POLICY ISSUE
(Notation Vote)

October 21, 2025 SECY-25-0087

FOR: The Commissioners

FROM: Michael F. King
Acting Executive Director for Operations

SUBJECT: RECOMMENDED REVISIONS TO THE BASELINE SECURITY SIGNIFICANCE DETERMINATION PROCESS

PURPOSE:

The purpose of this paper is to seek Commission approval to implement revisions to Inspection Manual Chapter (IMC) 0609, Appendix E, Part I, "Baseline Security Significance Determination Process (BSSDP) for Power Reactors," in order to reduce subjectivity, add risk insights, and promote consistency in security inspection findings. This paper provides a recommendation for specific revisions to the BSSDP for Commission approval consistent with Management Directive (MD) 8.13, "Reactor Oversight Process."

SUMMARY:

After seeking internal and external stakeholder feedback, staff from the Office of Nuclear Security and Incident Response identified an opportunity to improve U.S. Nuclear Regulatory Commission (NRC) security inspections by revising the BSSDP. The proposed BSSDP revisions would reduce the subjectivity of the existing tools, improve the consistency of inspection findings, and add new risk insights. Notably, the proposed revisions eliminate the current Significance Screen and BSSDP worksheet, which stakeholder feedback identified as potentially leading to subjective or inconsistent findings. New tables in the proposed BSSDP assess the likelihood an adversary would be able to identify and exploit deficiencies in licensee performance and the associated impact of a performance deficiency on the licensee's physical protection program.

CONTACT: Maury Brooks, NSIR/DSO
301-415-4064

BACKGROUND:

The current version of IMC 0609, Appendix E, Part I, also referred to as the BSSDP, is the assessment tool through which the NRC evaluates findings that impact the security cornerstone of the reactor oversight process (ROP). The BSSDP is used once a performance deficiency (PD) has been evaluated as more than minor using IMC 0612, Appendix B, "Issue Screening," and determined to be in the security cornerstone in accordance with IMC 0609, Attachment 4, "Initial Characterization of Findings." In the current BSSDP, NRC security inspectors apply several figures and tables to assess the significance of a given security inspection finding and to assign the appropriate corresponding significance level (i.e., green, white, yellow, or red).

IMC 0609, Appendix E, is divided into four parts with each part containing tools for the assessment of deficiencies pertaining to different program areas within the security cornerstone. Part I, "Baseline Security Significance Determination Process (BSSDP) for Power Reactors," is used to evaluate the significance of most physical protection findings in the security cornerstone. The current version of the BSSDP is split into six specific sections that contain the assessment tools that have been developed for physical protection findings:

- *Material control and accounting.* This section is used to determine the risk-significance of findings related to licensee protection, control, and accounting of special nuclear material.
- *Unsecured Safeguards Information.* This section is used to determine the risk-significance of findings related to licensee use, storage, and destruction of Safeguards Information.
- *Significance screen (Figure 4 in IMC 0609, Appendix E, Part I).* This is a process used to augment the BSSDP by using a set of selected events that share common characteristics and the impact on the physical protection program.
    - The majority of greater-than-green security findings are dispositioned through the significance screen.
- *Unattended openings.* This section is used to determine the risk-significance of findings related to licensee protection of unattended openings and underground pathways that bypass security barriers, such as the protected area barrier.
- *Target sets.* This section is used to determine the risk-significance of findings related to target sets, including target set processes, consideration of cyber-attacks, and target set oversight.
- *BSSDP worksheets (Figures 7-11 in IMC 0609, Appendix E, Part I).* These worksheets are used to determine the risk-significance of findings related to access authorization, access control, physical protection system, and contingency response by evaluating the impact areas, key attributes, and program elements impacted by the findings.

The NRC staff conducts an annual self-assessment of the ROP in accordance with IMC 0307, "Reactor Oversight Process Self-Assessment Program," dated May 3, 2022 (ML21341B399). In the annual self-assessments for calendar years 2022 and 2023, the staff committed to completing an assessment to determine whether any aspects of the BSSDP could be improved or clarified to promote a more consistent and less subjective application of the BSSDP. See SECY-23-0032, "Reactor Oversight Process Self-Assessment for Calendar Year 2022," dated April 7, 2023 (ML23026A346), and SECY-24-0030, "Reactor Oversight Process Self-Assessment for Calendar Year 2023," dated April 9, 2024 (ML24026A162).

