

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 2017

U.S. Nuclear Regulatory Commission
Office of Nuclear Security and Incident Response
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 *United States Code* (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 13th annual report, and covers calendar year (CY) 2017. In addition to 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).

Paperwork Reduction Act Statement

NUREG-1885, Revision 11, “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	7
2.3 Findings and Violations	7
2.4 Performance Indicator	8
2.5 Reactor Oversight Process Action Matrix	8
3. FORCE-ON-FORCE INSPECTION PROGRAM	10
3.1 Overview	11
3.2 Program Activities in 2017	11
3.3 Results of Force-on-Force Inspections	12
3.4 Discussion of Corrective Actions	13
4. SECURITY BASELINE INSPECTION PROGRAM AT COMMERCIAL NUCLEAR POWER REACTORS	14
4.1 Overview	14
4.2 Results of Inspections	14
5. CATEGORY I FUEL CYCLE FACILITY SECURITY OVERSIGHT PROGRAM	16
5.1 Overview	16
5.2 Results of Category I Fuel Cycle Facility Inspections	17
6. SECURITY INSPECTION PROGRAM RESULTS FOR CALENDAR YEAR 2017	18
6.1 Overview	18
6.2 Results of Inspections	18

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.....	6
Figure 4: Summary of Security Inspection Program Results for Calendar Year 2017	19

TABLES

Table 1: Calendar Year 2017 Force-on-Force Inspection Program Summary.....	13
Table 2: Calendar Year 2017 Security Inspection Summary for Commercial Nuclear Power Reactors (without Force on Force).....	14
Table 3: Calendar Year 2017 Security Inspection Summary for Category I Fuel Cycle Facilities (without Force on Force)	17
Table 4: Calendar Year 2017 Security Inspection Program Summary	18

PAGE INTENTIONALLY LEFT BLANK

ACRONYMS

10 CFR	Title 10 of the <i>Code of Federal Regulations</i>
ADAMS	Agencywide Documents Access and Management System
CAT I	Category I
CY	calendar year
DBT	design-basis threat
FOF	force-on-force
HEU	highly enriched uranium
MC&A	material control and accounting
NEI	Nuclear Energy Institute
NPP	nuclear power plant
NRC	U.S. Nuclear Regulatory Commission
PI	performance indicator
RIC	Regulatory Information Conference
RIS	Regulatory Issue Summary
ROP	Reactor Oversight Process
SA	security advisory
SDP	significance determination process
SGI	Safeguards Information
SL	severity level
SSNM	strategic special nuclear material
U.S.C.	<i>United States Code</i>

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 13th annual report covers CY 2017. In addition to providing information on the security response evaluation program FOF inspections, the NRC is providing additional information regarding the overall security performance of the commercial nuclear power industry and 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 SSNM.

Conducting FOF inspections 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 mitigating 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 programs and FOF inspections, 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). 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 $\text{grams} = (\text{grams contained Uranium-235}) + 2.5 (\text{grams Uranium-233} + \text{grams plutonium})$. 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 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.

