPECTION PROGRAM RESULTS FOR CALENDAR YEAR 2016 19
6.1 Overview 19
6.2 Results of Inspections 19
7. EVOLVING SECURITY INSPECTION ACTIVITIES 21
7.1 Overview 21
7.2 Cyber Security 21
7.3 Decommissioning Power Reactors 22
7.4 Category 1 and Category 2 Materials 22
8. STAKEHOLDER COMMUNICATIONS 23
8.1 Communications with the Public, Licensees, and Other Stakeholders 23
8.2 Calendar Year 2016 List of Generic Communications by Title 23
8.3 Communications with Federal, State, and Local Agencies 24

PAGE INTENTIONALLY LEFT BLANK

FIGURES

Figure 1: Reactor Oversight Framework 3
Figure 2: Inspectable Areas of the Security Cornerstone 5
Figure 3: Reactor Oversight Process 5
Figure 4: Summary of Security Inspection Program Results for Calendar Year 2016 20

TABLES

Table 1: Calendar Year 2016 Force-on-Force Inspection Program Summary 12
Table 2: Calendar Year 2016 Security Inspection Summary for Commercial Nuclear Power Reactors (without Force-on-Force) 15
Table 3: Calendar Year 2016 Security Inspection Summary for Category I Fuel Cycle Facilities (without Force-on-Force) 18
Table 4: Calendar Year 2016 Security Inspection Program Summary 20

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
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
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 twelfth annual report covers calendar year (CY) 2016. 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, and the common defense and security 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.

