INSPECTION MANUAL CHAPTER 0609 APPENDIX E, PART I

BASELINE SECURITY SIGNIFICANCE DETERMINATION PROCESS FOR POWER REACTORS

Effective Date:

0609EI-01 PURPOSE

The Baseline Security Significance Determination Process (BSSDP) incorporates areas of material control and accounting (MC&A), protection of Safeguards Information (SGI), and physical protection.

The BSSDP is utilized once a performance deficiency (PD) has been evaluated as more than minor using Inspection Manual Chapter (IMC) 0612, Appendix B, "Issue Screening Directions," and determined to be in the security area in accordance with IMC 0609, Attachment 4, "Initial Characterization of Findings."

01.01 Baseline Security Significance Determination Process Overview. The process for determining the correct SDP tool for analysis of findings is depicted in Figure 1, "Baseline Security SDP Flowchart."

01.02 MC&A SDP. Figure 2 is the flowchart for determining the risk-significance of findings related to licensee activities required by Title 10 of the *Code of Federal Regulations* (10 CFR) Part 74, "Material Control and Accounting of Special Nuclear Material (SNM)." This focuses on the effectiveness of records, procedures, and physical inventories used to control and account for SNM at nuclear power plants. Use of the flowchart is intended to determine the significance of findings involving protection against the theft or loss of SNM.

01.03 Unsecured SGI. Figure 3 is the decision tree for use in determining the risk-significance of findings related to licensee activities required by 10 CFR 73.22, "Protection of Safeguards Information: Specific Requirements." In using this decision tree, the significance determination process focuses on factors affecting the likelihood of compromise by evaluating the nature of the information and the conditions under which it was left unattended or improperly protected.

01.04 Unattended Opening (UAO). The flowchart depicted in Figure 4 is used in determining the risk-significance of findings related to licensee activities required by 10 CFR 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage." The significance determination process uses a graded approach by focusing on attributes of a licensee's defense-in-depth physical protection program in the disposition of UAOs. This process allows the final characterization to accurately reflect the risk-significance of the finding.

01.05 Target Sets. The flowchart depicted in Figure 5 is used in determining the risk significance of findings related to licensee activities required by 10 CFR 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors

against radiological sabotage." While this flowchart focuses on the areas applicable to target sets, including target set processes, consideration of cyber-attacks, and target set oversight, it also provides a link to the BSSDP Flowchart and cyber security SDP, if applicable. The BSSDP Flowchart and cyber security SDP's sheets are used to determine the risk-significance of target set findings that either resulted in a change to the protective strategy or impacted the cyber security program.

01.06 BSSDP Flowchart. The BSSDP Flowchart is depicted in Figure 6. Performance deficiencies that are not screened in previous sections are assessed for significance through a risk-informed process that assesses risk based on the likelihood that an adversary would be able to identify and exploit deficiencies and the actual or potential impact to the physical protection program.

0609EI-02 DEFINITIONS

Approved Location – A location designated for use or storage of SNM that allows the SNM to be readily located. The approved location is controlled so that the SNM is not loose (e.g., not on the spent fuel pool floor) or outside an appropriate container (e.g., fuel bundle or storage container designated to hold SNM).

Defense-in-Depth – Multiple independent and redundant layers of protection against the various attributes within the DBT, such that no single layer, no matter how robust, is exclusively relied upon.

Exploitable – A condition through which a potential adversary could defeat, circumvent, or otherwise takes advantage of a vulnerability in a security plan, equipment, or performance.

Target Set – The minimum combination of equipment or operator actions which, if all are prevented from performing their intended safety function or prevented from being accomplished, would likely result in significant core damage (e.g., non-incipient, non-localized fuel melting and/or core destruction) or a loss of spent fuel pool water inventory and exposure of spent fuel, barring extraordinary actions by plant operations.

Unsecured SGI – A condition involving SGI that increases the likelihood of compromise as a result of a failure of a licensee, or its contractor, to implement the protection requirements of 10 CFR 73.22 involving (1) secure storage, (2) document marking, (3) restricted access, (4) limited reproduction, (5) secure transmission, (6) external transmission, (7) enhanced automatic data processing system controls, and (8) appropriate destruction.

0609EI-03 GENERAL GUIDANCE

03.01 Initial Inspector Review

Before entering the BSSDP, the issue should be screened using IMC 0612, Appendix B, "Issue Screening Directions." When the results of that screening yield more than minor significance and the finding is determined to be in the security area in accordance with IMC 0609, Attachment 4, "Initial Characterization of Findings," the inspector should enter the BSSDP at the top of Figure 1.

03.02 Findings with Multiple Examples

When characterizing a finding, multiple individual PDs cannot be aggregated into one finding of greater significance. Additionally, when a finding is identified that has multiple examples, the most significant example should be used to characterize the overall significance of the finding.

03.03 Technical Basis for the SDP

Inspectors and staff should refer to IMC 0308, Attachment 3, Appendix E, “Technical Basis for the Baseline Security Significance Determination Process,” if more specific information is needed on a particular aspect of the SDP, or for information on how certain criteria and thresholds were established.

03.04 Using Inspection Manual Chapter 0609, Appendix M

As an alternative to existing quantitative SDP tools, IMC 0609 Appendix M, “Significance Determination Process Using Qualitative Criteria,” was developed to determine the safety significance of inspection findings that are difficult to estimate using available quantitative risk tools and methods. IMC 0609 Appendix M will be utilized when the SDP is not sufficient to allow the inspector to adequately assess the significance of a finding to provide qualitative and quantitative attributes for risk-informed decision making. In order to utilize IMC 0609 Appendix M, staff should consult a regional senior risk analyst and conduct a planning SERP as directed by IMC 0609 Appendix M guidance.

Per Figure 1, Appendix M will only be utilized in situations where the inspector is not able to adequately assess the significance of a finding using the BSSDP. These situations are expected to be rare and will include unique instances of significant and substantive failures of a licensee to implement a protective strategy that is able to defend against the design basis threat.

0609EI-04 EVALUATING MATERIAL CONTROL AND ACCOUNTING FINDINGS (FIGURE 2)

In evaluating MC&A findings, use Figure 2, MC&A SDP flowchart:

04.01 Does the finding involve only non-fuel SNM in quantities of less than one gram in aggregate?

If the finding involves only non-fuel SNM in quantities of less than one gram in aggregate (such as detectors, instruments, or sources), then the finding is Green.

If any aspect of the finding involves nuclear fuel (in any quantity), or non-fuel SNM greater than or equal to one gram, then continue to 04.02.

04.02 Did the finding involve missing SNM, and if so, was the missing SNM subsequently identified in an approved storage location within 7 days of identification that it was missing?

If the finding did not involve missing SNM, or the missing SNM was subsequently found in an approved storage location within 7 days of discovery that it was missing, then the finding is Green.

If the finding involved missing SNM and it was recovered outside an approved storage location, or if the search effort exceeded 7 days, then continue to 04.03.

04.03 Is the SNM considered lost?

Inspectors should evaluate the licensee's search efforts and recovery plans to determine if there is a reasonable expectation that further searches will lead to recovery of the SNM. If the inspector concludes that recovery of the SNM is unlikely after 7 days, the inspector should consider the material lost when evaluating the significance of the finding.

If the missing SNM was recovered outside an approved storage location, or if it was recovered after a search effort lasting greater than 7 days, then the finding is White.

If the missing SNM cannot be located after 7 days and a determination is made that further search efforts are not reasonably expected to recover the missing SNM, then the SNM is considered lost, and the finding is Yellow.

0609EI-05 EVALUATING UNSECURED SAFEGUARDS INFORMATION FINDINGS (FIGURE 3)

In evaluating unsecured SGI findings, use the Decision Tree for Unsecured SGI, Figure 3. Note that, in accordance with IMC 0612, Appendix B, "Issue Screening Directions," if a licensee's failure to protect SGI results in a compromise of the information, such a compromise would constitute an actual consequence of the PD. The PD should be evaluated using this SDP, while the actual consequences should be evaluated in parallel using the Enforcement Policy. IMC 0612 Appendix B describes the process for screening a PD with actual consequences through both the ROP and traditional enforcement.