In March of 2023, the staff solicited feedback on the current BSSDP from NRC security inspectors through an internal survey and discussions during annual security inspector counterpart meetings. Based on the results of this feedback, in September 2023, staff chartered a working group consisting of regional, technical training center, and headquarters staff under the leadership of an executive-level steering committee. The working group identified two phases of the project. The first phase focused on analyzing the results of surveys and feedback; identifying areas of perceived subjectivity and inconsistency within the BSSDP; and developing options to address the feedback and further risk-inform the BSSDP. The second phase involved developing any necessary revisions to the BSSDP identified in the first phase.

The staff held public meetings on March 20, 2024 (ML24099A216), June 24, 2024 (ML24191A380), December 18, 2024 (ML25014A205), and February 20, 2025 (ML25073A099), to solicit feedback from external stakeholders. In these public meetings, external stakeholders also highlighted concerns regarding complexity and subjectivity. The staff received additional recommendations from industry stakeholders to expand the existing significance screen to allow for inclusion of additional risk insights; to use the very low safety significance issue resolution (VLSSIR) process for issues that screen no greater than green; to distinguish between human and programmatic performance issues; and to establish a new process to focus on recurring, high-risk issues. Members of the public encouraged the NRC to ensure that any revisions still yield a robust screening tool to maintain public confidence that NRC-licensed facilities remain secure.

Using feedback from public meetings and NRC security inspectors, the working group developed recommendations to revise the BSSDP to improve guidance, reduce subjectivity and complexity, distinguish between human performance and programmatic performance issues, and improve risk-informed decision-making through objective risk determination.

The staff presented its revised BSSDP methodology during public meetings held on June 26, 2025 (ML25197A460), and July 14, 2025 (ML25198A310). The staff presented the likelihood of exploitability and impact to the physical protection program screening tools, described later in this paper, and solicited feedback. The staff also discussed examples of findings to provide practical demonstrations of the use of the proposed BSSDP and screening tools.

The staff noted multiple comments about the screening tools, including general support for the incorporation of human performance and programmatic considerations. The staff also noted concerns about an unintended apparent potential escalation path for findings related to access authorization. Comments were generally favorable, and concerns were addressed through additional staff review.

Many of the comments received and discussed during the public meetings were related to clarification and applicability of different conditions. Many of the questions were resolved through guidance that is contained in the proposed BSSDP. The staff revised the proposed BSSDP to address external stakeholder concerns, like the unintended escalation path, as necessary.

There were some aspects of stakeholder feedback that were not incorporated in the staff's proposal. Specifically, the working group noted that the VLSSIR process is already applicable to security related findings, which was further clarified in a May 2025 revision to IMC 0612, "Issue Screening." Therefore, the working group determined that no additional changes within the BSSDP effort are necessary to address industry recommendations related to VLSSIR. Additionally, the working group considered whether repetitive issues should be addressed in the

assessment of potential changes to the BSSDP. The working group determined that this approach would result in the aggregation of low risk-significance issues, which would be inappropriate. However, the working group determined that repetitive issues could be indicative of programmatic deficiencies, potentially increasing the focus on some recurring issues. High risk-significant issues already receive significant focus through the supplemental inspection program, so no additional changes are needed to address that part of the industry recommendation. The working group determined that focus on other repetitive issues can be accomplished, if appropriate, through the sample selection process of the baseline inspection program.

In accordance with MD 8.13, the staff must seek Commission approval for additions, deletions, or significant modifications to oversight processes, such as the significance determination process (SDP). The staff determined that the proposed changes to the BSSDP, based on the depth and scope of the changes and the extent of external stakeholder interest, represent a significant revision. Therefore, the staff is submitting this SECY paper for Commission review and approval.

DISCUSSION:

Summary of Historically Significant Findings that Informed BSSDP Revisions

Two significant findings occurred in 2022 that contributed to the determination that weaknesses in the BSSDP required the staff to initiate this revision. The first involved an unauthorized member of the public entering a site protected area (PA) through an unlocked door in a building that was adjacent to the PA. In this instance, the unauthorized individual was immediately detected, and site security initiated an appropriate response to the unauthorized intrusion.