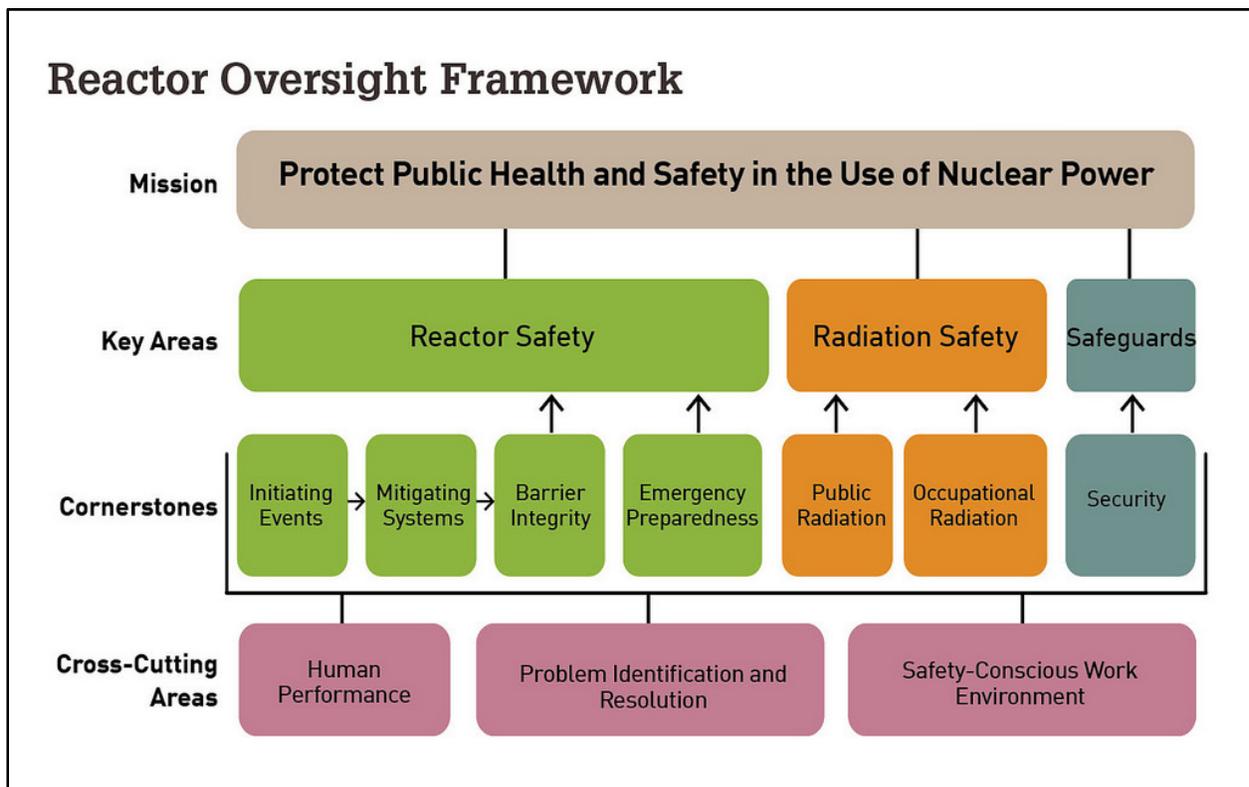


Figure 1: Reactor Oversight Framework

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. As a result of these actions, 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 assurance¹ that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to 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 design-basis threat (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 a facility's security status and conditions;
- (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."

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." (Agencywide Documents Access and Management System (ADAMS) Accession No. ML16279A345).

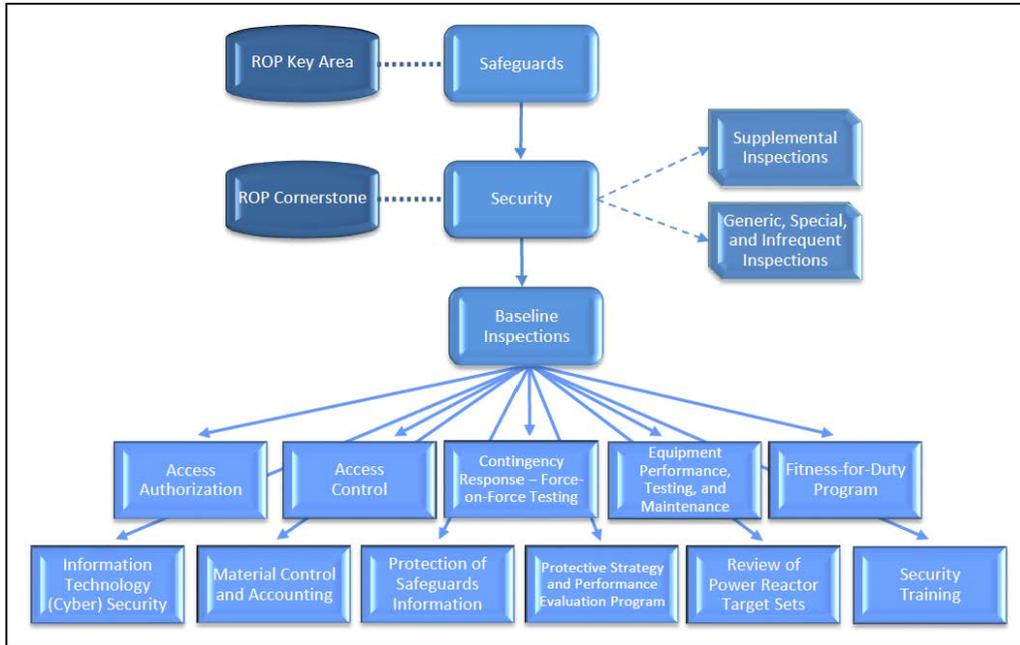


Figure 2: Inspectable Areas of the Security Cornerstone

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 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 matrix² 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.

² Section 2.5 contains additional information on the ROP action matrix.