05.01 Does the finding involve any of the following types of SGI?

a. Detailed specific information about two or more characteristics of the DBT;

b. Licensee's safeguards information regarding the physical security program, not easily discernible from observation at locations outside of the PA and would significantly aid an adversary in the defeating the protective strategy including (but not limited to):

   Safeguards Contingency Plan
   Physical Security Plan
   Training and Qualification Plan
   Protective Strategy Implementing Procedures
   Target Sets Booklet

c. Details that specifically indicate which security posts are dedicated armed response team members required by the security plan, or the total number of minimum armed responders and armed security officers required;

d. Prints, schematics, diagrams, or drawings that represent a substantial portion of a system within the licensee's protective strategy (e.g., a drawing that outlines the underground penetrations into the PA and the associated protective measures, or a drawing that describes the primary and backup power supplies for security systems) and identifies a condition or system configuration exploitable by an adversary; or,

e. Generic information (such as generic communications, industry guidance documents, or other similar documents) that provides details of security measures or processes, the compromise of which could potentially impact multiple facilities

If the finding involves SGI other than that of the type described in 05.01, then the finding is Green.

If the finding involves SGI of the type described in 05.01, then continue to 05.02.

05.02 Does the finding relate to a failure to physically control SGI (paper documents, universal serial bus (USB) flash drives, compact discs, etc.), or a failure to electronically control SGI data (such as files improperly stored on a network share, or unencrypted SGI disseminated via email)?

If the finding relates to a licensee's failure to exercise electronic control over SGI (such as storing files on a network or computer with network access, or emailing unencrypted SGI), then continue to 05.02.a.

If the finding relates to a licensee's failure to exercise physical control over SGI (whether in paper form or an electronic storage device such as a USB flash drive), then continue to 05.02.b.

a. Was electronic SGI identified and corrective actions begun within the appropriate timeframe?

SGI discovered on electronic storage media should be purged in a manner that ensures the information is not recoverable. Licensees should purge electronic storage devices of SGI in a manner consistent with 10 CFR 73.22(g)(4). Refer to Regulatory Guide 5.79, "Protection of Safeguards Information," for guidance on acceptable methods of purging electronic storage devices containing SGI.

If the SGI was discovered within 7 days of storage or processing on the affected electronic systems (such as email inboxes/outboxes, network shares, network accessible drives, or network backups) and within 24 hours of discovery the licensee commenced a process to identify, contain, or purge all recoverable SGI from those systems, then the finding is Green.

If the SGI was discovered after 7 days of storage or processing on the affected electronic systems or the licensee did not begin a process to identify, contain, or purge the recoverable SGI within 24 hours of discovery, then the finding is White.

b. Was the physically unsecured SGI protected from unauthorized access using encryption (Federal Information Protection Standard (FIPS) 140-2 or later) and an authentication mechanism such as a password?

While encryption is not an approved method of storing SGI data at rest, it does reduce the potential that the information will be compromised if left unattended. The failure to control encrypted media is therefore considered less significant than a failure to protect hardcopies or unencrypted storage media.

If the physically unsecured SGI was protected from unauthorized access using encryption and was unattended within the PA, then the finding is Green.

If the physically unsecured SGI was protected from unauthorized access using encryption and was unattended outside of a PA for less than 30 days, then the finding is Green.

If the physically unsecured SGI was protected from unauthorized access using encryption but was unattended outside of a PA for at least 30 days or more, then the finding is White.

If the physically unsecured SGI was either unencrypted storage media or hardcopies, then continue to 05.03.

05.03 Was the unsecured SGI located inside a controlled access area (CAA), OCA, or PA?

This step considers protections that may be provided by the environment in which the SGI was left unattended. An OCA provides some level of protection above that of a public space. PAs provide additional access control measures as well.

In addition to the consideration of OCA or PA areas, some licensees may have established CAAs (a location that is temporarily or permanently established which is clearly demarcated, access to which is controlled, and which affords isolation of the material or persons within it). A CAA may have been established by the licensee, or its contractors, at its plant or offsite facilities:

If the unsecured SGI was located within a PA, the finding is Green;

If the unsecured SGI was located within a CAA or OCA, then continue to 05.04;

If the unsecured SGI was located outside the OCA or CAA, then continue to 05.05.

05.04 Did the location where the SGI was left unattended provide limited access to the material?

A location provides limited access if it meets all of the following conditions:

- The area was locked or had access control measures;
- Individuals that frequented the area were part of a known population; and,
- Records of personnel entry were maintained to the area via key control or key card access.

If the location of the SGI provided limited access, then continue to 05.04.a.

If the location of the SGI did not provide limited access, then continue to 05.04.b.

a. Determine the duration of time that the SGI was left uncontrolled.

   i. If likelihood of discovery is high and the time is ≤ 14 days, the finding is Green.

   ii. If likelihood of discovery is high and the time is > 14 days, the finding is White.

   iii. If likelihood of discovery is low and the time is ≤ 30 days, the finding is Green.

   iv. If likelihood of discovery is low and the time is > 30 days, the finding is White.

b. Did the circumstances under which the SGI was left uncontrolled provide for a low or high likelihood of discovery?

The likelihood of compromise of SGI is determined by evaluating a combination of the conditions under which the material was left unattended (i.e., the likelihood of discovery) and the duration of time it was left unattended. Leaving SGI unattended in the open and leaving SGI unattended for a long period of time both increase the likelihood that the SGI could be compromised.

Storage conditions are related to the likelihood of discovery as follows:

1. High likelihood of discovery – the material could be readily identified by a casual observer (e.g., located on top of a desk, left unattended on a copy machine, left in a break room or other shared workspace).

   NOTE: An unmarked electronic storage device is considered to have a high likelihood of discovery, regardless of the location it was left unattended, because there is an increased risk that an individual could use the device for non-SGI purposes (unaware that it contains SGI), and cause a spillage of information onto unsecure computers or networks.

2. Low likelihood of discovery – the material could not be readily identified by a casual observer (e.g., in a desk drawer or in a filing cabinet). SGI left unattended in the PA (except unmarked electronic media as described above) shall be determined to have a low likelihood of discovery.

3. Once the likelihood of discovery has been determined, calculate the duration of time that the SGI was left unattended.

   i. If likelihood of discovery is high and the time is ≤ 1 hour, the finding is Green.

   ii. If likelihood of discovery is high and the time is > 1 hour, the finding is White.

   iii. If likelihood of discovery is low and the time is ≤ 96 hours, the finding is Green.

   iv. If likelihood of discovery is low and the time is > 96 hours, the finding is White.

05.05 Was the SGI in transit during the time it was left unattended?

Determine if the unsecured SGI was placed in transit (i.e., as specified in 10 CFR 73.22(f)).

If the SGI was not in transit, then continue to 05.06.

If the SGI was in transit and the SGI was considered to be partially protected, then the finding is Green. Material is considered to be protected if the package was traceable and/or protected by at least one wrapping.

If the SGI was in transit and the SGI was not considered to be partially protected, then the finding is White.

05.06 Was there limited access to the SGI when it was left unattended outside the OCA?

SGI left unattended in a space outside the OCA accessible to the public does not have limited access. Otherwise, a location provides limited access if it meets all of the following conditions:

a. The area was locked or had similar access control measures;

b. Individuals that frequented the area were part of a known population; and,

c. Records of personnel entry were maintained to the area via key control or key card access.

If there was limited access to the SGI, then go to 05.04.b.

If there was not limited access to the SGI, then the finding is White.

0609EI-06 EVALUATING UNATTENDED OPENING FINDINGS (FIGURE 4)

06.01 Identifying the impact area

Once the inspector(s) determines that the licensee failed to meet the requirements for the protection of an UAO found in 10 CFR 73.55(i)(5)(iii) the inspector(s) should then determine if the UAO could have allowed undetected access to either of the following impact areas, the protected area (PA) or the vital area (VA) or allowed undetected access from the PA into the VA.