Due to the subjectivity of the current BSSDP, significant differences in interpretation were identified amongst the staff for the appropriate risk factors to attribute to the performance deficiency. Some staff felt the guidance supported the attribution of tangential performance issues that compounded the performance deficiency, resulting in a finding of white significance. However, other staff felt the guidance was sufficiently vague such that only factors directly associated with the performance deficiency were appropriate, resulting in a finding of green significance.

Resolution of the differences in staff position resulted in significant internal effort and the expenditure of significant staff resources. The resulting green finding that was assessed for the licensee performance deficiency was disproportionate to the level of staff effort that was expended. The staff felt the differences in interpretation highlighted weaknesses in the current BSSPD that could not be easily resolved through implementation guidance changes.

Separately, the second significant finding involved an inspector-identified deficiency in the maintenance of a licensee's natural terrain vehicle barrier system such that a vehicle based improvised explosive device, in accordance with the design basis threat, could bypass the vehicle barrier. The initial determination assessed a finding of white significance.

Significant staff and licensee effort, including the use of contractor support, was expended in the assessment of the final risk significance of the finding. Other potential factors that could have mitigated the significance of the issue were not incorporated into the initial risk assessment process because there was no mechanism, at the time, to account for the difficulty in

identification of the performance deficiency or the level of direct impact to the licensee's physical protection program.

Similar to the first finding discussed, the resulting green finding that was assessed for the licensee performance deficiency was disproportionate to the level of staff and licensee effort that was expended. The staff felt that additional factors that directly contribute to the exploitability of performance deficiencies should be modeled in the assessment of risk significance; however, these factors are not readily part of the current BSSDP.

Previous revisions of the BSSDP corrected identified weaknesses in the process by focusing on implementation guidance or targeted edits to resolve specific deficiencies while leaving the structure and methodology of the BSSDP intact. While the final significance determination was correct for the above examples, the resources required to get to that determination illustrated to the staff that a different, holistic approach was necessary to improve the BSSDP's clarity and ability to yield repeatable, risk-informed significance determinations.

The proposed SDP, as described in the remainder of this paper, resolves the staff concerns associated with the current BSSDP. In both cases, the proposed SDP would significantly reduce the level of effort needed to assess the significance of similar findings and provide a more realistic assessment of risk that is based on exploitability and actual impact on the licensee's physical protection program. The proposed SDP design also aids staff in focusing on the licensee performance deficiency and the risk associated with the PD, rather than considering other circumstances that are outside the licensee's control.

Proposed Baseline Security Significance Determination Process Revisions

The staff developed a revised BSSDP framework that would eliminate the BSSDP worksheet and the significance screen. The staff concluded that the existing version of the BSSDP introduces subjectivity in assessing the significance of an identified PD by attributing the PD to individual inspection procedure elements that were not met. This process can overestimate the significance of a degraded condition and contribute to inconsistent significance determinations.

In place of the existing BSSDP worksheet and the significance screen, the staff developed a new flowchart and new assessment matrices (see Figure 6, Enclosure 1). The revised assessment methodology incorporates specific criteria with risk-informed principles. In the staff's proposed revision, PDs are assessed for significance based on the likelihood that a PD can be identified and exploited by an adversary and the potential impact to the physical protection program. For example, PDs that could only be identified by a high-level insider with direct access to the site were deemed less likely to be identified while items that could be observed by a general member of the public were deemed more likely to be identified. This provides credit for the licensee's insider mitigation program by acknowledging information protection and access controls.

The methodology also distinguishes between criteria related to human performance and programmatic issues. Human performance pertains to situations in which a PD would not have occurred if licensee staff had properly followed all relevant procedures, programs, and training. In contrast, programmatic issues are deficiencies embedded within the licensee's training, procedures, or operational processes. These types of PDs are considered predictable and identifiable because they can be detected through routine surveillance of licensee activities or by reviewing procedures, records, and documentation accessible to an insider. This distinction

is critical for accurately assessing the significance of PDs and implementing effective corrective actions.

