POLICY ISSUE
(Notation Vote)

February 3, 2026 SECY-26-0015

FOR: The Commissioners

FROM: Michael F. King
Executive Director for Operations

SUBJECT: RECOMMENDATIONS FOR REVISING THE SECURITY BASELINE INSPECTION PROGRAM INCLUDING THE FORCE-ON-FORCE INSPECTION PROGRAM

PURPOSE:

The purpose of this paper is to seek Commission approval to pursue key revisions to the U.S. Nuclear Regulatory Commission (NRC) security baseline inspection program, including the Force-on-Force (FOF) inspection program, based on stakeholder feedback and consistent with the goals established by Executive Order (EO) 14300, "Ordering the Reform of the Nuclear Regulatory Commission," issued on May 23, 2025. This paper is presented in conjunction with notation vote paper, "Recommendations to Revise the Reactor Oversight Process Baseline Inspection Program," and provides the staff's recommendation for modifying the security inspection program to improve efficiency and effectiveness and reduce unnecessary regulatory burden.

This paper also presents Commission notification items related to the FOF inspection program, including staff actions to implement a scoring methodology that bounds the complexity of exercise scenarios and to modify performance testing of tactics that are impractical to simulate and may lead to unfair engagement opportunities.

CONTACTS: Jeff Bream, NSIR/DSO/SOSB
301-415-0256

Becca Lagios, NSIR/DPR/OB
301-415-3301

Cliff Roundtree, NSIR/DSO/SPEB
301-287-3602

This SECY Paper, with the exception of enclosure 1, will be released to the public in **10** working days.

Some of the items discussed in this paper for Commission approval apply exclusively to the operating reactor inspection program and do not extend to the Category I fuel cycle inspection program. This distinction exists because oversight of fuel cycle facilities is independent of the Reactor Oversight Process (ROP), and thereby not subject to the significance determination process.

Additionally, these facilities defend against different design basis threats (DBTs) (i.e., Category I fuel cycle facilities defend against the DBT of theft or diversion of special nuclear material whereas operating power reactors defend against the DBT of radiological sabotage). Nevertheless, the staff is committed to pursuing the items approved by the Commission identified in this paper, including those provided for awareness, as potential changes to the oversight of Category I fuel cycle facilities, where appropriate. The staff will advance these changes through coordination with the Category I fuel cycle facilities and Naval Reactors and will keep the Commission fully informed of any modifications to the Category I fuel cycle inspection program.

SUMMARY:

This paper presents the staff's recommendations for revising the security baseline inspections within the Reactor Oversight Process (ROP). If approved, these recommendations, together with the ROP revisions previously outlined to the Commission in SECY-25-0045, "*Recommendations for Revising the Reactor Oversight Process*," (ML25127A212) would reduce direct inspection hours necessary to complete the security baseline inspection program by about 50 percent compared to current levels. Grounded in over 25 years of experience and lessons learned, the recommendations align with the NRC's commitment to being a modern, risk-informed, and performance-based regulator and complement other ongoing agency initiatives responding to the ADVANCE Act and EO 14300. These changes will maintain effective oversight of operating reactor security while improving program reliability and efficiency. In accordance with Management Directive (MD) 8.13, this paper includes proposed changes requiring Commission approval.

The staff also developed two revisions to the FOF program that require Commission notification: (1) Develop and implement a scenario scoring methodology[1] with a threshold to bound the total number of DBT attributes that could be employed against a licensee's contingency response; and (2) Implement modifications to performance testing of certain tactics (e.g., unattended openings, etc.) and instead use a risk-informed approach. The details involving these notification items are presented later in this paper.

Changes Requiring Commission Approval

The staff seeks Commission approval to revise the ROP security baseline inspection program as follows:

1. Retire eight of the existing 11 security inspection procedures (IPs) with an associated staff action that would transfer their risk-significant elements into two newly created IPs.
2. Retain and modify the periodicity of the material control and accounting procedure from

[1] The scoring methodology is being developed by industry stakeholders and will be evaluated by staff prior to endorsement and implementation.

triennial to "as-needed" with clear criteria for implementation based on licensee performance. Additionally, enhance the cybersecurity IP based on lessons learned from initial cycle performance including shifting periodicity from biennial to triennial.