06.02 Identifying and crediting physical barriers and intrusion detection systems

After the inspector(s) has made the determination as to what areas the UAO would allow access to and from, the inspector(s) must then determine the number of physical barriers and/or intrusion detection systems that an adversary must defeat prior to gaining access to a complete target set. The inspector(s) shall consider the ingress point of the unattended opening as the starting point to evaluate barriers and/or intrusion detection systems. The ingress point is defined as the exterior entrance (pipe outfall, manhole in the OCA that leads to PA or VA, tunnel, etc.) which an adversary would enter to defeat the UAO (e.g., if the UAO starts at a welded manhole in OCA which is captured in procedures and checked on some periodicity, the manhole would be the first barrier).

Note: Collocated physical barriers and/or intrusion detection systems will be considered one system. Examples of collocated systems include, but are not limited to, a steel door with an attached intrusion detection alarm, an Early Warning System (EWS) with a barrier and detection, or steel grating with a motion detection camera.

In making this determination, inspector(s) should typically only credit the physical barriers and/or intrusion detection systems at and beyond the ingress point that meet the following criteria. However, if the ingress point is surrounded by a barrier that meets the following criteria or a detection system that would detect entry prior to reaching the ingress point, or both (like an EWS that is maintained, tested, and implemented in accordance with the Physical Security Plan), then that barrier or detection system may also be credited in this process provided it also meets the following criteria:

Physical Barriers – A barrier that meets the definition in 10 CFR 73.2 and 73.55(e)(3)(iii). These physical barriers would require the adversaries to use defeat methodologies that, had it been observed, would result in an initiation of the licensee's protective strategy. Physical barriers include, but are not limited to: closed steel piping systems, closed concrete tunnels, secured manhole covers, and concrete blocks. To provide credit in this flow chart, the physical barriers are required to be captured in the licensee's security plan or implementing procedures and controlled by security. Controlled by security means checked on some periodicity (not required to be commensurate with task time) or monitored by security so that they are aware of the barrier's integrity.

Intrusion Detection Systems – Video Analytics, Volumetric Systems, and Planar Systems specifically identified and documented by security for use in the implementation of its protective strategy and are monitored by a member of the on-duty security force capable of initiating a security response (consistent with NUREG-1959). Early warning systems located within the owner controlled area or protected area may be given credit, if the inspector(s) determine the system is reliable and provides for detection and assessment.

The inspector will evaluate the system to ensure it performs its intended function, is maintained and tested consistently with the manufacturer's specification, and is compensated for when not in service.

06.03 The inspector(s) should then use the following steps to determine the significance of UAO related findings:

If the pathway could allow undetected access into the PA, the inspector(s) should then determine if this was due to emergent work, such as unplanned outages, unplanned plant configuration changes, or unplanned equipment changes of less than 7 days (168 hours). Findings resulting from the above stated criteria would screen as a Green.

If the pathway was not due to emergent work, such as unplanned outages, unplanned plant configuration changes, or unplanned equipment changes and could allow undetected access into the PA, the inspector(s) should then determine the number of physical barriers and or intrusion detection systems that an adversary would be required to defeat prior to gaining access to a complete target set.

For PA entry points that require passage through two or more physical barriers or intrusion detection systems prior to allowing access to a complete target set, the finding is screened as Green.

For PA entry points that require passage through one physical barrier or intrusion detection system prior to allowing access to a complete target set, the finding is screened as White.

For PA entry points where passage through no physical barriers or intrusion detection systems prior to allowing access to a complete target set, the finding is screened as Yellow.

If the pathway could allow undetected access into the VA, the inspector(s) should determine if this was due to emergent work, such as unplanned outages, unplanned plant configuration changes, or unplanned equipment changes of less than 7 days (168 hours). Findings resulting from the above stated criteria would screen as Green.

If the pathway was not due to emergent work, such as unplanned outages, unplanned plant configuration changes, or unplanned equipment changes and could allow undetected access into the VA and has lasted longer than 7 days (168 hours), the inspector(s) should determine the number of physical barriers and/or intrusion detection systems that an adversary would be required to defeat prior to gaining access to a complete target set.

For VA entry points that require passage through one or more physical barriers or intrusion detection systems, prior to allowing access to a target set component(s) that does not comprise of a complete target-set, the finding is screened as Green.

For VA entry points that require passage through one or more physical barriers or intrusion detection systems prior to allowing access to a complete target set, the finding is screened as White.

For VA entry points where passage through no physical barriers or intrusion detection systems, prior to allowing access to complete target set, the finding is screened as Yellow.

If the pathway could allow undetected access from the PA into a VA, the finding is screened as Green.

0609EI-07 EVALUATING TARGET SET FINDINGS (FIGURE 5)

In evaluating target set findings, use Figure 5, Target Set SDP flowchart:

07.01 Does this PD result in changes to the licensee's target sets that can be corrected without requiring changes to the licensee's protective strategy or cyber security plan?

If yes, then continue to 07.03.

If no, and a change to the licensee's protective strategy or cyber security plan is required, then go to 07.02.

A change to the licensee's protective strategy is defined as (not an all-inclusive list):

a. Addition of new security personnel,
b. Reassignment of existing security personnel to a new defensive position,
c. Reassignment of existing security personnel to existing defensive positions as either an initial position or an automatic redirect,
d. Assignment of a timeline to an armed security officer,
e. Modification of barriers to increase adversary delay, or
f. Additional credited operator action to existing target sets.

07.02 Is this PD cyber-related?

If yes, transition to IMC 0609, Appendix E, Part IV, Cybersecurity Significance Determination Process for Power Reactors.

If no, then process the finding in accordance with the BSSDP worksheets described in this document. Licensee's shall analyze and identify site-specific conditions, <u>including target sets,</u> that may affect the specific measures needed to implement the requirements

of this section and shall account for these conditions in the design of the physical protection program in accordance with 10 CFR 73.55(b)(4).

07.03 Does the licensee consider cyber-attacks in the development and identification of target sets?

If the licensee considers cyber-attacks, then go to 07.04.

If the licensee does not consider cyber-attacks, then the finding is Green. The licensee shall consider cyber-attacks in the development and identification of target sets in accordance with
10 CFR 73.55(f)(2).

07.04 Did the licensee adequately document and maintain the process used to develop target sets?

A failure to adequately document and maintain the process used to develop target sets includes (not an all-inclusive list):

a. Process did not identify target set elements and/or locations,
b. Incorrect grouping of target set elements,
c. Flawed methodology to identify target sets,
d. Process not maintained to identify new target set elements, or
e. Site-specific analysis used to develop target sets is not documented and/or maintained.

Review 10 CFR 73.55(m) for applicability. The licensee is expected to periodically review target sets for completeness and continued applicability consistent with the requirements of
10 CFR 73.55(m), ‘‘Security program reviews.’’

If yes, then continue to 07.05.

If no, then the finding is Green.

For target set equipment or elements in the protected or vital area, the licensee shall document and maintain the process used to develop and identify target sets, to include the site-specific analyses and methodologies used to determine and group the target set equipment or elements in accordance with 10 CFR 73.55(f)(1).

For target set equipment or elements that <u>are not</u> contained within the PA or VA, the licensee must identify and document target set equipment or elements consistent with the requirements in 10 CFR 73.55(f)(1) and they shall be accounted for in the licensee’s protective strategy in accordance with 10 CFR 73.55(f)(3).

07.05 Does the PD involve the licensee’s process for the oversight of target set equipment and systems to ensure changes to the configuration are considered in the protective strategy?

If yes, the finding is Green. The licensee shall implement a process for the oversight of target set equipment and systems to ensure that changes to the configuration of the identified equipment and systems are considered in the licensee’s protective strategy.

Where appropriate, changes must be made to documented target sets in accordance with 73.55(f)(4).

Review 10 CFR 73.58, “Safety/security interface requirements for nuclear power reactors” for applicability.

If no, then continue to 07.02.