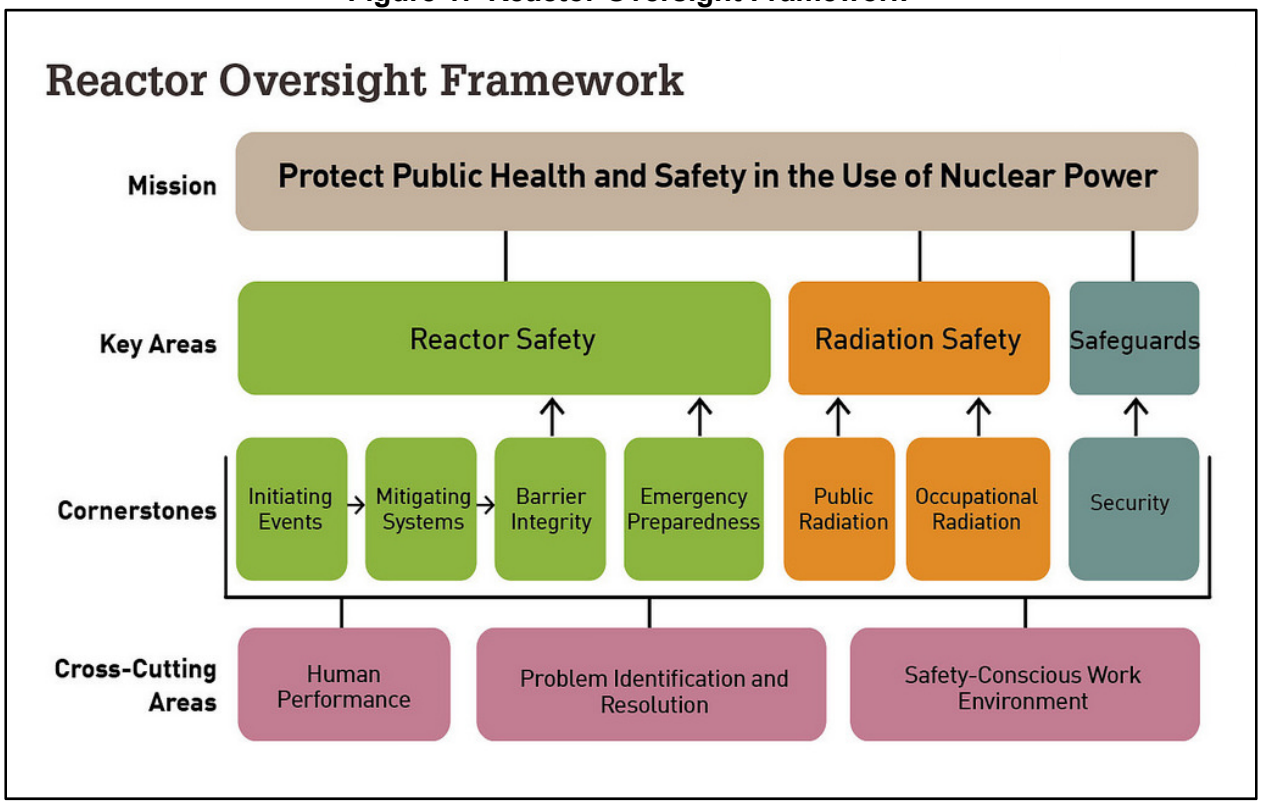
PAGE INTENTIONALLY LEFT BLANK

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

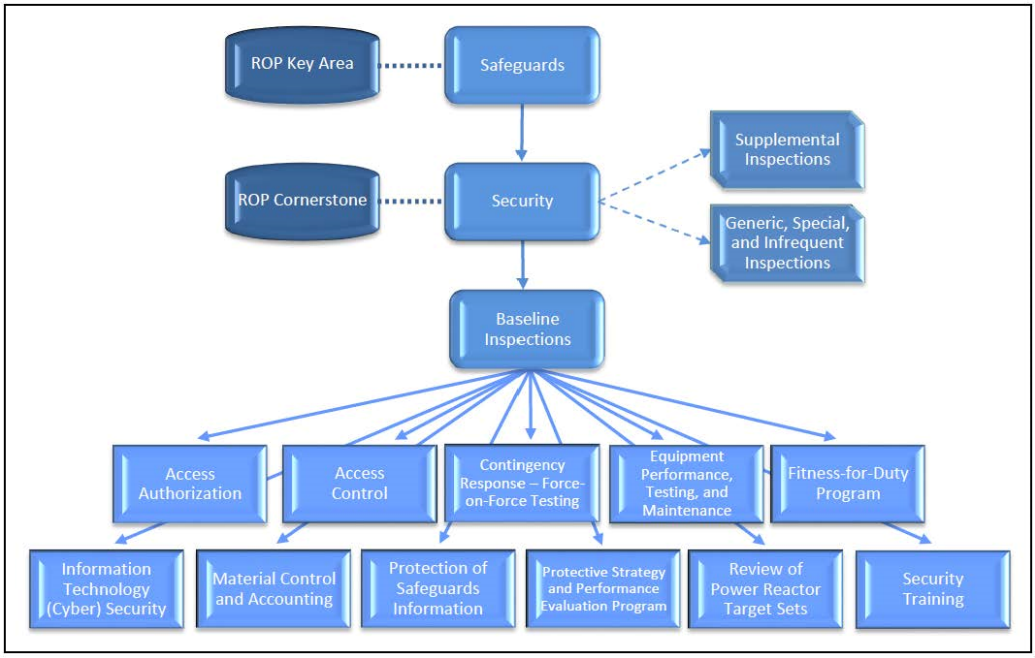


As part of its actions following the terrorist attacks of September 11, 2001, the NRC issued a number of orders requiring licensees to strengthen security programs in several areas. During 2009 the NRC completed a rulemaking that made generally applicable security requirements similar to these orders 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 meet the general performance objective of 10 CFR 73.55(b), which is to provide high assurance[1] that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.

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 ensure 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."