3. Revise the FOF IP to include two exercises, an update to the method for characterizing exercise outcomes, and an option to increase the licensee's role in exercise scenario development.

On October 21, 2025, staff submitted SECY-25-0087, *"Recommended Revisions to the Baseline Security Significance Determination Process"* (ML25168A179), which requires Commission approval. Additionally, on June 5, 2025, the staff submitted SECY-25-0045 on proposed revisions to the ROP based on the assessment conducted as part of Section 507 of the ADVANCE Act which the Commission approved on January 26, 2026. In parallel with this paper, staff is submitting a separate notation vote paper proposing revisions to the ROP inspection program for the other cornerstones outside of security. The approved changes in SECY-25-0045, the recommendations in SECY-25-0087, and the parallel ROP program paper (ML25247A048) are not dependent on the recommendations in this SECY (and vice versa).

BACKGROUND:

The current baseline security inspection program for operating power reactors consists of 11 inspection procedures performed by trained and qualified inspectors in physical security, cybersecurity, plant operations, and protection of special nuclear material. The program has remained largely consistent since the revised 10 CFR 73.55 security rule became effective in 2010. While moderate revisions have been made over time to adjust inspection focus or in response to industry events, most changes have been iterative, such as adjusting inspection periodicity or consolidating similar inspection elements into common procedures. Currently, the security oversight program includes six triennial IPs, three biennial IPs, and two annual IPs. Collectively, these 11 IPs cover the physical security inspectable areas, which encompass access authorization and control, equipment maintenance and testing, fitness for duty program, armed response capabilities and training, contingency planning, control of special nuclear material, and associated cyber security measures. Through these inspections, the NRC ensures that licensee security programs are effectively implemented and compliant with regulatory requirements, thereby maintaining robust protection against potential threats.

A key element of the NRC's baseline security inspection program is the FOF inspection program which the NRC conducts in accordance with Section 170D of the Atomic Energy Act of 1954,[2] which was promulgated as part of the Energy Policy Act of 2005. Section 170D requires, in part:

> Not less often than once every 3 years, the Commission shall conduct security evaluations … [that] include force-on-force exercises. The force-on-force exercises shall, to the maximum extent practicable, simulate security threats in accordance with any design basis threat applicable to a facility. In conducting a security evaluation, the Commission shall mitigate any potential conflict of interest that could influence the results of a force-on-force exercise, as the Commission determines to be necessary and appropriate.

The NRC's current FOF program has evolved since it was relaunched in November 2004 in response to internal and external feedback, the maturity of the NRC's inspection program,

[2] Section 170D of the Atomic Energy Act of 1954: https://www.govinfo.gov/link/uscode/42/2210d

licensees' security strategies, and observed licensee performance. In alignment with EO 14300 and based on external stakeholder feedback, the staff assessed the current FOF program and developed recommendations for modifications, while ensuring mitigation of any potential conflicts of interest that could influence exercise outcomes.

Since 2004, the FOF program has undergone multiple revisions to incorporate new inspection guidance, lessons learned, and Commission direction. The most significant changes have involved the number of NRC-led FOF exercises, and the treatment of violations associated with exercise outcomes. Most recently, in SRM-COMSECY-19-0006, "*Revised Security Inspection Program Framework (Option 3) in Response to SRM-SECY-17-0100*" (ML24138A045), the Commission approved a staff proposal to reduce the number of NRC-led exercises from two to one per site with one enhanced observation of a licensee FOF exercise per triennial cycle. The staff outlined its implementation plan in a note to Commissioner's Assistants dated September 4, 2024 (ML24193A257). While the staff has implemented the revised security inspection program framework (Option 3) in response to the SRM-COMSECY-19-0006 on January 1, 2026, the staff is presenting an alternative proposal to the Commission to further refine the FOF inspection program to better align with the broader oversight program changes being developed in response to EO 14300, Section 5.g.

