BASELINE SECURITY SIGNIFICANCE DETERMINATION PROCESS FOR POWER REACTORS

Effective Date: September 21, 2018

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 has been evaluated as more than minor using Inspection Manual Chapter (IMC) 0612, Appendix B, "Issue Screening," 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 Significance Screen. The significance screen process is depicted in Figure 4. It is used to augment the BSSDP by using a set of selected events that share common characteristics and the impact on the physical protection program/time analysis tool.

01.05 Unattended Opening (UAO). 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." 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.

01.06 Target Sets. The flowchart depicted in Figure 6 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 baseline worksheets 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.

01.07 BSSDP Flowchart. The BSSDP includes the following attributes: access authorization, access control, physical protection system, and contingency response.

a. Figures 7, 8, 9, and 10 are the worksheets that are used to evaluate the impact areas, key attributes, and program elements pertaining to physical protection obtained from the security cornerstone and the applicable security baseline inspection procedures. The worksheet identifies the layers of protection defined in the defense-in-depth concept (owner controlled area (OCA), protected area (PA), and vital areas (VAs)), identifies the key attributes impacted, and categorizes the program elements (Tier I, Tier II, and Tier III) based on their importance to the overall effectiveness of physical security.

b. The Figure 11 assessment table is used to quantify the significance of the finding by evaluating the impact areas, key attributes, and program elements impacted by the finding. The relationship between the total number of program elements affected under each tier and impact areas yields a value that is proportional to the significance of the finding. The assessment table characterizes the security significance of the inspection finding by providing an objective and common framework allowing for a predictable and repeatable assessment.

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).

Impact Areas – Layers (OCA, PA, and VA) of security which support the licensee's defense against the design basis threat.

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.

Key Attributes – Characteristics (access authorization, contingency response, access control, and physical protection) of the Security cornerstone that are critical for the licensee to maintain in order to defend against the DBT through implementation of NRC requirements.

Program Elements – Inspection areas that are included in the security baseline inspection procedures (IP 71130 and its attachments). The areas are reflective of the defense-in-depth aspects of the licensee's security plans.

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.

Tier – A categorization process based on each program elements importance to the overall physical security effectiveness as part of the NRC's regulatory requirements.

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." 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 performance deficiencies 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.

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," 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 performance deficiency. The performance deficiency 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 performance deficiency 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:

a. The area was locked or had 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 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.

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

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

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

viii. 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 SIGNIFICANCE SCREEN FOR PHYSICAL PROTECTION (Figure 4)

Any finding that involves the attributes of Physical Protection will initially be processed using the Significance Screen for Physical Protection, Figure 4.

06.01 Determine if the finding involves one or more of the entry criteria:

a. Failure to identify a firearm, explosive, incendiary device, or other item that could be used to commit radiological sabotage during a search for such material and the material entered the Protected Area;

b. Unsearched (or partially searched) vehicle where the unsearched portion could carry an explosive of relevant TNT equivalent inside one or more calculated safe standoff distances for that TNT equivalent blast;

c. Multiple officers who are either armed responders or armed security officers or are performing physical protection program functions (e.g., search functions, access control functions, or compensatory measures), were found simultaneously inattentive; or

d. An actual event (not a potential event) that resulted in a degraded or inoperable security system that could have allowed unauthorized, undetected access, where licensee testing and maintenance processes failed to identify the degradation or inoperable condition (i.e., a system that was not adequately designed, installed, or not maintained or tested in a manner where it is capable of performing its intended function). In certain instances, a licensee may have previously identified a degradation of the security system; however, the licensee failed to perform timely or adequate corrective actions that prevented an actual failure of the system that could allow unauthorized or undetected access following identification. In this case the finding would meet significance screen entry criteria. A failure of a single component would not constitute a system failure, unless that component was integral to a larger system (e.g., a central alarm station (CAS)/secondary alarm station (SAS) computer system or a multiplexer).