Figure 2: Inspectable Areas of the Security Cornerstone



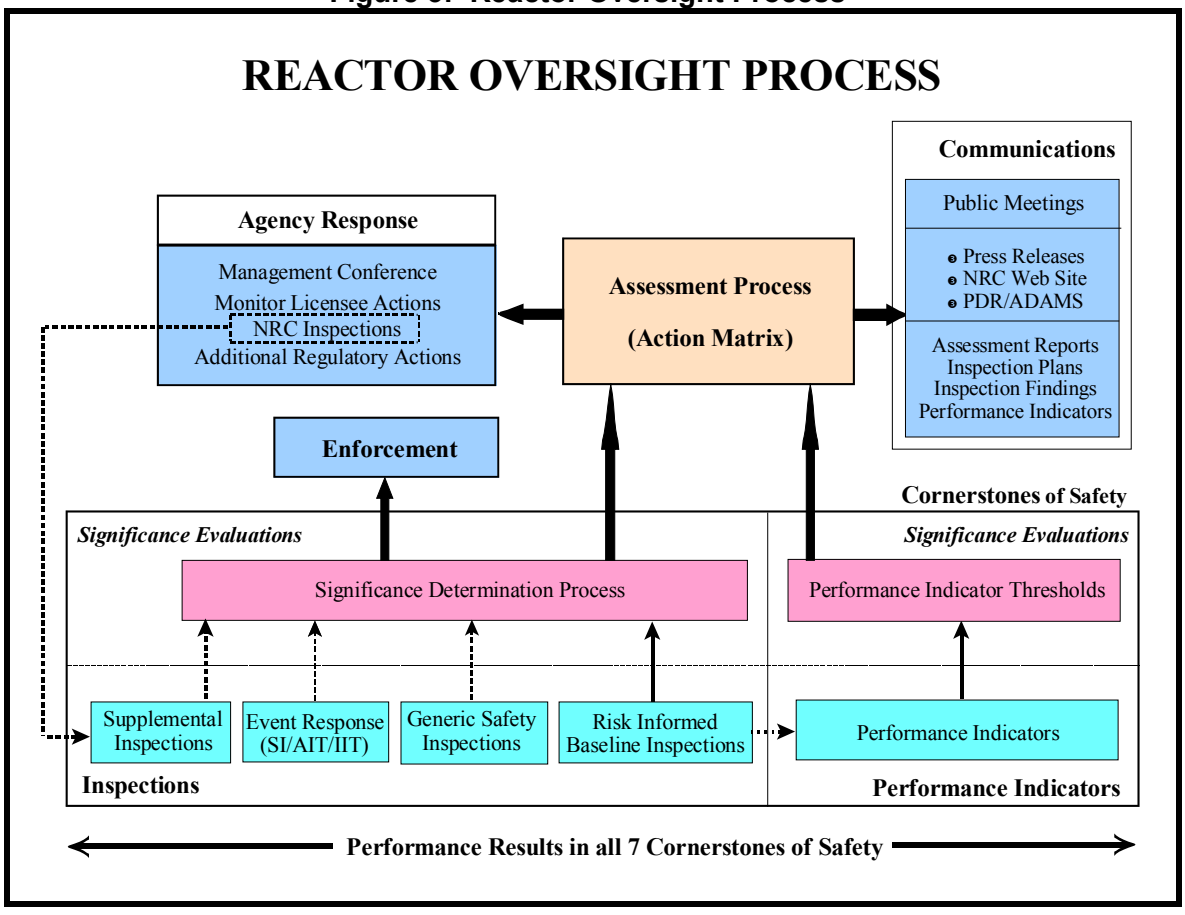
[1] In a memorandum to Victor M. McCree, Executive Director for Operations, from Annette L. Vietti-Cook, Secretary of the Commission, dated October 5, 2016, "Staff Requirements – SECY-16-0073 – Options and Recommendations for the Force-on-Force Inspection Program in Response to SRM-SECY-14-0088," the Commission provided the following direction, "In implementing the NRC's regulatory program, either in developing new regulations, inspecting licensee compliance with regulations, or executing the FOF program, the staff should be mindful that the concept of 'high assurance' of adequate protection found in our security regulations is equivalent to 'reasonable assurance' when it comes to determining what level of regulation is appropriate." The Staff Requirements Memorandum can be found at https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML16279A345.

The security 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.