DISCUSSION:

The staff analyzed the baseline security inspection program to identify opportunities to improve efficiency, enhance effectiveness and reduce regulatory burden. The staff found that the existing program primarily focuses on verifying compliance with discrete regulatory requirements rather than assessing overall security risk-significant licensee activities. To address this, the staff recommends replacing the existing IPs with new inspections that emphasize observations of licensee security performance and concentrate on risk-significant licensee activities and programs. This analysis was conducted alongside a broader review of the entire ROP and historical industry performance over the program's 25-year history. The broader analysis and supporting data are provided in the companion paper (ML25247A048) that outlines proposed modifications to baseline inspection programs for the cornerstones other than security. To maintain conciseness, this document does not repeat that data.

When developing the inspection program changes described in this paper, the staff based its recommendations on several key assumptions. First, the NRC will maintain the current inspectable areas in the baseline security inspection program, as these areas collectively provide comprehensive coverage of critical security functions, including access controls, response capabilities, and contingency planning. Preserving these areas ensures that the program continues to address the full spectrum of security performance elements without introducing gaps in oversight. Second, the NRC will ensure at least an annual touch point for physical security to promote predictable use of NRC and licensee resources by reducing periods of concentrated inspection activity that can strain staffing, training schedules, and operational planning. Based on the staff's experience, annual touch points allow both the NRC and licensees to allocate personnel and logistical support more efficiently, minimizing disruptions to normal operations while sustaining oversight effectiveness.

For the FOF portions of the program, the staff considered several factors to ensure effectiveness and efficiency. Because the FOF exercises serve as a cornerstone of the protective strategy element of the NRC's oversight program, the staff sought to retain fundamental tenets of the program, including maintaining adversary performance standards and robust simulation capabilities, consistent application of performance-based scenarios, and alignment with the Commission's expectations for realistic threat representation. Additionally, the staff sought to balance the resource intensity of FOF inspections with the need for meaningful performance insights. As a result, the staff determined that the most efficient approach to revising the FOF program is to leverage efficiencies in exercise planning to reduce resource burden and incorporate best practices from other agencies to better risk-inform the program and ensure consistency in implementation.

The staff also determined that the inspection program should eliminate the observation of a licensee-conducted exercise and instead conduct two exercises during the triennial FOF IP. This approach aligns generally with Commission direction in SRM-COMSECY-19-0006 which called for one NRC-conducted FOF exercise and one enhanced NRC observation of a licensee-conducted exercise; however, the revised approach reduces redundancy by combining common activities into a single visit rather than two separate visits. The staff considers the current sample size of two exercises optimal because it provides a more comprehensive view of overall program performance. A single exercise may conclude quickly or involve a narrow attack vector, offering limited engagement for most security force participants. Conducting two exercises in one inspection also optimizes the use of resources that are already onsite for exercise conduct (e.g., MILES gear, mock adversary force participants, SOCOM advisors, and licensee resources). The shift back to two exercises is accompanied by other proposed improvements to mirror aspects of the emergency preparedness exercise program and NRC operator licensing examination framework, including evaluation of licensee developed scenarios and an emphasis on licensee identification of deficiencies.

COMMISSION APPROVAL ITEMS:

Retire and Replace Identified Baseline Security Inspection Procedures

The staff recommends retiring the following IPs and consolidating their risk-significant attributes and requirements into new IPs:

- IP 71130.01, "Access Authorization"
- IP 71130.02, "Access Control"
- IP 71103.04, "Equipment Performance, Testing, and Maintenance"
- IP 71130.05, "Protective Strategy Evaluation and Performance Evaluation Program"
- IP 71130.07, "Security Training"
- IP 71130.08, "Fitness-for-Duty Program"
- IP 71130.09, "Security Plan Changes"
- IP 71130.14, "Review of Power Reactor Target Sets"

The staff identified risk-significant inspection activities within these procedures and developed new procedures, described below, to minimize redundancy, optimize resource utilization, and prioritize inspector observations of licensee performance. The proposed IPs would reduce inspection travel costs, balance direct inspection effort across the inspection cycle, leverage resident inspector flexibility, and maintain risk-significant inspection by physical security inspectors with subject matter expertise.