This initial decision will result in either the finding meeting one of the above criteria, which would then require proceeding to Section 06.02, or the Significance Screen Process would not be applicable and the finding would be evaluated by the UAO flowchart (Figure 5), the Target Set flowchart (Figure 6) or the BSSDP flowcharts (Figures 7, 8, 9, and 10.)

06.02 Determine the impact the finding has on the physical protection program.

This step evaluates the conditional risk associated with the performance deficiency's impact on the physical protection program. The examples that are provided in the table to assist staff identification of each consequence are not an all-inclusive list.

Table 1: IMPACT TO THE PHYSICAL PROTECTION PROGRAM (IPPP)
Low • An unsearched (or partially unsearched) vehicle identified within the analyzed safe standoff distance for either the CAS, SAS, or multiple armed responders, as described in the DBT for a coordinated external assault. Medium • A deficiency or deficiencies in the design and maintenance of detection equipment resulting in an uncompensated loss of portions of the PA perimeter IDS. • An unsearched (or partially unsearched) vehicle identified within the analyzed safe standoff distance for protected target set components that do not comprise a complete or standalone target set, as described by the DBT. High • An unsearched (or partially unsearched) vehicle discovered within the analyzed safe standoff distance for a standalone target or protected target set components that constitute a complete target set, as described by the DBT. • A licensee's search fails to detect a firearm, explosive, incendiary device, or other item that could be used to commit radiological sabotage.

Table 1: IMPACT TO THE PHYSICAL PROTECTION PROGRAM (IPPP)
• A deficiency or deficiencies in the design and maintenance of detection equipment resulting in an uncompensated loss of all PA perimeter IDS. • Multiple inattentive officers.

06.03 Determine the duration that the deficiency existed.

Evaluate 1 year prior to the last occurrence of the deficiency (i.e., the time when the licensee failed to search a vehicle or failed to identify a firearm during a search process). Note that this is a calculation of time that the licensee is exposed to the vulnerability associated with the finding, which may be less than the total time the non-compliance existed. For example, if a licensee fails to search a vehicle, the vulnerability exists while the unsearched vehicle is within the explosive minimum standoff distance. However, if the performance deficiency is incorporated into the licensee's operating procedures and processes, and as a result is predictable and identifiable through surveillance of licensee activities, then consider the total time the non-compliance existed.

06.04 Combine IPPP and time to arrive at a significance determination.

Using the duration of the finding, apply that period to the IPPP/Time Matrix of Figure 4 to arrive at the significance of the finding.

0609EI-07 EVALUATING UNATTENDED OPENING FINDINGS (Figure 5)

07.01 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.

07.02 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, man hole in the OCA that leads to PA or VA, tunnel, etc.) which an adversary would enter to defeat the UAO (e.g., 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 barriers 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 consistent with the manufactures specification, and is compensated for when not in service.

07.03 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-08 EVALUATING TARGET SET FINDINGS (Figure 6)

In evaluating target set findings, use Figure 6, Target Set SDP flowchart:

08.01 Does this performance deficiency 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 08.03.

If no, and a change to the licensee's protective strategy or cyber security plan is required, then go to 08.02.

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 position as either an initial position or an automatic redirect,

d. Assignment of timeline to an armed security officer,
e. Modification of barriers to increase adversary delay, or
f. Additional credited operator action to existing target sets.

08.02 Is this performance deficiency cyber-related?

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, including target sets, 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).

If yes, then process the finding in accordance with the cyber security SDP worksheets described in IMC 0609, Appendix E, Part IV, "CYBER SECURITY SIGNIFICANCE DETERMINATION PROCESS FOR POWER REACTORS." Cyber-related indicates a target set element, or function of the target set equipment or element, that are critical digital assets.

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

If the licensee considers cyber-attacks, then go to 08.04.

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).

08.04 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 08.05.

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 are not 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).

08.05 Does the performance deficiency 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 08.02.

0609EI-09 EVALUATING FINDINGS USING THE BASELINE SECURITY SIGNIFICANCE DETERMINATION FLOWCHART PROCESS

Upon entering the BSSDP Flowcharts, first determine if the finding impacted portions of the defense-in-depth provided by the OCA, PA, or VAs and could adversely impact the key attributes (access controls, physical protection, access authorization, and contingency response).