In developing the revisions, the staff aimed to risk-inform the inspection program and integrate performance-based approaches, reinforcing the NRC commitment to effective and security-focused oversight. The staff's assessment was also consistent with direction in section 507 of the Accelerating Deployment of Versatile, Advanced Nuclear for Clean Energy Act of 2024 (ADVANCE Act) to maximize the efficiency of reactor oversight and inspection programs through appropriate use of risk-informed, performance-based procedures that focus on credible security risks. These efforts to modernize and streamline the SDP will enable more targeted and meaningful inspection follow-up and strengthen the agency's ability to prioritize issues that matter most to the NRC's safety and security mission.

While specific values could not be quantified, the staff has determined that the revised BSSDP will also lead to a reduction in staff effort to assess the significance of inspection findings. The current BSSDP requires staff to review multiple inspection procedures and figures within the BSSDP to perform the significance assessment. This process is often time-consuming and requires additional effort by management to review and verify. The revised BSSDP simplifies the process, which will lead to reduced staff effort and better-targeted utilization of inspector resources.

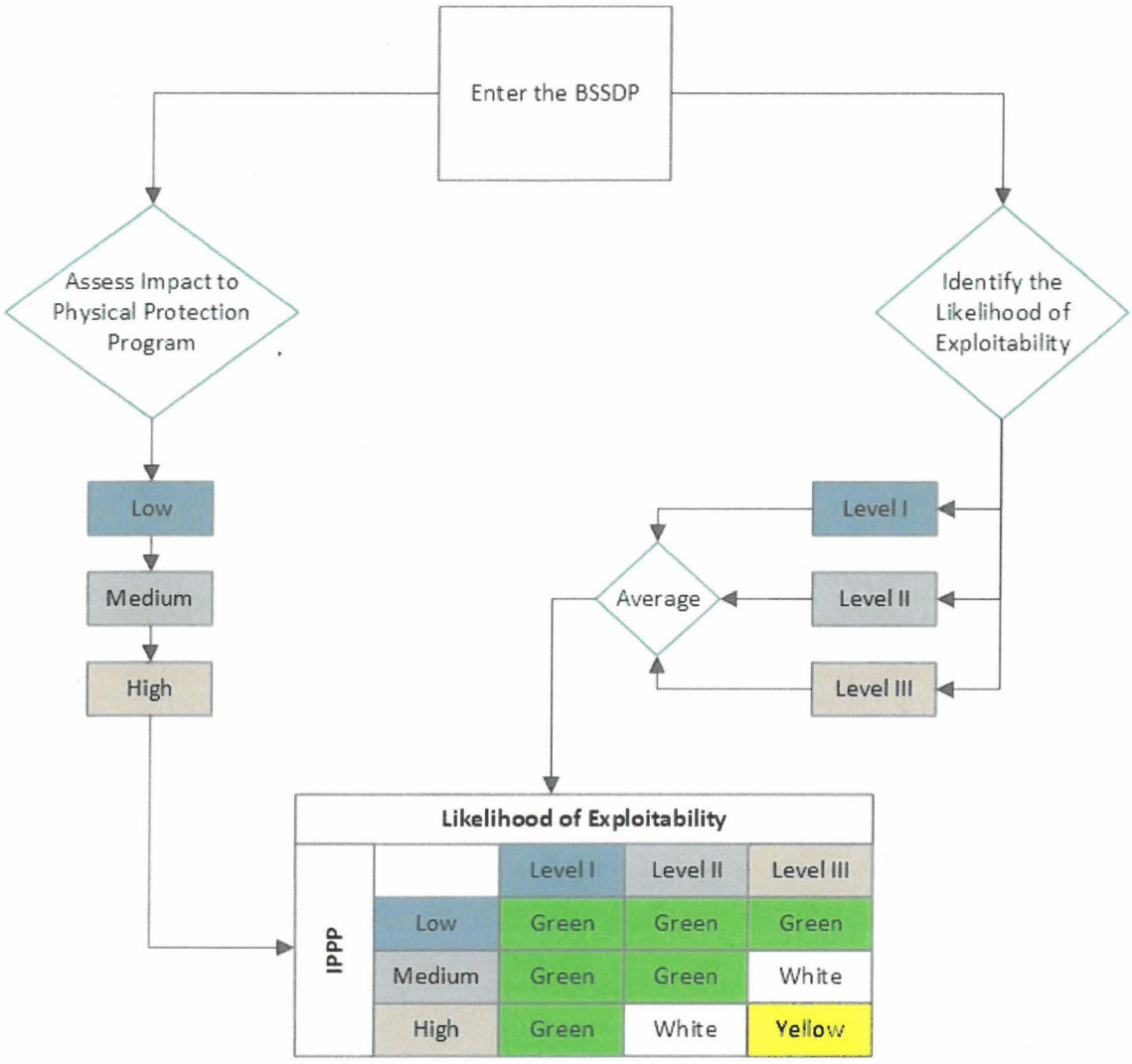

Figure 6 from revised IMC 0609, Appendix E, Part I

Likelihood of Exploitability

The likelihood of exploitability screening tool, included in revised IMC 0609, Appendix E, Part I, is a determination of how likely it is that a design-basis threat adversary would be able to identify and exploit the PD in the planning or conduct of a hostile action in order to achieve radiological sabotage. This is analogous to the risk triplet (i.e., what can go wrong, how likely it is, and what are the consequences) used in other NRC SDPs. However, in contrast to the probabilistic risk analyses that exist for safety-related events, no NRC processes exist to quantify changes in core damage frequency for security-related events and PDs, in part because existing tools do not allow the staff to assign initiating event frequencies and assess the failure rates of security personnel without assigning overly conservative or unrealistic values. This means that assigning probabilistic factors to the security cornerstone, without using an inaccurate and overly conservative probability of 1.0, is difficult. Therefore, the proposed revisions use qualitative, but objective, criteria to determine the likelihood of exploitability.