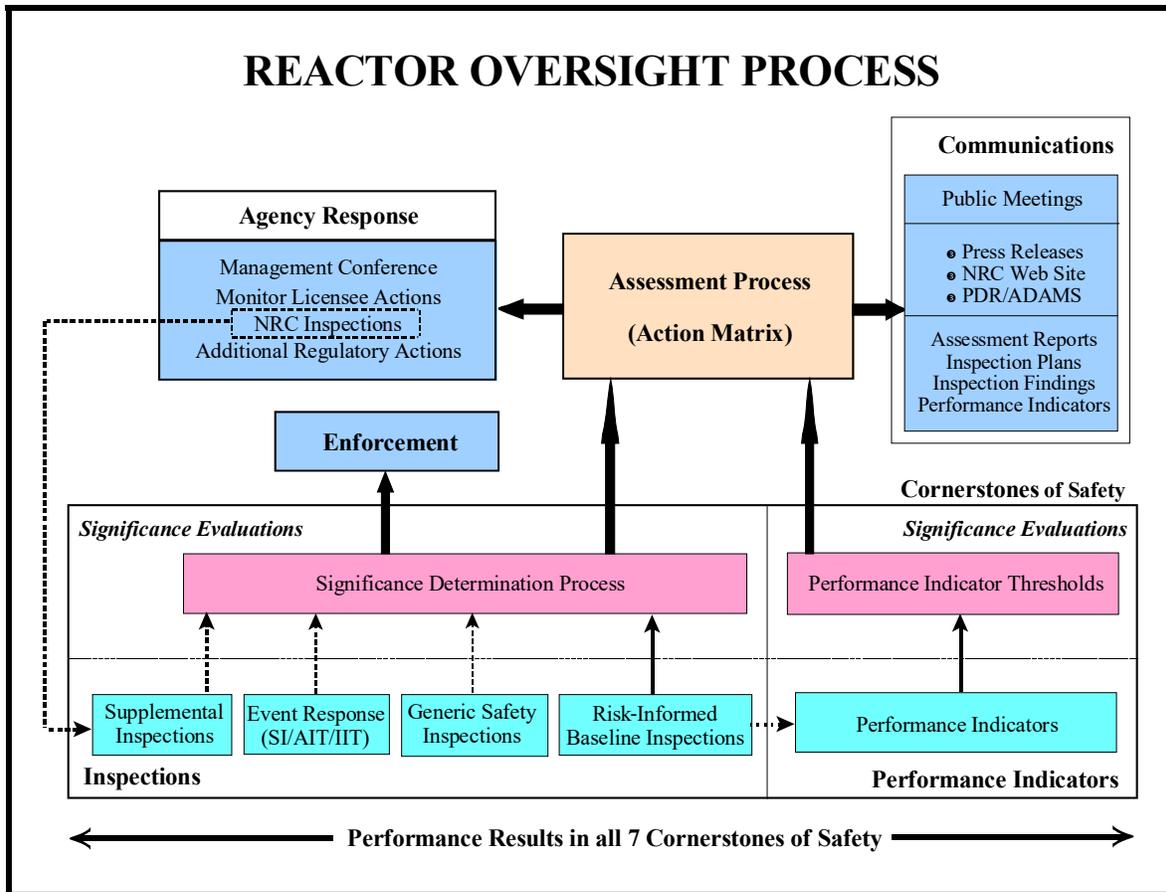


Figure 3: Reactor Oversight Process³

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

³ For additional information on the NRC's ROP, please refer to NUREG-1649, "Reactor Oversight Process" (Revision 6, July 2016, ADAMS Accession No. ML16214A274).

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 uses the baseline security SDP to evaluate security-related findings and determine the significance of security program deficiencies.

During CY 2017, the NRC monitored and evaluated 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 inspection 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 noncited 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. 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 affect the ability of the NRC to perform its regulatory oversight function, or violations involving willfulness. The NRC staff categorizes these violations in terms of four levels of severity to show their relative importance or significance. It assigns Severity Level (SL) I to the most significant violations. SL I violations are those that resulted in, or could have resulted in, serious safety or security consequences. SL II violations are those that resulted in, or could have resulted in, significant safety or security consequences. SL III violations are those that resulted in, or could have resulted in, moderate safety or security consequences. SL IV violations are those that are less serious but are of more-than-minor concern, that resulted in no or relatively inappreciable potential safety or security consequences. For particularly significant violations, the Commission reserves the use of its discretion to assess civil penalties in accordance with Section 234 of the Atomic Energy Act of 1954, as amended.