0609EI-08 EVALUATING FINDINGS USING THE BASELINE SECURITY SIGNIFICANCE DETERMINATION FLOWCHART (FIGURE 6)

Any finding that does not meet one of the entry criteria for the previous assessment tools or that those tools directed to the BSSDP Flowchart will be evaluated per the guidance contained in this section.

08.01 Determine the Likelihood of Exploitability

The Likelihood of Exploitability is a determination of how likely a DBT adversary would be able to identify or utilize the PD in the planning or conduct of a hostile action in order to achieve radiological sabotage. This is analogous to the risk triplet utilized in other NRC SDPs but applies qualitative criteria to the determination of likelihood due to the difficulty in assigning probabilistic factors to the security cornerstone.

The inspector should assess the PD against the criteria in the table below to identify the appropriate level of exploitability. The criteria in the table are not all-inclusive, and more than one criterion may be applicable. If the PD meets more than one criterion, an average of the identified levels should be used to identify the most appropriate 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) should be assessed as Level II.

In averaging, results will be rounded to the nearest whole number: 0.1, 0.2, 0.3, 0.4 are rounded down, and 0.5, 0.6, 0.7, 0.8, 0.9 are rounded up.

Each of the criteria in the table below represent a direct escalation path from Level I to Level III. Meeting the higher criterion negates the corresponding lower criterion. For example, a performance deficiency that is only documented in an SGI procedure but can be readily observed by someone with access to the site would be assessed at Level II.

A Human Performance PD is a non-repetitive, unpredictable event in which if licensee staff followed all appropriate procedures, programs, and training, the PD would not have occurred. Programmatic issues are performance deficiencies that are incorporated into the licensee’s training, procedures, or processes. Programmatic issues 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 repetitive 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 the insider as described in 10 CFR 73.1.

If the inspector cannot identify an appropriate criterion, assess the unique aspects of the PD against the collected criteria to identify the most appropriate impact level. Additionally, if the

duration of a programmatic PD cannot be determined, assess the duration at greater than one year.

Likelihood of Exploitability	
I	• Human Performance PD (not involving contraband) impacted only critical group staff. • Programmatic PD existed for less than 30 days. • PD was not readily observable, predictable, or repeatable (e.g., unknown, contained in SGI procedures, etc.). • Limited or isolated impact to PA barrier security detection and assessment system or component.
II	• Human Performance PD impacted licensee staff and contractors with UA/UAA (including materials, vehicles, packages handled by staff with UA). • Programmatic PD existed for 30 days to one year. • PD could be identified by personnel with access to the site or to non-SGI licensee procedures. • Multiple consecutive sections of the PA barrier security detection and assessment system or component were impacted.
III	• Human Performance PD impacted escorted personnel or personnel without UA/UAA (e.g., visitor, vehicle, bulk/hazardous material). • Programmatic PD existed for greater than one year. • PD could be identified with publicly available information or observation. • Greater than 75% of the sections of the PA barrier security detection and assessment system or a component with a single point vulnerability were impacted.

08.02 Determine Impact to the Physical Protection Program (IPPP)

The IPPP is a determination of the consequences of the PD on the effectiveness of the licensee's physical protection program and its ability to respond to an adversary action. This is analogous to the risk triplet utilized 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.

The inspector should assess the PD against the criteria in the table below to identify the appropriate impact. The criteria in the table is not all inclusive, and depending on the conditions of the PD, more than one criterion may be applicable. If the PD meets more than one criterion, choose the highest impact for assessment of the significance.

If the inspector cannot identify an appropriate criterion, assess the unique aspects of the PD against the overall impact statement to identify the most appropriate impact level.

Impact to the Physical Protection Program	
Low	Failure of a component of the physical security plan or protective strategy for which there is limited impact to the ability of the licensee to defend against the design basis threat of radiological sabotage.

	Failure of a key program element related to the prescribed requirements and standards for the establishment, implementation, and maintenance of the fitness-for-duty (FFD) or Access Authorization (AA) program resulting in limited program impact. Examples include: • Inadequate search of personnel, material, or vehicle for which no contraband was present, or unauthorized personnel entered the protected area but was immediately identified or in positive control of security personnel the entire time. • UA/UAA inappropriately granted or maintained. • Staff with UA inappropriately granted access to VA for which they do not have continuing need. • Previously unidentified or unanalyzed vulnerability in the protective strategy that could allow an adversary to compromise one or more components (but not all) of a multi-component target set. • One armed responder, armed security officer, or alarm station operator unavailable or unable to respond to a contingency event due to availability of response equipment, being out of position, or attentiveness. • Limited failure of the training and qualification program not directly associated with protective strategy response duties. • Limited failure of detection or assessment system such that unauthorized persons could enter the protected area undetected but would likely be detected through other means. • A cyber event, cyber vulnerability, or failure to implement cybersecurity controls on a CDA or CDAs that would adversely degrade the security function or security functions of a CDA, but the compromise would likely be detected through alternate controls that are in place.

Med	Failure of a component of the physical security plan or protective strategy for which there was a moderate impact to the ability of the licensee to defend against the design basis threat of radiological sabotage. Failure of a key program element related to the prescribed requirements and standards for the establishment, implementation, and maintenance of the FFD or AA program resulting in moderate program impact. Examples include: • UA/UAA inappropriately granted or maintained, the affected staff entered the PA, and the affected staff should have been denied for trustworthiness and reliability. • Previously unidentified vulnerability in the protective strategy that could allow an adversary to compromise a complete target set but for which the protective strategy can respond. • Multiple (but not full shift complement) armed responders, armed security officers, or alarm station operators unavailable or unable to respond to a contingency event due to the failure to be properly qualified (in accordance with the training and qualification plan), availability of response equipment, being out of position, or attentiveness. • Significant failure of detection or assessment system such that unauthorized persons could enter the protected area undetected. • A cyber event, cyber vulnerability, or failure to implement cybersecurity controls on a CDA or CDAs that would degrade a security function or security functions on a CDA. • Personnel responsible for program implementation lack sufficient knowledge, skills, and abilities to implement the FFD program according to procedural requirements.

High	Failure of a component of the physical security plan or protective strategy for which there is a significant impact to the ability of the licensee to defend against the design basis threat of radiological sabotage. Failure of a key program element related to the prescribed requirements and standards for the establishment, implementation, and maintenance of the FFD or AA program resulting in significant program impact. Examples include: • Contraband entered the protected area, or an unauthorized person entered the protected area undetected and uncontrolled. • Previously unidentified vulnerability in the protective strategy that could allow an adversary to compromise a complete target set for which the protective strategy cannot prevent. • A full shift of armed responders, armed security officers, or alarm station operators unavailable or unable to respond to a contingency event due to the failure to be properly qualified (in accordance with the training and qualification plan), availability of response equipment, being out of position, or attentiveness. • Significant failure of the security training and qualification program such that security officers would be unable to implement the protective strategy to successfully respond to an adversary attack. • A cyber event, cyber vulnerability, or failure to implement cybersecurity controls on a CDA or CDAs that has degraded a security function or security functions on a CDA that would affect the security force's ability to respond within the protective strategy assumed timelines.

08.03 Assess PD Significance

Using the matrix in Figure 6, the inspector should assess PD significance as the cross point between Likelihood of Exploitability and IPPP.

Impact to the Physical Protection Program	Likelihood of Exploitability		
	I	II	III
Low	Green	Green	Green
Medium	Green	Green	White
High	Green	White	Yellow

08.04 Finding Examples

Examples are included for illustrative purposes and are not all inclusive.

a. The licensee implemented a change to the protective strategy that removed required response equipment from service. The removed response equipment directly impacted the ability of armed response force personnel to respond to the design basis threat. The

change was implemented 90 days before it was identified by an inspector; however, not all response positions were vulnerable to the adversary tactic.

- Likelihood of Exploitability: Level II – Programmatic PD existed for 30 days to a year; Level I – PD not readily observable, predictable, or repeatable (e.g., unknown, contained in SGI procedures, etc.); **Level II**
- IPPP: **Medium** - Multiple (but not full shift complement) armed responders, armed security officers, or alarm station operators unavailable or unable to respond to a contingency event due to failure to be properly qualified (in accordance with the training and qualification plan), availability of response equipment, being out of position, or attentiveness.
- Significance: **Green**

b. Identification of an unanalyzed condition results in a protective strategy change due to the determination that a protected target set component is vulnerable to a DBT tactic. The PD existed for greater than a year but only affected one component of a multi-component target set.