To determine the appropriate level of exploitability, NRC inspectors would assess the PD against specific criteria contained in the likelihood of exploitability table (Section 08.01, Enclosure 1) that assess the duration of the PD, ease of observation, and human and programmatic considerations. If the PD meets more than one criterion, inspectors will consider all applicable criteria and use the average of the identified levels to identify the appropriate overall level of exploitability based on the unique factors of the PD. For example, a PD that is not readily observable, predictable, or repeatable (Level I) but that impacts a system subject to a single point vulnerability (Level III) would be assessed as Level II. This determination accounts for the difficulty in identifying the PD through readily accessible means but is based on the inherent exploitability of a single point vulnerability. The enclosed IMCs provide more detail on how the determinations are calculated.

Human Versus Programmatic Issues

The staff's proposed revision also includes guidance on how to distinguish between human performance and programmatic PDs in the likelihood of exploitability tools. Specifically, human performance PDs are non-repetitive or unpredictable such that if licensee staff followed all appropriate procedures, programs, and training, the PD would not have occurred. Programmatic PDs are incorporated into the licensee's training, procedures, or processes. Programmatic PDs can also manifest in instances where organization culture, leadership, or accountability practices allow for deficiencies in performance to propagate to the point that deficient performance is repeated or predictable. As a result, programmatic PDs are predictable and identifiable through surveillance of licensee activities or through access to procedures, records, or documentation available to an insider. Therefore, the proposed revision assesses likelihood of exploitability for human performance PDs primarily based on the nature of the group of people affected, while the likelihood of exploitability for programmatic PDs is primarily based on the length of time for which the PD existed.

Impact to the Physical Protection Program

The staff's proposal also includes revisions to the existing impact to the physical protection program screening tool in IMC 0609, Appendix E, Part I. This tool is used by inspectors to determine the consequences of a PD on the licensee's physical protection program (Section 08.02, Enclosure 1). As with the likelihood of exploitability, the impact to the physical protection program tool uses a method analogous to the risk triplet used in other NRC SDPs but applies qualitative criteria to the determination of consequences due to the difficulty in assigning probabilistic factors to the security cornerstone. Inspectors will assess PDs as low, medium, or high impact to the physical protection program using various factors that affect the licensee's ability to respond to an adversary action. The impact to the physical protection tool progresses from low to medium to high continuously so that, for example, if a "high" factor applies, it would include the "medium" factor. For this reason, if the PD meets more than one criterion, rather than averaging, the inspector will choose the highest impact criterion to assess the significance of the PD.