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[2] 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[3]



2 Additional information on the ROP action matrix is provided in Section 2.5.

3 For additional information on the NRC's ROP, please refer to NUREG-1649, "Reactor Oversight Process" (Revision 6, July 2016), which can be found at http://www.nrc.gov/docs/ML1621/ML16214A274.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, security information is included in the quarterly updates to action matrix inputs. 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 (i.e., blue) to reflect greater-than-green significance. Not specifying the actual color of greater-than-green security inputs is consistent with the 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 the 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 the 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 SDP.

During CY 2016, the NRC continued to monitor and evaluate the Baseline Security SDP to ensure it continued 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 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 SDP 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 are also typically related 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 the traditional enforcement process at commercial nuclear power reactors to evaluate violations that resulted in actual safety or security consequences, violations that may impact the ability of the NRC to perform its regulatory oversight function, or violations 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 is 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 2016, 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 https://www.nrc.gov/reactors/operating/oversight/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 a 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 input results in a repetitive degraded cornerstone, multiple degraded cornerstones, multiple yellow inputs, or one 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. 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 https://www.nrc.gov/reactors/operating/oversight/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 performance-based FOF inspection exercises, which simulate combat between a mock adversary force and a licensee's security force. At an NPP, the mock adversary force attempts to reach and simulate damage to significant components of safety-related systems (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 mock 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 meet the general performance objective, which is to provide high assurance to protect against radiological sabotage in accordance with the DBT, compensatory measures outlined in the licensee security plans are put in place.[4] 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 one exercise to satisfy inspection requirements, but only when the licensee has successfully demonstrated an effective strategy in that exercise with no significant issues identified. If those conditions are not met, the inspection team may have to extend the inspection or return to the site to conduct a subsequent exercise.

[4] 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 2016). These documents are available at http://pbadupws.nrc.gov/docs/ML1523/ML15232A263.pdf and https://www.nrc.gov/docs/ML0436/ML043620052.pdf.

3.2 Program Activities in 2016

Program activities in CY 2016 marked the third year of a 3-year ROP and FOF inspection cycle, as well as the third year implementing a revised FOF inspection procedure. Following the procedure revisions, the 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.

In a February 2014 Staff Requirements Memorandum,[5] 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 NRC's Executive Director for Operations provided the evaluation results to the Commission in a SECY paper dated August 20, 2014.[6] 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 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 reported its findings to the Commission on June 1, 2016.[7] On October 5, 2016,

---

5 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.

6 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.

7 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.

the Commission issued a Staff Requirements Memorandum,[8] which approved the staff's recommended option to conduct an assessment of the security baseline inspection program. The NRC staff will submit a notation paper to the Commission in CY 2017 with recommendations on enhancements to the security inspection program to include evaluating whether credit could be given for diverse and flexible coping strategies equipment and whether the NRC should provide credit for local, State, or Federal law enforcement response to establish coping time for security events.

In July 2016, the staff submitted a memorandum to the Commission[9] requesting approval to revise the notification of licensees for upcoming NRC-conducted FOF exercises from the current period of 9–15 months prior to the inspection to 24 months prior to the inspection. The Commission approved the staff's request in a Staff Requirements Memorandum dated August 10, 2016.[10] This change will provide for increased planning and coordination, which will minimize disruptions to the NRC and licensees without impacting the integrity of the inspection program and will better align the FOF inspection program with the ROP.

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. U.S. Special Operations Command members also support the NRC inspection team in the tactical planning of FOF exercises. Additionally, FOF inspection team members review adversary team briefings to ensure that the information provided accurately reflects established parameters. The composite adversaries used for inspections continue to meet expectations for a credible, well-trained mock adversary force. 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 identified.

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 the 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(ies) before the adversary(ies) simulated the destruction of multiple target set

---

8 Memorandum to Victor M. McCree, Executive Director for Operations, from Annette L. Vietti-Cook, Secretary of the Commission, dated October 5, 2016, "Staff Requirements – 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=ML16279A345.

9 Memorandum to the Commission from Victor M. McCree, Executive Director for Operations, dated July 25, 2016, "Proposed Revision to the Notification Process for Force-on-Force Inspections," which can be found at https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML16167A168.