- Likelihood of Exploitability: Level III – Programmatic PD existed for greater than one year; Level I – PD not readily observable, predictable, or repeatable (e.g., unknown, contained in SGI procedures, etc.); **Level II**
- IPPP: **Low** - Previously unidentified or unanalyzed vulnerability in the protective strategy that could allow an adversary to compromise one component of a multi-component target set
- Significance: **Green**

c. Multiple security officers were found to have been assigned to a shift without completing all required training, in accordance with the Training and Qualification Plan, for their assigned responsibilities in accordance with the protective strategy. The officers demonstrated insufficient knowledge, skills, and abilities in an area that significantly affected the licensee's ability to implement their protective strategy. All response positions for a shift were affected by the PD. The officers were on shift for 60 days.

- Likelihood of Exploitability: **Level II** - Programmatic PD existed for 30 days to one year.
- IPPP: **High** - A full shift of armed responders, armed security officers, or alarm station operators unavailable or unable to respond to a contingency event due to failure to perform training (in accordance with the training and qualification plan), availability of response equipment, or attentiveness.
- Significance: **White**

d. The licensee failed to correct a fault in the security power distribution system that could have resulted in an uncompensated loss of the PA perimeter intrusion detection and assessment system upon a loss of offsite power. The deficiency was documented in licensee maintenance records and existed for greater than one year.

- Likelihood of Exploitability: Level III - Significant (i.e., >75%) sections of the PA barrier security detection and assessment system or component with a single point vulnerability; Level III - Programmatic PD existed for greater than one year; Level II -

PD could be identified by personnel with access to the site or licensee procedures; **Level III**

- IPPP: **Medium** - Significant failure of detection or assessment system such that unauthorized persons could enter the protected area undetected.
- Significance: **White**

e. Licensee security officer failed to identify a firearm in a compartment of a contractor vehicle prior to the vehicle entering the PA. The contractor vehicle was escorted by licensee personnel with unescorted access and positive control of the contractor and vehicle was maintained at all times while inside the PA. However, the licensee escort was not aware of the firearm and could not certify positive control of the contraband.

- Likelihood of Exploitability: Level III - Human Performance PD impacted escorted personnel or personnel without UA/UAA (e.g., visitor, vehicle, bulk/hazardous material); Level I - PD was not readily observable, predictable, or repeatable (e.g., unknown, contained in SGI procedures, etc.); **Level II**
- IPPP: **High** - Contraband entered the protected area, or an unauthorized person entered the protected area undetected and uncontrolled.
- Significance: **White**

f. A cyber event or vulnerability was identified on an X-ray system but did not impact the security search functionality of the system, The code had been in place since the last system update that was 2 years before.

- Likelihood of Exploitability: Level I - PD was not readily observable, predictable, or repeatable (e.g., unknown, contained in SGI procedures, etc.); Level III: Programmatic PD existed for greater than one year; **Level II**
- IPPP: **Low** – A cyber event, cyber vulnerability, or failure to implement security controls on a CDA or CDAs that resulted in an unmitigated vulnerability, but the compromise would likely be detected through other established means.
- Significance: **Green**

g. A cyber event or vulnerability that was on the security system for 30 days to a year causing the loss or impairment of a security function such as the video surveillance system causing a reduction in reliability; reduction in ability to detect, delay, assess or respond to malevolent activities; reduction of ability to call for or communicate with offsite assistance; or the reduction in emergency response ability to implement appropriate protective measures in the event of a radiological emergency.

- Likelihood of Exploitability: **Level II** - Programmatic PD existed over one year.
- IPPP: **High** – Then condition resulted in a delayed ability to detect and respond to the cyber compromise
- Significance: **White**

0609EI-10 REFERENCES

IMC 0308, Attachment 3, Appendix E, “Technical Basis for the Baseline Security Significance Determination Process”

IMC 0609, Attachment 4, “Phase 1 – Initial Screening and Characterization of Findings”

IMC 0612, Appendix B, “Issue Screening Directions”

NRC Enforcement Policy

Regulatory Guide 5.79, “Protection of Safeguards Information”

END

Figures:

1. Baseline Security Significance Determination Process Flowchart
2. Material Control and Accounting Significance Determination Process Flowchart
3. Decision Tree for Unsecured SGI
4. Unattended Opening Significance Determination Process Flowchart
5. Target Set Significance Determination Process Flowchart
6. Baseline Security Significance Determination Flowchart

Attachment:

1. Revision History for IMC 0609, Appendix E, Part I

Figure 1: Baseline Security Significance Determination Process Flowchart

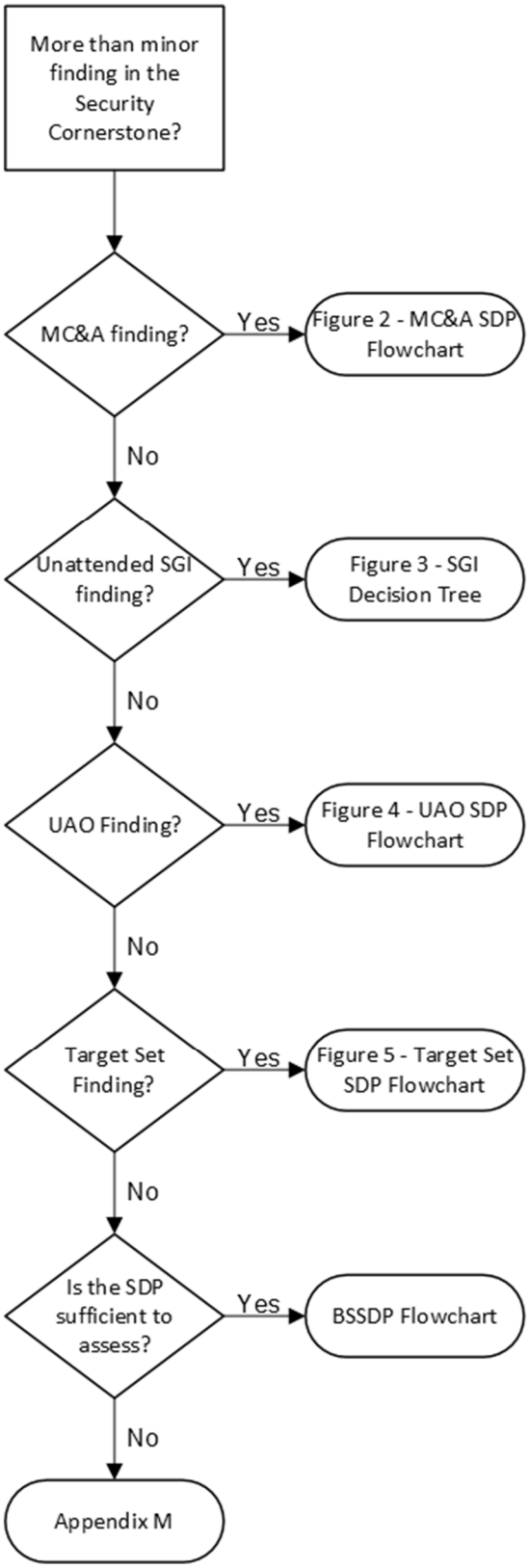


Figure 2: Material Control and Accounting Significance Determination Process Flowchart