Significance Assessment and Examples

Following identification of the likelihood of exploitability and the impact to the physical protection program, the PD is screened using a matrix that ascribes significance to the PD based on the intersection point between the two factors (see Figure 6, Enclosure 1). Additionally, the staff included examples to illustrate the application of the process and provide further guidance to NRC inspectors and external stakeholders.

Further Risk Insights to Resolve Rare or Unique Security Findings

In rare cases, security PDs may fall outside the scope of both the newly developed examples and the Table in Enclosure 1. This may occur when the unique complexities of an inspection finding challenge decisionmakers in achieving an objective and reliable risk-informed decision. For these instances, IMC 0609 Appendix M, "Significance Determination Process Using Qualitative Criteria" would be applied. Currently, IMC 0609 Appendix M serves as an alternative to existing quantitative SDP tools to determine the safety significance of inspection findings that are difficult to estimate using available risk tools and methods; however, it has not historically been used to assess security findings due to staff perception that it was not applicable to the security cornerstone despite being applicable to all ROP cornerstones. The staff included clarification and guidance in IMC 0609, Appendix E, Part I for using IMC 0609, Appendix M for those infrequent situations where the BSSDP might not provide an accurate assessment of risk.

Validation of Revised Significance Determination Methodology

The staff performed validation testing of the proposed BSSDP against all 2024 security findings to confirm that the tool appropriately and consistently determined the significance of security findings. Additionally, select findings from 2020-2023 associated with the significance screen were included in the validation testing. Only findings that were assessed via the existing significance screen and BSSDP worksheet were reviewed. In total, 35 security inspection findings were assessed during this review.

In all but two instances the draft BSSDP result matched the significance result arrived at using the current tools. The two deviations were both associated with a complete loss of security function. Specifically, both findings involved failures of the licensee to maintain the backup and uninterruptible power supply for security response in an operable condition for a period of greater than 1 year. In both instances, this loss of security function resulted in a condition where a loss of offsite power would significantly challenge licensee response capability to detect, assess, and respond to a security threat until compensatory measures were enacted. Additionally, both instances were documented in licensee maintenance records and easily identifiable to personnel with access to the licensee computer systems. Neither licensee properly identified the significance of the non-functional system on the operation of security or prioritized maintenance to correct the deficiency. In one instance, the failure was identified through a loss of offsite power that resulted in a complete loss of security power for several hours and resulted in a yellow finding, as assessed through the significance screen. The second instance was identified by an NRC inspector during a baseline security inspection and resulted in a green finding as assessed through the BSSDP worksheet. Only the actual loss of security power differentiates the two findings. The proposed BSSDP assessed white significance for both findings.

Because of the similarities in the findings, both findings would be assessed the same in accordance with the proposed BSSDP. Specifically, likelihood of exploitability would be

assessed as Level III and the IPPP would be assed as medium. The actual loss of offsite power is not a factor in the proposed BSSDP.

For the likelihood of exploitability, the failure of the backup power system affected greater than 75% of the protected area barrier (Level III), was a programmatic deficiency that existed for greater than one year (Level III), and could be easily identified by a person with access to the site or licensee records (Level II). The average of the identified criteria results in a Level III determination.

The IPPP assessment of medium is based on a determination that the failure of the secondary power supply could result in a loss of detection capability such that an unauthorized person could potentially enter the protected area undetected. That determination is based on the assumption that licensees cannot protect the site from a loss of offsite power if the secondary power supply is not available. For these reasons, loss of offsite power is a common initial event in force-on-force exercises. In these examples, an adversary causing a loss of offsite power at the initiation of an attack would be able to exploit the failure of backup power to enter the site without causing an alarm.

Many of the potential factors that would risk-inform the significance of a similar finding in the proposed BSSDP are not present in the existing BSSDP. For example, if the equipment failure was the result of limited human error or was not readily known to the site population, the finding would be less significant. Also, changes to the assessment matrix allow for the time the deficiency existed to more appropriately reflect the risk of the finding. For example, if the performance deficiency existed for less than one year, the resultant finding would be green.