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 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 2017, 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 list 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 cornerstones; 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's 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 list 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>.

PAGE INTENTIONALLY LEFT BLANK

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 two 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 force to prevent the adversary from reaching target sets, thus preventing 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 NRC goal is to balance actual personnel and plant safety and security while conducting a security exercise.

In preparation for the FOF inspections, 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. The FOF inspections consider security baseline inspection results and security plan reviews. Any significant deficiencies in the protective strategy identified during FOF inspections 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 of protection 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.

3.2 Program Activities in 2017

Program activities in CY 2017 marked the first year of a 3-year ROP and FOF inspection cycle, as well as the first year implementing a revised FOF inspection procedure. This revision

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, ADAMS Accession No. ML043620052).

removed an addendum that addressed specific issues involving FOF rules of engagement from the inspection procedure and adjusted the resource estimate to complete the inspection procedure samples. The NRC based the resource allocation adjustment on efficiencies gained through previous years of implementing FOF inspections. The addendum was no longer necessary because the NRC incorporated the material into other appropriate guidance documents. During CY 2017, the agency assessed the revisions to ensure the program continued to provide NRC inspectors with useful insights into licensees' ability to implement a protective strategy that defends against the DBT of radiological sabotage.

Additionally, the Commission continues deliberation on a set of staff proposed recommendations for enhancements to the security inspection program that include options to improve the efficiency of the FOF inspection program.

FOF inspection team members continue to provide the necessary monitoring of information to assist the mock adversary force in defining and developing mission plans used during FOF inspections. U.S. Special Operations Command members also support the NRC inspection team in the tactical planning of FOF inspections. 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 one in which the licensee demonstrates 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. An indeterminate exercise is one 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 one 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 before the adversary simulated the loss of target set elements. An ineffective exercise is one 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.

By the end of 2017, the NRC had completed the first year of the fifth 3-year cycle of FOF inspections. Between January 1, 2017, and December 31, 2017, the NRC conducted 19 FOF inspections (at 19 commercial power reactors but no CAT I fuel cycle facilities) and identified 9 findings that related to areas of the security baseline inspection program. Table 1 summarizes the 19 FOF inspections conducted in CY 2017.

Table 1: Calendar Year 2017 Force-on-Force Inspection Program Summary

19	Total number of inspections conducted (two exercises per inspection)
34	Total number of effective exercises
0	Total number of indeterminate exercises
3	Total number of marginal exercises
1	Total number of ineffective exercises
0	Total number of canceled exercises
9	Total number of inspection findings
9	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 2017, 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. Three exercises in CY 2017 were determined to be marginal because the licensees neutralized the adversary at a location, or in preparation to enter a location, that contained a single element target set. In all these cases, the licensees took appropriate corrective actions.

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 observed corrective actions applied in each of these categories during 2017.

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. The 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 103 out of 106 baseline security findings issued in CY 2017 were of very low security significance (i.e., Green or SL IV violations).

Table 2: Calendar Year 2017 Security Inspection Summary for Commercial Nuclear Power Reactors (without Force-on-Force)

215	Total number of security inspections conducted
106	Total number of inspection findings
98	Total number of Green findings
3	Total number of greater-than-Green findings
5	Total number of SL IV violations
0	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: BWX Technologies, Inc., located in Lynchburg, VA, and Nuclear Fuel Services, Inc., located in Erwin, TN. 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 is licensed to use and process a formula quantity of SSNM. The SSNM must be protected against acts of radiological sabotage, theft, and diversion. 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, MD, and Atlanta, GA, respectively, 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 HEU-related physical security areas to be inspected either annually, biennially, or triennially. The HEU physical security areas include access authorization, access controls, contingency response, equipment performance, fitness for duty, material controls, protection of sensitive and classified information, target area reviews, and security training. The core inspection program also requires two MC&A inspections annually and a transportation security inspection once every 3 years.

The core inspection program includes 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 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. As previously stated, there were no FOF inspections conducted at CAT I fuel cycle facilities in CY 2017.

**Table 3: Calendar Year 2017 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
4	Total number of SL IV violations
0	Total number of greater-than-SL IV violations

6. SECURITY INSPECTION PROGRAM RESULTS FOR CALENDAR YEAR 2017

6.1 Overview

In CY 2017, the NRC conducted 230 security inspections at operating commercial power reactors and CAT I fuel cycle facilities, including FOF inspections. Those inspections resulted in a total of 110 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 107 out of 110 security inspection findings issued in CY 2017 were of very low security significance (i.e., Green or SL IV violations). Figure 4 provides a graphic summary of the CY 2017 security inspection findings. This information gives an overview of licensee performance within the security cornerstone. The SGI version of this report (Enclosure 2) contains detailed discussions on each finding.