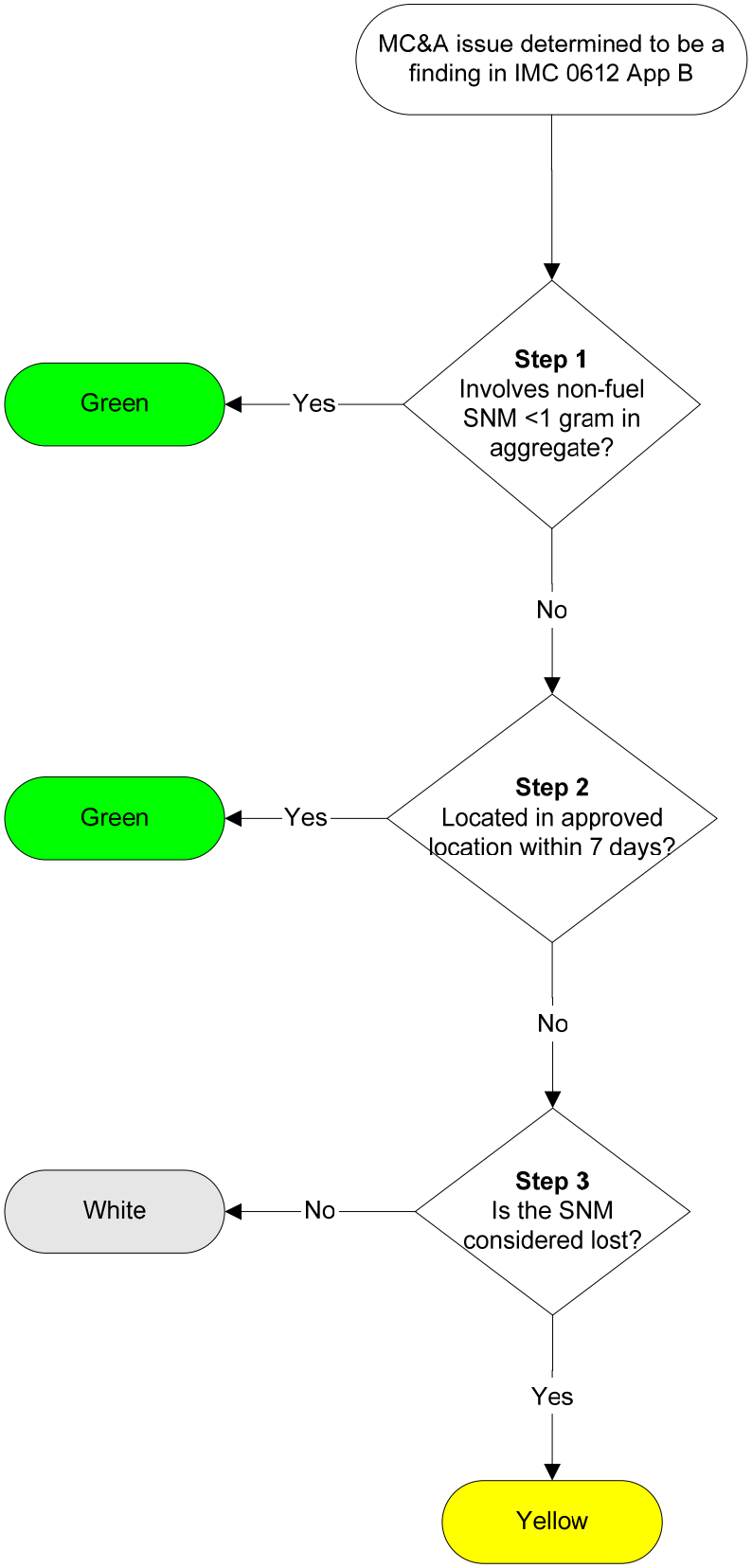


Figure 3: Decision Tree for Unsecured Safeguards Information

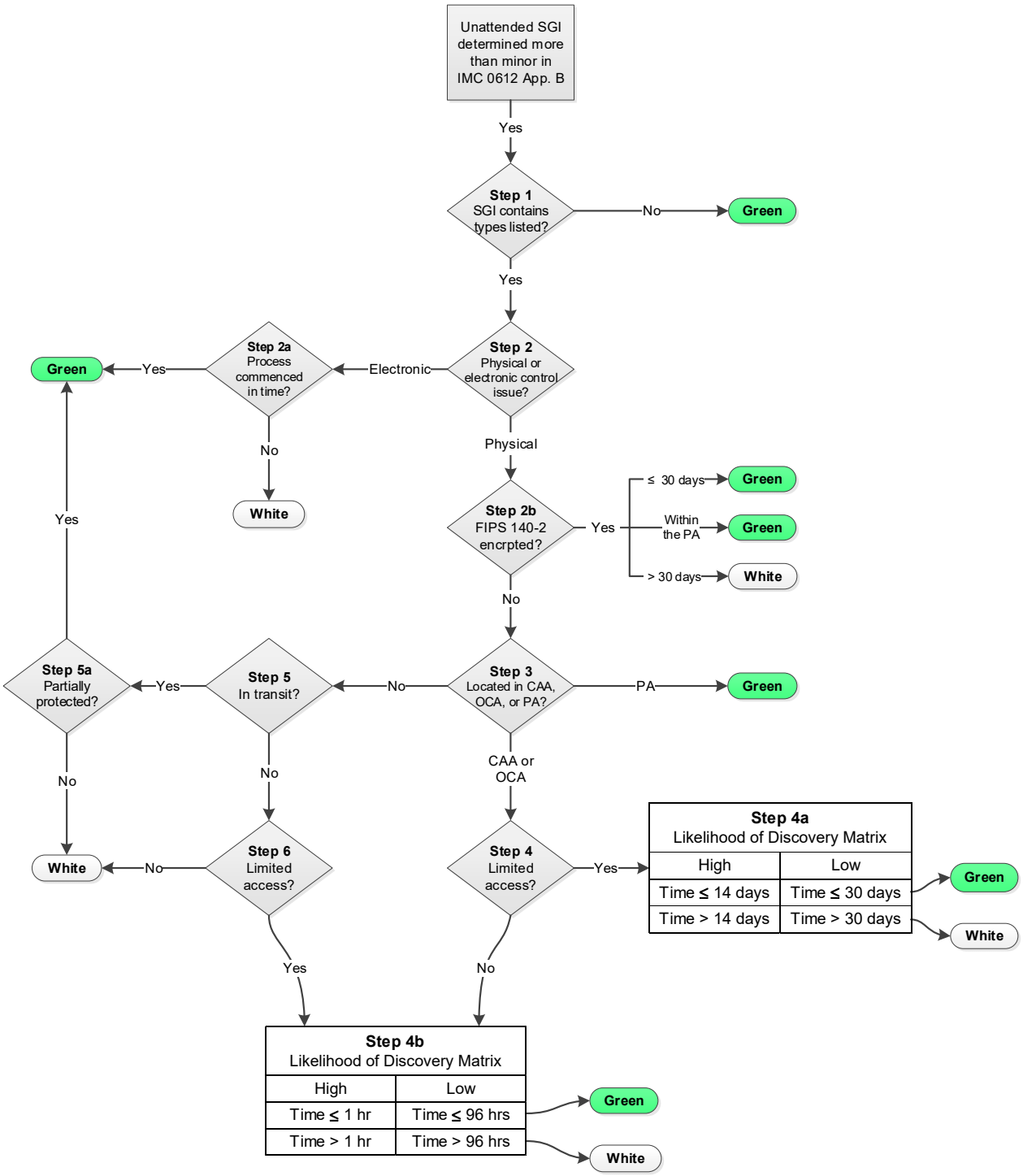


Figure 4: Unattended Opening Significance Determination Process Flowchart