10 Memorandum to Victor M. McCree, Executive Director for Operations, from Annette L. Vietti-Cook, Secretary of the Commission, dated August 10, 2016, "Staff Requirements – COMSECY-16-0016 – Proposed Revision to the Notification Process for Force-on-Force Inspections," which can be found at https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML16223A639.

elements. An ineffective exercise is an exercise in which the licensee did not demonstrate 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 the protective strategy for the conduct of the FOF exercise.

By the end of 2016 the NRC had completed the third year of the fourth 3-year cycle of FOF inspections. Between January 1, 2016, and December 31, 2016, the NRC conducted 21 FOF inspections (at 20 commercial power reactors and 1 CAT I fuel cycle facility) and identified 20 findings that related to areas of the security baseline inspection program. Table 1 summarizes the 21 FOF inspections conducted in CY 2016.

Table 1: Calendar Year 2016 Force-on-Force Inspection Program Summary

21	Total number of inspections conducted (two exercises per inspection)
37	Total number of effective exercises
1	Total number of indeterminate exercises
1	Total number of marginal exercises
1	Total number of ineffective exercises
2	Total number of canceled exercises
20	Total number of inspection findings
20	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 2016 one exercise was deemed ineffective, resulting from the licensee's inability to demonstrate an effective implementation of its protective strategy to defend designated target set components. One exercise in CY 2016 was determined to be marginal because the adversary(ies) was neutralized at a location, or making preparations to enter a location, that contained a single element target set. Additionally, one exercise was deemed indeterminate because of significant controller performance issues. Specifically, the licensee failed to properly control the exercise, which resulted in the NRC inspection team's inability to assess the licensee's capability to implement its protective strategy. In these cases, the licensees took appropriate corrective action. Two exercises were canceled in CY 2016 because of dangerous weather conditions (i.e., substantial rain, lightning, and tornado warnings).

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 routinely 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, gates, or locks on doors. If a licensee determines that earlier detection and assessment capabilities 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 area 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 2017, the first year of the fifth 3-year cycle of FOF inspections, began with 19 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.

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 120 out of 128 baseline security findings issued in CY 2016 were of very low security significance (i.e., green or SL IV violations).

Table 2: Calendar Year 2016 Security Inspection Summary for Commercial Nuclear Power Reactors (without Force-on-Force)

189	Total number of security inspections conducted
128	Total number of inspection findings
117	Total number of green findings
2	Total number of greater-than-green findings
3	Total number of SL IV violations
6	Total number of greater-than-SL IV violations

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. 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 the FOF inspection results discussed in Section 3.

Table 3: Calendar Year 2016 Security Inspection Summary for Category I Fuel Cycle Facilities (without Force-on-Force)

14	Total number of security inspections conducted
3	Total number of inspection findings
3	Total number of SL IV violations
0	Total number of greater-than-SL IV violations

6. SECURITY INSPECTION PROGRAM RESULTS FOR CALENDAR YEAR 2016

6.1 Overview

In CY 2016, the NRC conducted 224 security inspections at operating commercial power reactors and CAT I fuel cycle facilities, including FOF inspections. Those inspections resulted in a total of 151 findings.