Table 4: Calendar Year 2017 Security Inspection Program Summary

230	Total number of security inspections conducted
110	Total number of inspection findings
98	Total number of Green findings
3	Total number of greater-than-Green findings
9	Total number of SL IV violations
0	Total number of greater-than-SL IV violations

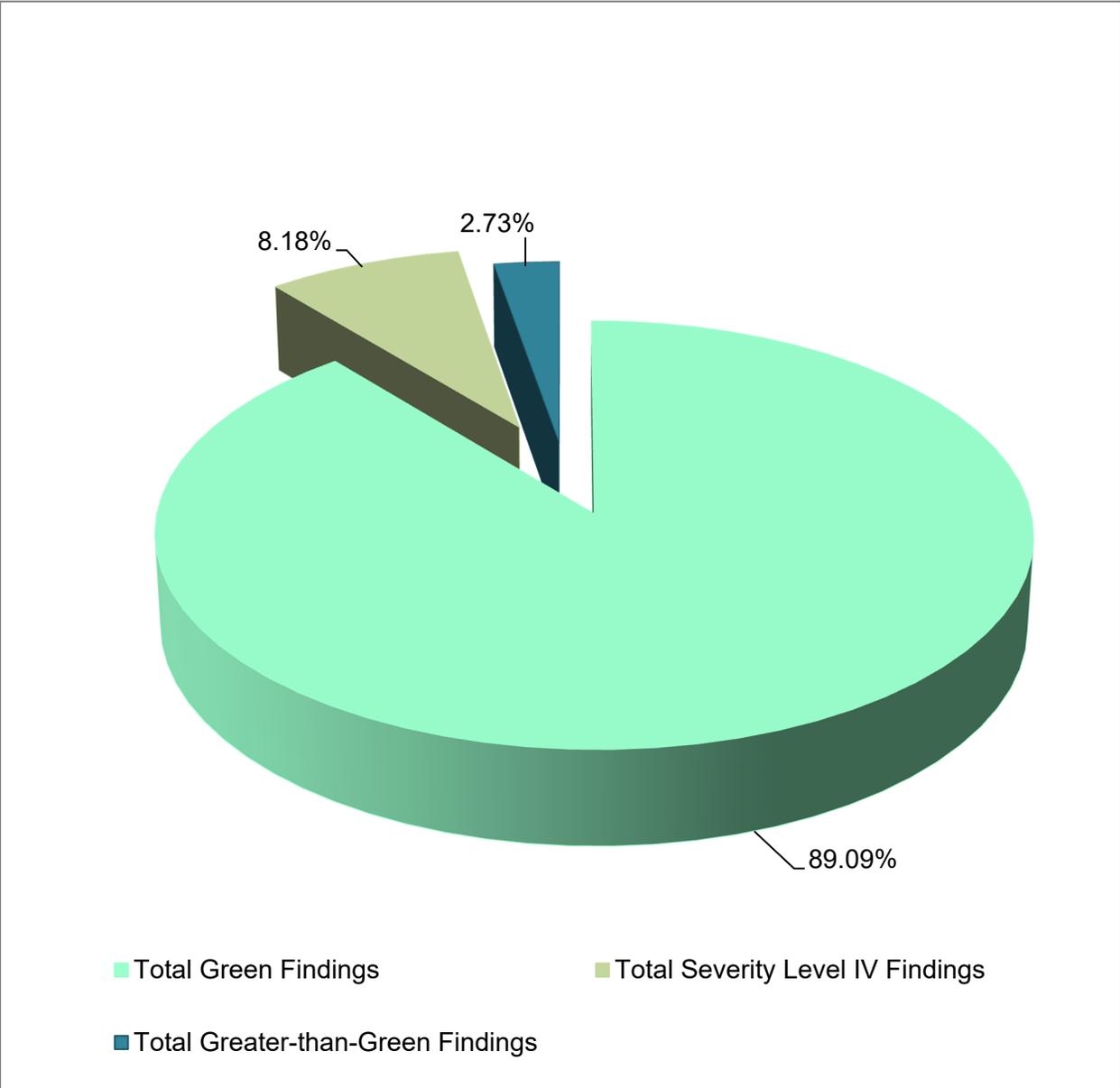


Figure 4: Summary of Security Inspection Program Results for Calendar Year 2017