In place of the eight retired IPs, the staff recommends implementing two new IPs described below:

- IP 71130.15, "Security Operations"

  Under this new annual IP, site resident inspectors will observe licensee security operations and equipment to verify compliance with regulatory requirements, the physical security plan, and implementing procedures. This IP will focus on daily security operations, the material condition of security systems, staffing levels, and the resolution of identified security deficiencies. This is consistent with the broader ROP initiative to capitalize on resident inspector expertise by shifting select inspection effort for areas that fit within their existing scope and responsibilities. A limited amount of training will be required to ensure resident inspectors can effectively implement this IP. This training will be scheduled and conducted if the Commission approves the proposal.

- IP 71130.16, "Security Performance"

  Under this new annual IP, regional security inspectors will verify that licensee performance complies with regulatory requirements, the physical security plan, and implementing procedures. Inspectors will select samples based on licensee activities and performance from the following areas: access control, physical security program, equipment testing and maintenance, security training, target sets, access authorization, fitness for duty, and security plan changes. This IP is predominately comprised of risk-significant aspects of the current IPs while allowing regional offices to tailor security inspection activities to individual site performance.

The staff has designed these new procedures to ensure adequate coverage of the risk-significant elements of the physical protection program by focusing on defense-in-depth principles that safeguard against the DBT of radiological sabotage. This approach will emphasize inspection activities that verify the effectiveness of security systems and personnel reliability programs, while testing critical capabilities such as intrusion detection, alarm response, access control, and contingency actions. By aligning with the objectives of the Physical Protection cornerstone, the procedures will provide assurance that licensees maintain robust security measures to protect public health and safety.

Retained but Modified Inspection Procedures

The staff recommends retaining the following two IPs but modifying them to maximize effectiveness.

- IP 71130.11, "Material Control and Accounting (MC&A)"

  The staff identified that this IP could be revised to an "as needed," procedure that would only be implemented if predefined criteria associated with special nuclear material handling or fuel reconstitution activities are identified. The contents of this IP would be transferred to a new procedure in IMC 2201, "Security Inspection Program for Operating Commercial Nuclear Power Reactors," Appendix C, "Generic, Special, and Infrequent Inspections." The basis for this change is that the historic events that led to the development of this IP no longer reflect current licensee performance based on a review of licensee performance history from the last 10 years.

- IP 71130.10, "Cybersecurity"

Under this proposal, IP 71130.10, "Cybersecurity," would be retained but updated. As noted in SECY-25-0045, the periodicity of this IP would be revised from biennial to triennial. Historically, inspections of licensee cybersecurity programs have produced many findings, as would be expected during initial implementation of a relatively new requirement. Now that initial inspections have been completed, the staff assessed that licensees have demonstrated greater compliance and that cybersecurity can be adequately evaluated on a triennial basis.

Additionally, the staff is revising the inspection requirements to update sample selection guidance using risk-informed principles and consequence assessments. The inspection would also reduce reliance on subject matter expert (SME) contractors to one per inspection. The staff recommends a long-term oversight strategy that includes evaluating further reduction in the SME contractor support and transitioning inspection support functions in-house by the start of the next triennial inspection cycle in 2029.