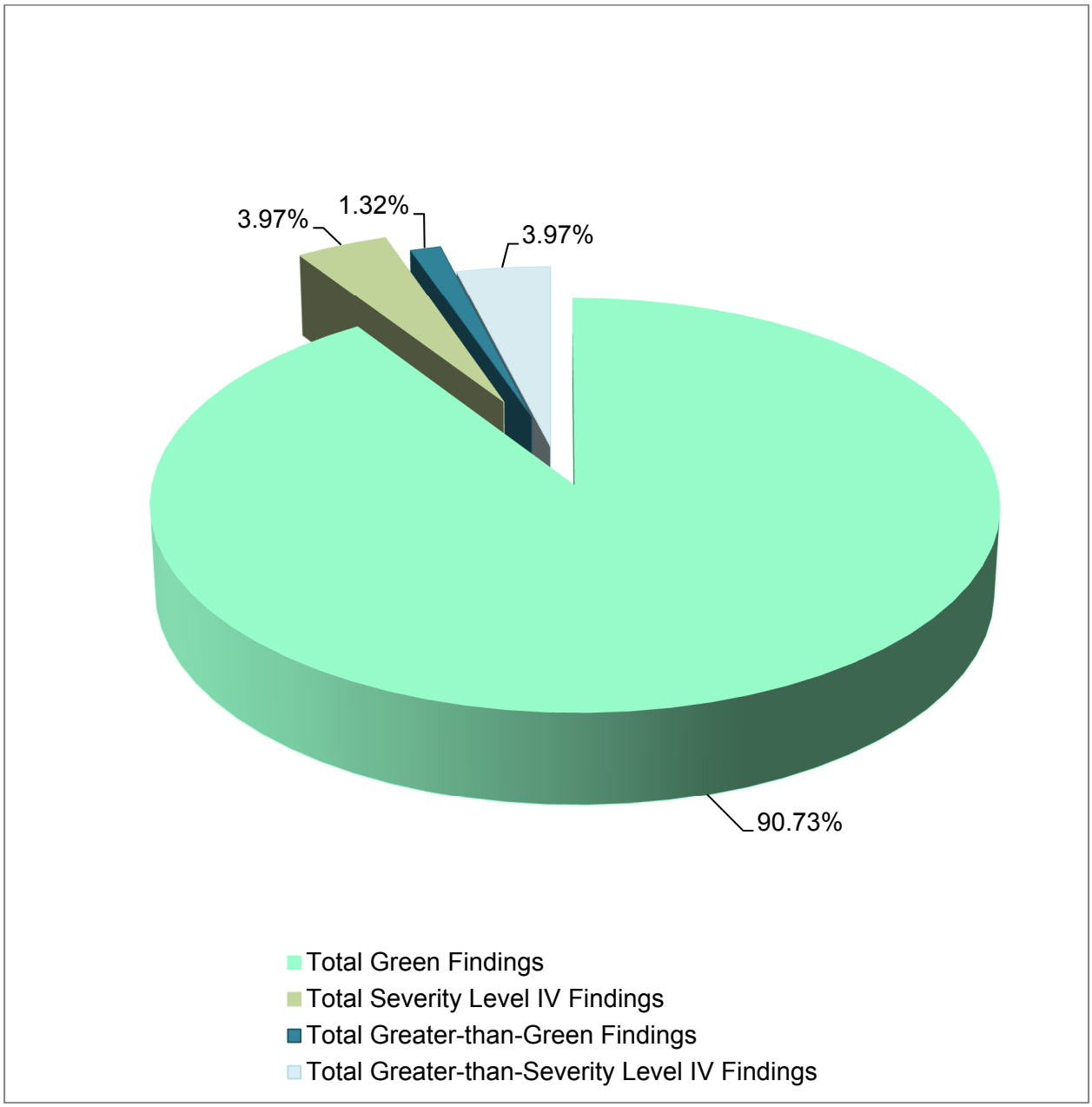
6.2 Results of Inspections

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 143 out of 151 security inspection findings issued in CY 2016 were of very low security significance (i.e., green or SL IV violations). Figure 4 provides a graphic summary of the CY 2016 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 2016 Security Inspection Program Summary

224	Total number of security inspections conducted
151	Total number of inspection findings
137	Total number of green findings
2	Total number of greater-than-green findings
6	Total number of SL IV violations
6	Total number of greater-than-SL IV violations

Figure 4: Summary of Security Inspection Program Results for Calendar Year 2016



7. EVOLVING SECURITY INSPECTION ACTIVITIES

7.1 Overview

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

This 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 staff is reviewing license amendment requests to delay implementation for sites planning to or currently in decommissioning status. The staff has recently approved the delay for San Onofre Nuclear Generating Station and removal of cyber requirements for Kewaunee Power Station. The NRC began cyber security inspections in January 2013 and completed all interim implementation inspections by the end of CY 2015, and plans to begin full implementation inspections in the latter half of 2017.