If it is determined that the finding impacts the OCA, PA, or VA and impacts one or more key attributes, the analysis will require the staff to determine the effect on the program elements required by Commission regulations or orders. The number of key attributes affected by the finding and the impact the finding has on one or more of the program elements directly affect the licensee's ability to ensure the common defense and security of its facility. Therefore, the significance of the finding will range from very low security significance, a Green finding, to high security significance, a Red finding. The process for determining significance incorporates the following:

09.01 Determine the impact area. Determine if the finding impacts the OCA, PA, or VA area, or any combination thereof by using the maximum possible effect to an impact area and the total number of key attributes impacted.

When characterizing a finding, the information must be sufficient to determine if findings associated with programs, procedures, or personnel failures could allow access or impact an area (e.g., could the finding impact the OCA, PA, or VA) with no intervening action (e.g., defense-in-depth). Whether or not an individual actually accessed an area or a breach of an area actually occurred, is irrelevant to the security programs inability to prevent the deficiency.

During the development of the BSSDP, the staff developed several scenarios that conveyed the same or similar circumstances as the example below.

Example**:** Based on the work activity and limited background information available for a contractor, the licensee determined that the individual should only be allowed limited authorized site access to the OCA. However, due to a process deficiency, the licensee mistakenly granted the individual full authorized site access to the OCA, PA, and VA. The individual retained this status for 1 week before the mistake was identified and corrective action taken. However, the licensee was able to verify that, while on site, the individual never left the OCA and, therefore, never entered the PA or VA.

In this example, the facts clearly reflect that the licensees program and processes allowed the individual to mistakenly receive full authorized site access to the OCA, PA, and VA; therefore, the BSSDP would identify the VA as the most significant area of impact.

It could be suggested if the licensee was able to verify that the individual never left the OCA, then the OCA should be the area of impact. However, there were no programs, procedures, personnel, equipment, or barriers in place that would have prevented the individual from choosing to enter the PA or VA once the individual received full site access. Therefore, the finding is more significant, regardless of whether or not an individual actually entered the PA or VA, because the potential existed and nothing within the licensee's protective strategy would have prevented the individual from doing so, once the licensee improperly granted the individual access.

Therefore, it must be emphasized that when an inspector uses the BSSDP to characterize a finding, the inspector must consider all of the facts associated with the finding. In addition, these facts must be sufficient to demonstrate that, while a deficiency existed, there were no adequate programs, procedures, personnel, equipment, or barriers in place and designed to prevent a potential adversary from taking advantage of vulnerabilities in the security plan, equipment, or performance.

09.02 Determine the Affected Program Elements. Determine the finding's impact on the total number of program elements under each tier, which are obtained from the baseline inspection procedures and guidance required by Commission regulations. (Reference Figure 7 which includes direct reference to inspection requirements. Those references that do not include sub levels (e.g., a, b, c, etc.) refer to all of the inspection requirements in the referenced section).

In determining the affected program elements, evaluate the degraded condition. The term "degraded condition" is intended to describe a reduction in the security of the reactor plant, or other attributes. In determining the affected program elements, evaluate the degraded condition associated with the specific PD being evaluated. This would be the PD that was the proximate cause of the degraded condition. Even if the degraded condition results in other potential violations, the SDP is focused on the PD that caused the degraded condition. Example: An access control related PD results in allowing access to unauthorized individual into the PA. Elements associated with the proximate cause (access control, such as failure to identify or failure to check PADS) should be considered for elements in this SDP. Elements associated with other resulting violations (AA, such as individuals in the PA that didn't meet AA requirements) would not be considered if they were not associated with the proximate cause PD (there was no failure or PD in implementation of the AA program).

The program elements for psychological testing, credit history review, and reviewing official's determination in granting unescorted access are duplicated within the three tiers in Access Authorization. Determine which tier by the following:

a. Tier I: finding is related to initial access authorization.

b. Tier II: finding is related to reinvestigation.

c. Tier III: finding is more than one incorrect determination related to reinvestigation.