Revise and Enhance the FOF Inspection Program

The staff recommends the current FOF IP (71130.03) be retained but renumbered as IP 71130.17 and modified in three ways. First, the staff recommends that the FOF inspection program be modified so it consists of a single triennial inspection that includes two FOF exercises. In providing this recommendation, the staff recognizes that in SRM-SECY-17-0100, "*Security Baseline Inspection Program Assessment Results and Recommendations for Program Efficiencies*," dated October 9, 2018 (ML18283A072), the Commission directed the staff to submit for approval a revised security inspection framework that would modify the NRC FOF inspection program to include one NRC FOF exercise and an enhanced NRC inspection of a licensee annual FOF exercise. The staff submitted this revised framework in COMSECY-19-0006, "*Revised Security Inspection Program Framework (Option 3) in Response to SRM-SECY-17-0100*," dated May 21, 2019 (ML19038A485). The Commission approved the revised FOF inspection program on May 17, 2024, and the staff implemented the revised procedure on January 1, 2026, to coincide with the start of the 8th triennial FOF cycle.
While the staff has implemented the revised security inspection program framework (Option 3) in response to the SRM-COMSECY-19-0006, the staff is presenting this alternative proposal to the Commission to further refine the FOF inspection program to better align with the broader oversight program changes being developed in response to EO 14300, Section 5.g. Specifically, this recommendation combines two triennial inspections focused on protective strategy evaluation into one activity to improve efficiency, optimize resource use, and reduce costs while maintaining sample size consistency and enhancing opportunities to observe security program performance through multiple exercises.

The current sample size of two exercises is considered optimal because single exercises may conclude quickly, provide limited engagement for most security force participants, or test only a narrow attack vector. The staff believes that preserving two exercises ensures that the NRC can fully assess the licensee's implementation of its protective strategy by providing the staff with two separate opportunities to observe the licensee's response to diverse exercise scenarios. Conversely, a single exercise would limit the NRC's ability to assess the protective strategy by limiting the observations of the licensee's response and potentially overemphasize the impact of artificialities and simulations that could limit the opportunity for meaningful observations. Additionally, this option significantly reduces the potential for reinspection, which, in a single exercise framework, would be necessary if problems arose during the exercise that prevented the NRC from evaluating the licensee's ability to defend against the DBT, as required by Section 170D of the AEA.

Second, the staff proposes changing how exercise outcomes are characterized. Currently, licensee performance is labeled *effective*, *ineffective*, or *indeterminate* based on the inspection team leader's ability to reliably determine the outcome of the FOF exercise results. An ineffective exercise is treated as a failure of the protective strategy, resulting in a performance deficiency and a very low safety significance (Green) finding under the NRC significance determination process (SDP). Licensees must enter these findings into their problem identification and resolution (PI&R) programs for corrective action. Under the proposal, ineffective exercises would no longer be considered performance deficiencies or SDP findings on their own but other deficiencies would still be assessed as appropriate through the inspection program. Deficiencies in licensee performance during FOF exercises would continue to be addressed through the licensee PI&R programs per 10 CFR Part 73, Appendix B, with the NRC reviewing corrective actions during routine baseline inspections.

This approach acknowledges that exercise artificialities, such as simulations and time-outs, can skew performance. The NRC would still evaluate licensee performance and document results for follow-up through normal inspection sampling of the licensee's corrective actions, but without issuing violations. The staff also proposes eliminating "effective" and "ineffective" terminology, which has fostered a "win or lose" mindset and disputes over scenario planning. Removing these terms would shift the inspection emphasis to overall readiness, continuous learning, and the correction of weaknesses identified during FOF exercises, further refocusing licensee physical security programs on the identification and correction of observed deficiencies. This change slightly reduces documentation (~2 hours per case) and requires revising the format of the annual Report to Congress on the Security Inspection Program, as formal outcome determinations would no longer be made.

Third, the staff is proposing a change to how FOF exercises are developed by allowing licensees to have an increased role in scenario development, at the option of the licensee. Under this proposal, if selected by the licensee, the NRC would identify target sets and attack vectors, and select the DBT attributes to evaluate physical protection program elements; the licensee would then use these inputs to develop the exercise scenario, a detailed mission narrative, and the exercise controller matrix. The licensee-developed exercise would be subject to NRC review and approval to maintain the ability to mitigate any potential conflicts of interest that could influence the results of the exercise (see Enclosure 2).