The staff determined that the current BSSDP emphasizes event occurrence while underemphasizing total impact the performance deficiency has on the physical protection program. The staff recognizes that the existing BSSDP does not fully incorporate risk insights that contribute to the realism of the impact to the physical protection program. The proposed BSSDP developed by the staff revises this approach to more consistently and realistically assess risk. Specifically, the proposed BSSPD allows for considerations and factors that directly contribute to a realistic determination of risk to be included earlier in the determination of significance.

The staff determined that the above-discussed findings, as well as others that were assessed during validation demonstrate that the proposed BSSDP is able to more quickly and consistently assess the significance of findings. By including additional risk criteria and risk assessment methods, the staff determined that the proposed BSSDP is more consistent with the rest of the reactor oversight process, will reduce staff effort in assessing significance, and will result in significance determinations that are less subjective and more realistic.

Alignment with Other Items Before the Commission

The staff determined that this revision to the BSSDP aligns with other proposed changes to the reactor oversight process and issue screening. Specifically, changes to more-than-minor screening discussed in a separate paper to the Commission would integrate well into this proposed BSSDP through the assessment of the impact to the physical protection program. If the more-than-minor recommendations are approved by the Commission, issues that do not meet the Low impact to the physical protection program category could immediately screen as minor without the need for the inspectors to perform additional assessments or reviews. The staff anticipates that this assessment method would better screen issues that do not result in

impacts to the physical protection program while maintaining an appropriate focus on risk-significant issues.

Training Needs Analysis

Initial and periodic training on the revised BSSDP framework is required to ensure its consistent application. The staff will develop introductory training following Commission review and approval of the proposed BSSDP. Initial training will be incorporated into the appropriate IMC 1245, "Qualification Program for Reactor Inspectors," appendices. Additionally, periodic refresher training will be incorporated into the annual security inspector counterpart meeting.

RECOMMENDATION:

The staff recommends that the Commission approve the staff's proposal to revise the current BSSDP as documented in enclosures 1 and 2. Among other changes shown in the enclosures, the staff recommends eliminating the significance screen (i.e., Figure 4 in IMC 0609, Appendix E, Part I) and BSSDP worksheets (i.e., Figures 7-11 in IMC 0609, Appendix E, Part I) and replacing them with the newly proposed Figure 6 in IMC 0609, Appendix E, Part I, which assesses significance using the likelihood of exploitability and impact to the physical protection program screening tools.

RESOURCE:

Resource needs for fiscal year (FY) 2026 are included in the current budget estimate. Resources for FY 2027 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.

Michael F. King
Acting Executive Director
for Operations

Enclosures:
1. IMC 0609, Appendix E, Part I Rev. 0
2. IMC 0308, Attachment 3, Appendix E Rev. 0

SUBJECT: STAFF RECOMMENDATION FOR REVISIONS TO THE BASELINE SECURITY SIGNIFICANCE DETERMINATION PROCESS DATED: October 21, 2025

ADAMS Accession No.: ML25168A179 (Pkg.) SECY: ML25168A177, Encl 1: ML25168A178, Encl. 2: ML25168A76

OFFICE	NSIR/DSO/SOSB	NSIR/DSO/SOSB	NSIR/DSO/SOSB
NAME	MBrooks	JBream	DDavis
DATE	6/18/25	6/18/25	6/30/25
OFFICE	NSIR/DSO	NRR	R-IV/DRSS
NAME	TInverso	RFelts	TBloomer
DATE	7/2/25	7/2/25	7/3/25
OFFICE	R-1	R-II	R-III
NAME	DCollins	JLara	JGeissner
DATE	7/28/2025	8/1/25	7/28/25
OFFICE	R-IV	OE	OCHCO/ADHRLD
NAME	JMonninger	BPham	SCochrum
DATE	7/8/25	8/7/25	7/28/25
OFFICE	NRR/OD	OGC	NSIR
NAME	GBowman	KGamin	CErlanger
DATE	7/17/25	8/21/25	9/4/25
OFFICE	OEDO/EDO (A)		
NAME	MKing		
DATE	10/ 21 /25		

OFFICIAL RECORD COPY