09.03 Determine the point value of the finding. Once the effects on the impact area, the total number of key attributes, and the total number of program elements have been identified, add up the total number of points across all attributes and tiers.

09.04 Correlate the point value to a significance color. The BSSDP assessment table will then establish a color finding by combining a quantitative and algorithmic approach which proportionally relates the total number of program elements impacted under each tier to the area affected.

If it is determined that the finding could not impact the defense-in-depth provided by the OCA, PA, or VA, or that none of the key attributes were impacted, the analysis will require the staff to determine if the finding could result in a condition in which a potential adversary is able to defeat, circumvent, or otherwise take advantage of a vulnerability in a security plan, equipment or performance to determine the security significance of the finding (Figures 7, 8, 9, and 10).

09.05 Step-by-step example. The following is a step-by-step evaluation of a typical security inspection finding that demonstrates how the baseline BSSDP is to be used in determining the significance of findings.

An NRC security inspector identified a performance deficiency with the licensee's weapons training. The inspector determined that the licensee's qualification course for the new contingency weapon was inadequate because it did not include an appropriately sized target to demonstrate acceptable performance. The inspector determined that all members of the security force had received the inadequate formal training. Subsequent testing, using an appropriately sized target, determined that 10 security officers assigned to shifts as armed responders did not meet the qualification requirements.

The failure to provide adequate training to ensure the qualification of security force personnel involves: (1) personnel assigned to VAs and affected the initial training, training plan and implementing procedures, and firearms familiarization training elements of the physical protection key attribute; and (2) the protective strategy and protective strategy assessment elements of the contingency response key attribute.

a. Determine if the finding could result in an impact to the defense-in-depth provided by the OCA, PA, or VA. (Figures 7, 8, 9, and 10)

   It was determined that the finding involves personnel assigned shifts in all impact areas (OCA, PA, and VA).

b. If the response in Step 09.05.a is "Yes," determine if the finding impacts one or more of the key attributes.

   It was determined that the finding involves the following key attributes:
   Physical Protection and Contingency Response.

c. Determine the impacted area using the maximum possible affected area.

It was determined that the VA was the impacted area resulting in the maximum possible impact.

d. Within each impacted key attribute, identify the program element(s) impacted within each tier.

Physical Protection key attribute:
Tier I - Day and night fire qualification (71130.07-02.03)
Tier II – Training and qualification plan and implementing procedures (71130.07-02.05)

e. Input the impacted area into the window located into the BSSDP Assessment Table, Figure 7.

Impact area = VA

f. Input the total number of program elements associated with the appropriate key attribute and tier into the BSSDP Assessment Table, Figure 11.

Physical Protection key attribute
Tier I - Input 1 program elements impacted
Tier II -Input 1 program element impacted

g. Once the impacted area and total number of program elements impacted have been input into the BSSDP Assessment Table, the significance is assessed by combining a quantitative and algorithmic approach that proportionally relates the total number of program elements impacted under each tier to the area infiltrated. This process is repeated for each key attribute. If no program elements were impacted under a key attribute, it is assumed that the value will yield zero.

After the weighted values (derived from pairing rows with columns) are obtained by using the matrix in Figure 11, a subtotal is calculated for each key attribute thus resulting in a total. The total is the number used to determine the significance (Green, White, Yellow, or Red) to the finding by determining what range of parameters it falls into as shown in Figure 11.