The staff developed this proposal to more closely align with the NRC oversight approach for licensee emergency preparedness programs. Specifically, the recommendations mirror aspects of the emergency preparedness exercise program, including licensee development of exercise scenarios and an emphasis on licensee identification of deficiencies. Additionally, providing optionality regarding scenario planning mirrors the NRC operator licensing examination framework by providing optimal flexibility should licensees prefer to play an increased role in scenario development. The staff anticipates most, if not all, operating reactor licensees would opt for an increased role in exercise development. However, the NRC would continue to perform exercise development, similar to the current methodology, if licensees do not take advantage of this option.

Revised Inspection Framework Resource Estimates

The proposed revisions to the ROP security baseline inspection program aim to eliminate redundant activities and optimize resource allocation based on licensee performance, reducing implementation effort by 41–48%. To assist in evaluating the proposal, the staff has provided an "at-a-glance" comparison of the current and proposed security inspection program.

Current Baseline Security Inspection Program

Procedure Number	Freq	Title	Minimum Samples	Minimum Hours Annualized	Nominal Samples	Nominal Hours	Nominal Hours Annualized
71130.01	T	Access Authorization	1	6	1	24	8
71130.02	A	Access Control	1	20	1	28	28
71130.03	T	Contingency Response – Force-on-Force Testing	1	92	1	393	131
71130.04	B	Equipment Performance, Testing, & Maintenance	1	15	1	39	18
71130.05	T	Protective Strategy Evaluation and Performance Evaluation Program	2	23	2	90	30
71130.07	B	Security Training	1	10	1	27	14
71130.08	T	Fitness-For-Duty Program	1	5	1	24	8
71130.09	A	Security Plan Changes	1	6	1	7	7
71130.10	B	Cybersecurity	1	31	1	70	35
71130.11	T	Material Control and Accounting	1	5	1	15	5
71130.14	T	Review of Power Reactor Target Sets	1	3	1	9	3
						ANNUALIZED TOTAL	**287**

Proposed Baseline Security Inspection Program

Procedure Number	Freq	Title	Minimum Samples	Minimum Procedure Hours	New Min Hours (Annualized)
71130.10	T	Cybersecurity	3	63	21
71130.15	A	Security Operations (Resident Inspectors)	6	16	16
71130.16	A	Security Performance (Regional Inspectors)	4	64	64
71130.17	T	Force-on-Force Exercise	1	144-208	48 - 69
				ANNUALIZED TOTAL	**149 – 170**

The resource estimate for the FOF inspection reflects the potential range for licensee-developed exercises or NRC-developed exercises. Specifically, if the licensee opts to develop the exercise scenarios, the staff estimates one Team lead and one inspector for 2 days to approve the scenarios (32 hours). Conversely, if the licensee opts for the NRC to develop the scenarios, the staff estimates one Team Leader and three inspectors for 3 days to develop and approve the scenarios (96 hours). Both options would include one Team Leader and three inspectors for 3.5 days to evaluate the exercises performance (112 hours) for a total of 144 hours and 208 hours respectively. Both estimates would be reduced by approximately 32 hours (one Team lead and three inspectors for 1 day) if the NRC only performs one FOF exercise.

Staff Assessment of Pros and Cons

The staff has identified the following common pros and cons across each inspectable area discussed in this paper.

Pros:

- Enhances inspection flexibility by consolidating multiple annual, biennial, and triennial inspections into a single activity, improving efficiency and aligning with other ROP changes.
- Reduces travel costs in response to ADVANCE Act directives by leveling direct inspection activities across the inspection cycle.
- Acknowledges licensee performance improvements in areas such as cybersecurity and MC&A, while retaining the ability to inspect special nuclear material controls when necessary.
- Streamlines FOF inspections by significantly reducing direct inspection effort during the current planning week.
- Increases licensee engagement in FOF exercise development by allowing planning responsibilities to shift from the NRC and mock adversary force director to the licensee. Increased involvement may encourage licensees to explore repeatable and predictable conditions not traditionally tested.
- Eliminates issuance of formal findings based on FOF outcome results which will help shift the historical "win/lose" culture surrounding FOF exercises toward a focus on identification and correction of performance issues.
- Optimizes FOF resource utilization by maximizing use of exercise assets (e.g., MILES gear, CAF team resources) and reducing NRC travel costs.
- Maintains FOF exercise sample size consistency with SRM-COMSECY-19-0006 while improving efficiency. The current sample size of two exercises enhances the ability to observe overall program performance.
- Supports contingency planning to complete inspections without additional travel when issues arise, such as weaknesses identified in the first exercise, cancellations due to weather, or artificialities limiting insights.