Most inspections revealed several very low security significance violations of cyber security plan requirements. Licensees are increasing their ability to identify problems and are working with the NRC on remediation solutions. No significant violations were identified. Because the cyber security requirements are new, and licensees demonstrated a good-faith attempt to implement the requirements, the NRC 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 NRC issued 10 CFR 73.77, "Cyber Security Event Notifications," that requires 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 rule became effective on December 2, 2015, and had 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.[11] 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 determine whether any program improvements are needed.[12]

A cyber security working group was established in 2011 to review fuel cycle facilities' cyber security programs 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. In March 2015, the Commission voted and approved the initiation of an expedited cyber security rulemaking for fuel cycle facilities.[13] The NRC started working on the rulemaking in mid-2015 and completed the final regulatory basis in March 2016. Throughout CY 2016, the NRC worked on the draft proposed rule and expects it to be delivered to the Commission in fall 2017.

7.3 Decommissioning Power Reactors

The NRC provides oversight of licensee security programs at decommissioning power reactors through a security inspection program that examines licensee activities in order to assess performance and to ensure that a licensee's overall security program is meeting applicable NRC regulations (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 ensures that core inspection procedures used at reactors entering the decommissioning process provide 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.

7.4 Category 1 and Category 2 Materials

To date, no significant issues have been identified regarding the protection of Category 1 and Category 2 quantities of material at these facilities.

---

11 For more information on the NRC's cyber security roadmap, please refer to https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML16354A258.

12 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.

13 For more information on the Commission's direction to the 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.

8. STAKEHOLDER COMMUNICATIONS

8.1 Communications with the Public, Licensees, and Other Stakeholders

The NRC publically releases the cover letters to NPP security-related inspection reports. 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.[14] For example, the agency presents a variety of security topics at its Regulatory Information Conference, held each spring in Rockville, Maryland.[15] Security topics at the Regulatory Information Conference range from security-related rulemaking efforts to activities associated with security inspection and oversight of NRC-licensed facilities to the latest cyber security and emergency preparedness and response activities undertaken by the agency.

The NRC also communicates with the public, licensees, and other stakeholders by disseminating generic communications and key lessons learned from security activities and inspections. The NRC analyzes findings and observations from the security inspection program to determine potential generic issues. When applicable, the NRC staff supplements periodic security meetings held with the industry and other key stakeholders and develops generic communications, such as security advisories, as a means of effectively communicating security-related issues. In CY 2016, the NRC issued 12 Security Advisories, 3 Regulatory Issue Summaries related to security, 1 Information Notice related to security, and no Information Assessment Team Advisories (see Section 8.2 for a complete list).

After each FOF inspection, the NRC staff compiles 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 2016 List of Generic Communications by Title[16]

Security Advisories

SA 16-01, SA 16-02, SA 16-03	"National Special Security Event for the 2016 Presidential State of the Union Address"
SA 16-04, SA 16-05, SA 16-06	"National Special Security Event for the 2016 Nuclear Security Summit"

Security Advisories *(cont'd)*

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

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

[16] 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/.

SA 16-07, SA 16-08	"National Special Security Event for the 2016 Republican National Convention"
SA 16-09, SA 16-10	"National Special Security Event for the 2016 Democratic National Convention"
SA 16-11, SA 16-12	"National Special Security Event for the 71st United Nations General Assembly"

Regulatory Issue Summaries

RIS 16-05	"Embedded Digital Devices in Safety-Related Systems"
RIS 16-10	"License Amendment Requests for Changes to Emergency Response Organization Staffing and Augmentation"
RIS 16-12	"NRC Employee Access to Switchyards at Licensee Facilities"

Information Notices

IN 16-10	"Identification and Protection of Unattended Openings and Underground Pathways that Intersect a Security Boundary"

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 the Federal Bureau of Investigation continue to support initiatives to enhance integrated response planning for NPPs.

The Federal Bureau of Investigation 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 26 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.