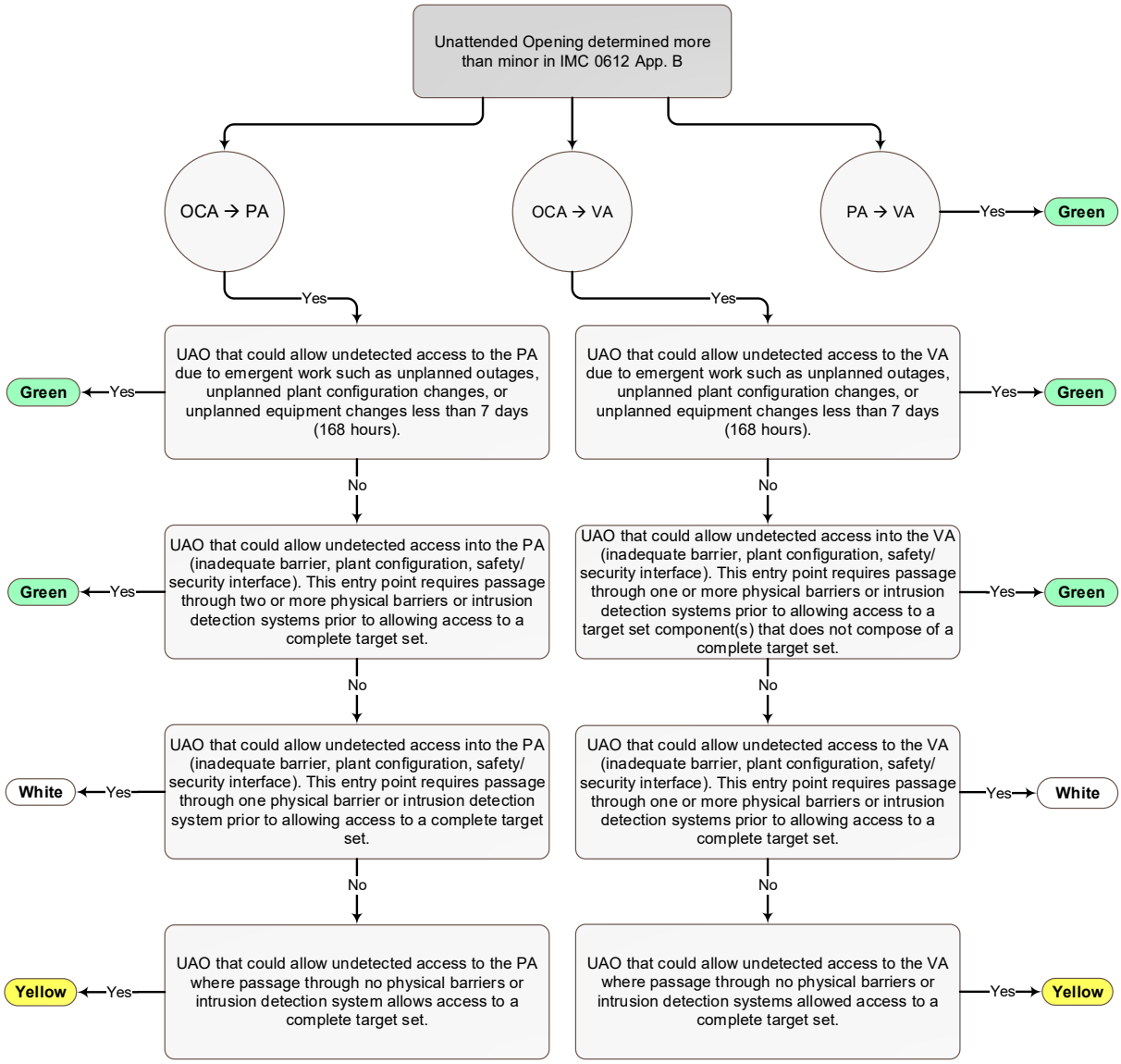


Figure 5: Target Set Significance Determination Process Flowchart

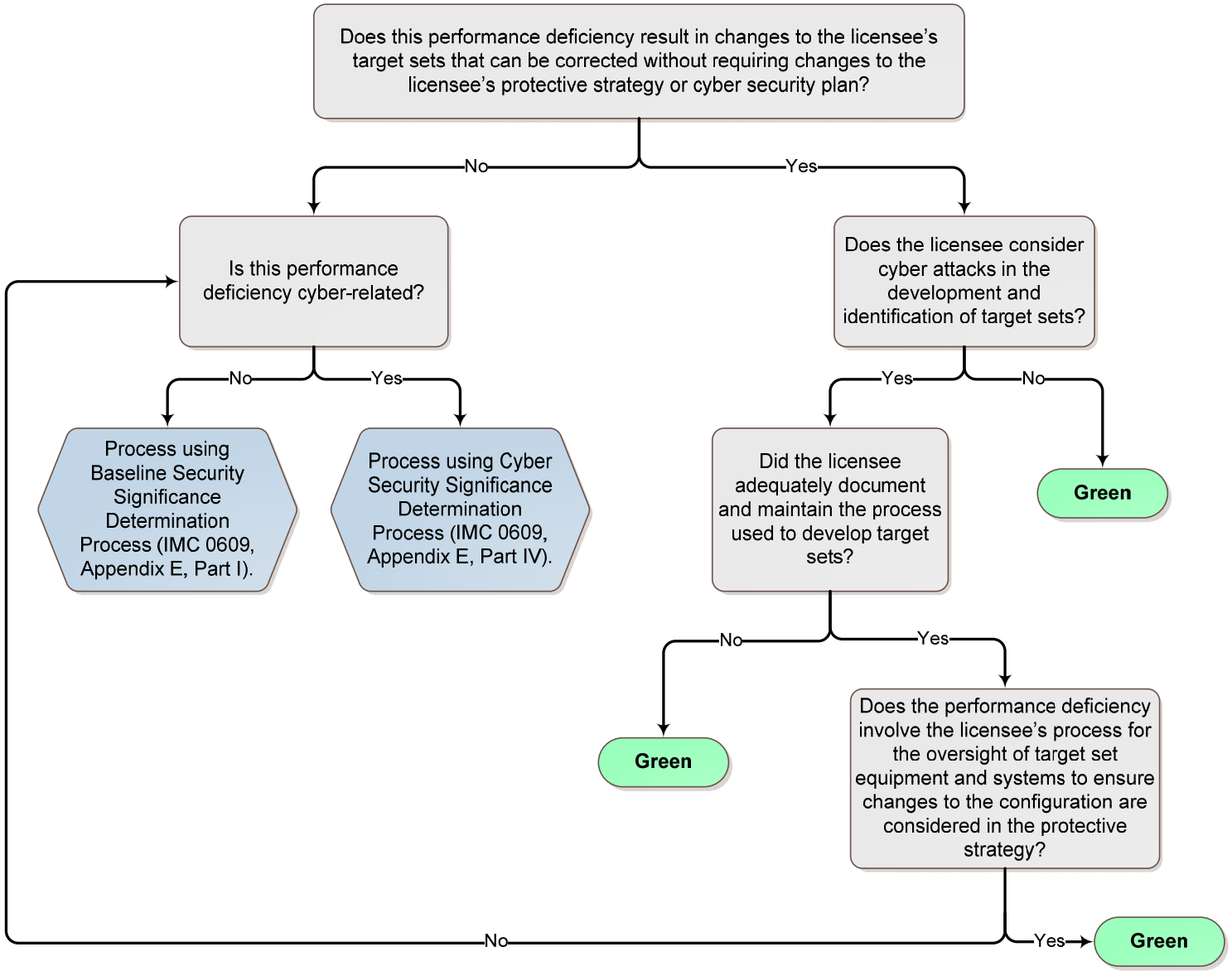
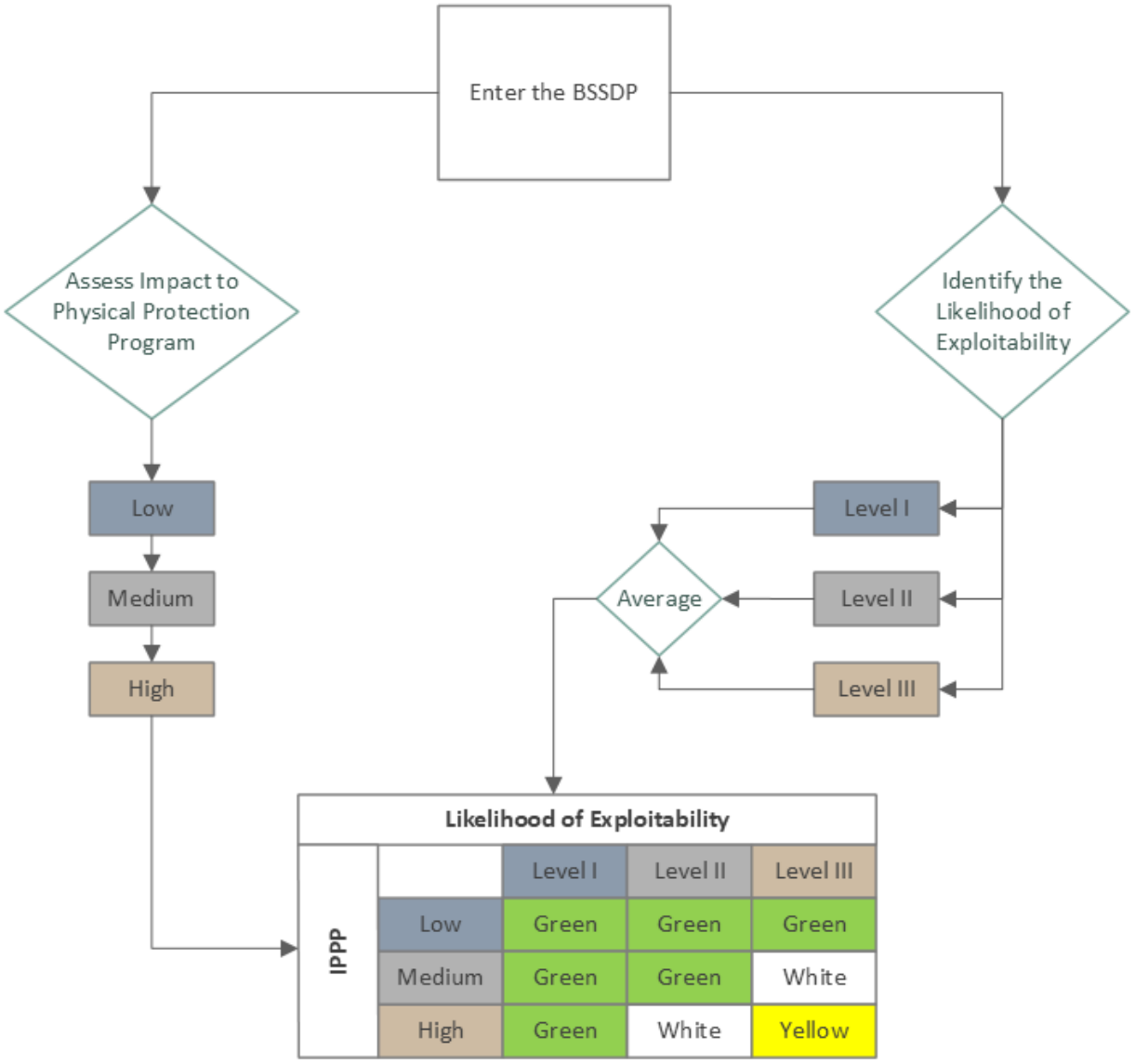