Cons:

- May reduce the ability to identify areas of noncompliance in lower-risk areas, though this aligns with a risk-informed approach that prioritizes higher-significance issues.
- Increased flexibility could result in some areas not being inspected at regular intervals, which differs from the current program's structured schedule.
- As cybersecurity becomes increasingly important with digital upgrades, this option could delay NRC identification of deficiencies if not self-identified by licensees, emphasizing the need for strong licensee programs.
- Could lead to variability across the industry in the quality of licensee-developed FOF exercise scenarios, creating a new escalation path between the NRC and licensees during the development of scenarios. This would require new guidance, training, and external engagement to ensure consistency.
- May create a perception that NRC oversight is less direct because licensees would have a greater role in the design of their own testing, requiring clear communication to address concerns about independence and conflict of interest.

- Could be perceived as reducing licensee accountability for correcting deficiencies identified during exercises, since violations would not be issued for exercise outcomes.

Industry Engagement and Feedback

In developing the recommendations in this paper, the staff sought input from external stakeholders through closed public meetings and also reviewed a letter from the Nuclear Energy Institute (NEI) and its members on September 2, 2025 (ML25245A250). Overall, the nuclear industry expressed mixed perspectives on the changes outlined in this paper. Stakeholders generally supported staff recommendations to consolidate the inspection program but noted concerns that incorporating maximum flexibility into the program design could create challenges in preparing for NRC inspections.

Industry representatives also supported proposals to allow licensee participation in FOF scenario planning and to remove the FOF program from the SDP, stating that *"this promotes a more constructive oversight model—one that emphasizes improvements to protective strategies rather than 'pass/fail' outcomes—and better aligns with the program's safety and security objectives."*

Several stakeholders questioned the need for additional oversight, observing that the current security baseline inspection program, consisting of a single FOF exercise and one NRC observation of a licensee-conducted exercise, already provides sufficient opportunities for the NRC to evaluate protective strategies. Some feedback referenced the Commission's direction in SRM-COMSECY-19-0006, describing the staff proposal as a potential regression and an increase in oversight. However, when considering broader changes to the baseline security program, some stakeholders indicated a preference for conducting two exercises during a single inspection for efficiency, rather than the current approach of separating exercises across two inspections.

COMMISSION NOTIFICATION ITEMS:

Development of a Scoring Methodology

The staff plans to evaluate an industry-developed scoring methodology, similar to the DOE FOF program, that sets a maximum threshold to ensure sufficiently challenging, yet realistic scenarios while also limiting the number of DBT attributes used against a licensee's contingency response. This approach ensures scenarios remain challenging yet reasonable for a private security force to defend against. The Security Policy Verification Committee working group[3] recommended using an NRC-specific version of DOE's Graded Adversary Scenario Scoring Matrix (GASSM), modified to reflect differences in DBT attributes between the agencies. This change would prevent overly complex scenarios while continuing to simulate DBT tactics, techniques, and characteristics to the maximum extent practicable.

This approach leverages intelligence-based insights to focus on the most probable attributes, reducing artificialities and improving realism. While the change will require additional NRC

[3] The Security Policy Verification Committee is a joint committee between NNSA, Department of Defense and the NRC that focuses on coordination and collaboration on nuclear security matters across the enterprise. The SPVC includes 9 working groups covering issues from uncrewed systems to vulnerability risk management. See Enclosure 2 for more information.

resources to address implementation challenges and could create a perception that exercises do not test the full DBT, the overall resource burden is expected to decrease as experience grows. The nuclear industry supports this change, noting that a structured scoring methodology will enhance efficiency, promote consistency, and ensure realism in future inspections. NEI plans to submit a proposed methodology in February 2026.

Implement Changes to Performance Testing Certain Tactics

The staff plans to adopt a risk-informed approach in place of performance-based testing for certain tactics that are difficult to accurately simulate and do not provide fair engagement opportunities, making it challenging to assess whether they represent credible threat vectors. For example, unattended openings, narrow pathways intersecting a security boundary, often create unrealistic simulations and unfair engagement conditions. This adjustment reflects lessons learned throughout the history of the FOF program. While this change would lead to some tactics no longer being performance tested, potentially creating a perception that not all DBT attributes are evaluated, FOF exercises will continue to simulate the DBT to the maximum extent practicable, and other security baseline inspections will be used to assess pathways and viable tactics for potential vulnerabilities.

This approach aligns with the NRC's vision of being a modern, risk-informed regulator by allowing staff to accept well-managed risks without compromising the agency's mission. It also improves inspection efficiency by reducing time spent developing and testing unrealistic simulations. The nuclear industry supports this change, noting that these tactics have historically challenged exercise realism, led to indeterminate outcomes, and required significant resources to simulate and test.

COMMITMENT:

Based on directions received from the Commission, the staff will engage external stakeholders in the development of any new guidance documents. Additionally, the staff will develop an implementation schedule with consideration for mid-inspection cycle implementation for these options. The staff will notify the Commission prior to implementation consistent with Management Directive 8.13, "Reactor Oversight Process."

RECOMMENDATION:

The staff recommends that the Commission approve the revised security baseline inspection program and associated guidance as described in this paper including:

1. Retire eight of the existing 11 security IPs with an associated staff action that would transfer their risk-significant elements into two newly created IPs.

2. Retain and modify the periodicity of the material control and accounting procedure from triennial to "as-needed" with clear criteria for implementation based on licensee performance. Additionally, enhance the cybersecurity IP based on lessons learned from initial cycle performance including shifting periodicity from biennial to triennial.

3. Revise the FOF IP to include two exercises, an update to the method of characterizing exercise outcomes, and an option to increase the licensee's role in exercise scenario development.

RESOURCES:

The recommendations presented in this paper will result in an overall reduction in the current level of inspection effort. Additional staff resources will be needed to develop the revised FOF IP and implementation guidance. Enclosure 1 provides the resource and timing impacts.

Partial resources for IP and guidance development, for fiscal year (FY) 2026 are included in the FY 2026 President's Budget. If the Commission directs the staff to begin work in FY 2026, resources would be reallocated from lower-priority work. Resources for FY 2028 and beyond will be addressed through the planning, budgeting, and performance management process.

COORDINATION:

The Office of the General Counsel reviewed this package and has no legal objection. The Office of the Chief Financial Officer reviewed this package for resource implications and has no objections.

Michael F. King
Executive Director
for Operations

Enclosures:
1. Estimated Resources (OUO-SII)
Non-Public
2. Additional Background on FOF
Program

<u>SUBJECT</u>: RECOMMENDATIONS FOR REVISING THE SECURITY BASELINE INSPECTION PROGRAM INCLUDING THE FORCE-ON-FORCE INSPECTION PROGRAM DATED: February 3, 2026

ADAMS Accession Numbers: ML25279A191 Pkg; ML25279A192 SECY; ML25279A193 Encl. 1; ML26028A054 Encl. 2

OFFICE	NSIR/DSO	NSIR/DSO	NSIR/DSO	NSIR/DSO	NSIR/DSO
NAME	RLagios	CRoundtree	JBream	JClark	CPantalo
DATE	10/7/25	10/8/25	10/7/25	10/8/25	10/8/25
OFFICE	NSIR/DSO	NSIR	OCFO	OGC	EDO
NAME	TBowers	KWilliams	CCarroll	DTaggart	MKing
DATE	10/15/25	11/5/2025	1/30/2026	1/30/2026	2/3/2026

OFFICIAL RECORD COPY