Figure 6: Baseline Security Significance Determination Flowchart



Attachment 1: Revision History for IMC 0609, App. E, Part I

Commitment Tracking Number	Accession Number Issue Date Change Notice	Description of Change	Description of Training Required and Completion Date	Comment Resolution and Closed Feedback Form Accession Number (Pre-Decisional, Non-Public Information)
N/A	09/25/06	Researched commitments back four years - none found.	N/A	N/A
N/A	09/25/06 CN 06-025	1) Updated guidance to add minor wording revisions. 2) Added additional Program elements to the Physical Protection SDP Worksheet.	N/A	None
N/A	ML083120269 12/04/08 CN 08-034	Changed the name of the IMC to Baseline Security SDP; revised the description of the SFRP; corrected Figure 3 to include Section A; and incorporated the MC&A key attribute. W200500185 is the ticket associated with this revision.	N/A	ML083120442
N/A	ML093491010 01/27/10 CN 10-003	Enhanced the Baseline Security SDP by Incorporating a decision tree for unsecured safeguards information findings and a significance screen for physical protection findings. Also, reordered the sections in the IMC to follow the Figure 1 Baseline Security SDP Flowchart.	N/A	ML093491015
N/A	ML11081A001 06/27/12 CN 12-011	Incorporates changes to the SGI tree and the Significance Screen, based on feedback from use of these tools. Editorial changes to improve readability and usability.	N/A	ML12170A803 Closed FF: 0609E1-1726 0609E1-1727 0609E-1707

Commitment Tracking Number	Accession Number Issue Date Change Notice	Description of Change	Description of Training Required and Completion Date	Comment Resolution and Closed Feedback Form Accession Number (Pre-Decisional, Non-Public Information)
N/A	ML11081A001 06/27/12 CN 12-011	Incorporates changes to the SGI tree and the Significance Screen, based on feedback from use of these tools. Editorial changes to improve readability and usability.	N/A	ML12170A803 Closed FF: 0609E1-1726 0609E1-1727 0609E-1707
N/A	ML14007A469 01/15/14 CN 14-002	Revised Figure 5 to increase clarity for inspector use by providing separate Figures for each attribute. Revised numbering in program element boxes in Figures 5, 6, 7, & 8 to align with revisions to the baseline inspection procedures.	N/A	
N/A	ML14322A904 10/26/15 CN 15-021	Incorporated revised unattended opening significance determination process flowchart. Additionally, revised significance screen entry criteria for clarification. Completed editorial revisions in accordance with IMC 0040.		ML15238B622 Closed FF: 0609EP1-1978
N/A	ML16252A303 09/08/2016 CN 16-024	Revised to reflect minor editorial changes on pages 13 and 14 for clarity and alignment consistent with Figure 5-Unattended Opening Flowchart on page 23.	N/A	ML16256A114

Commitment Tracking Number	Accession Number Issue Date Change Notice	Description of Change	Description of Training Required and Completion Date	Comment Resolution and Closed Feedback Form Accession Number (Pre-Decisional, Non-Public Information)
N/A	ML18164A326 09/17/18 CN 18-032	This document has been revised in response to Staff Requirements – SECY 16-0073 (Options and Recommendations for the Force-On-Force Inspection Program) and the March 2017 Assessment Team (Regions and HQ) review for redundancy's and efficiencies of the 71130 series IPs for power reactors. Specifically this revision included a change to the Safeguards Decision Tree for consistency with the changes to the enforcement policy regarding the protection of classified information; clarified the entry criteria and modified the significance ranking criteria of the Significance Screen: added additional screening criteria to the Unattended Opening Flowchart and; removed targets from the significance screen and created a target set flowchart. All SDP changes made during this revision were based on the objective of increasing clarity, consistency, and predictability. Upon completion of a SUNSI review, the staff concluded that this document should be de-controlled. Consistent with the staff's SUNSI determination, this document has been de-controlled and the SUNSI markings have been removed. Consistent with COMSECY-16-0022, "Proposed Criteria for Reactor Oversight Process Changes Requiring Commission Approval and Notification" this revision met the criteria for the submittal of a Commissioners Assistant (CA) Note. The CA Note (ML18165A297 dated 7/30/2018) was submitted to the Commissioners Assistant's informing the Commission of the SDP changes.	N/A	ML18240A366 0609E1-2090 ML18255A033 0609EP1-2221 ML18255A033

Commitment Tracking Number	Accession Number Issue Date Change Notice	Description of Change	Description of Training Required and Completion Date	Comment Resolution and Closed Feedback Form Accession Number (Pre-Decisional, Non-Public Information)
N/A	ML22178A222 11/08/22 CN 22-025	This document was revised to align the IP requirements listed in figures 7, 8, 9, and 10 with the current IP requirements in IP 71130 and its associated attachments. The assessment table depicted in figure 11 was revised to account for the changes to figures 7, 8, 9, and 10. Minor editorial changes were made throughout the document consistent with NRC writing style guidance.	N/A	ML22178A221
N/A	ML25168A178 XX/XX/XX CN 25-xxx	This document was revised to reduce subjectivity, add risk insights, and achieve greater consistency in inspection findings. The significance screen and BSSDP flowchart were removed and replaced with the revised section 8.		