Note that there may not be a corresponding one-for-one relationship between the total number of program elements impacted and the resulting subtotal from the assessment table in all cases.

i. Physical Protection key attribute
Tier I – [Rows: Columns] = [VA: 1 program element impacted] = 2
Tier II – [Rows: Columns] = [VA: 1 program element impacted] = 1

ii. The BSSDP Assessment Table yields the following values:
Subtotal for Physical Protection = 2 + 1 = 3
Total for the issue screened = 3 (Green)

0609EI-10 REFERENCES

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

IMC 0612, Appendix B, “Issue Screening”

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

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. Significance Screen Process
5. Unattended Opening Significance Determination Process Flowchart
6. Target Set Significance Determination Process Flowchart
7. Baseline Security Significance Determination Process Worksheet, “Access Authorization”
8. Baseline Security Significance Determination Process Worksheet, “Access Control”
9. Baseline Security Significance Determination Process Worksheet, “Physical Protection”
10. Baseline Security Significance Determination Process Worksheet, “Contingency Response”
11. Baseline Security Significance Determination Process Assessment Table

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

Figure 1 – Baseline Security Significance Determination Process Flowchart

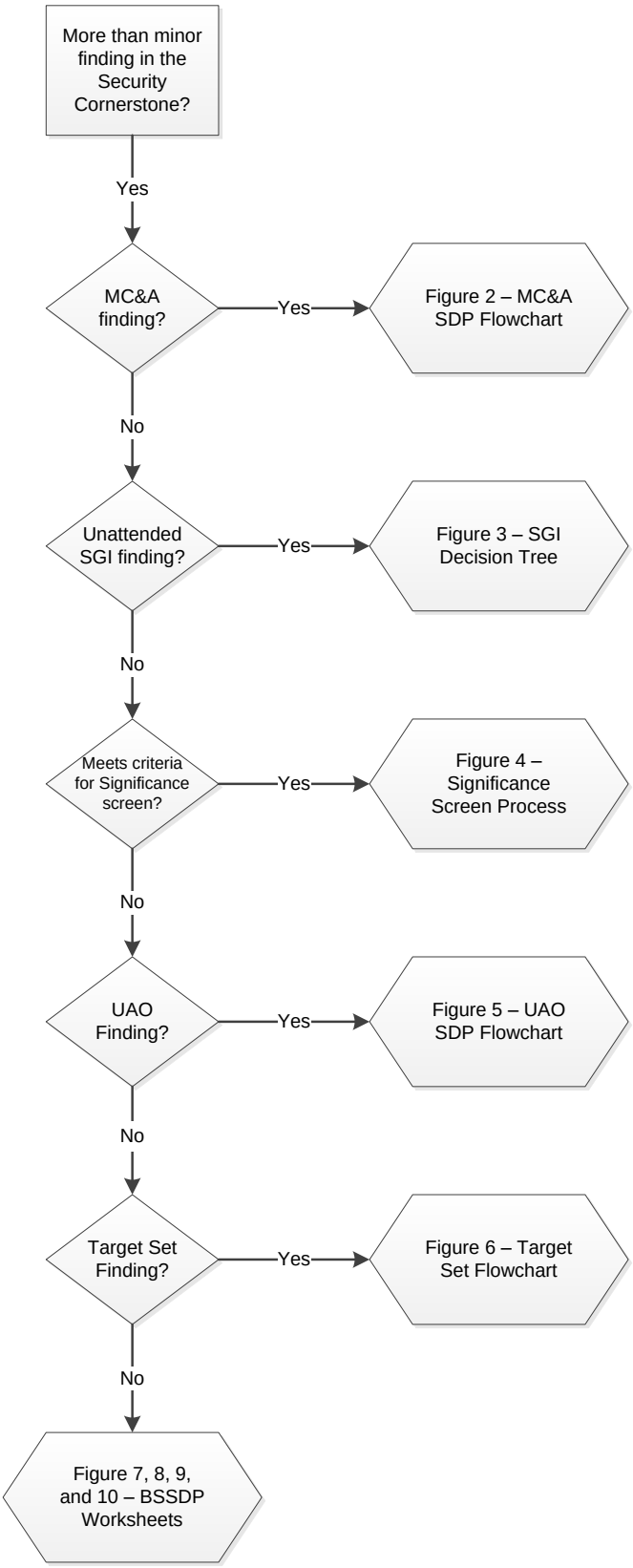


Figure 2 – Material Control and Accounting Significance Determination Process Flowchart

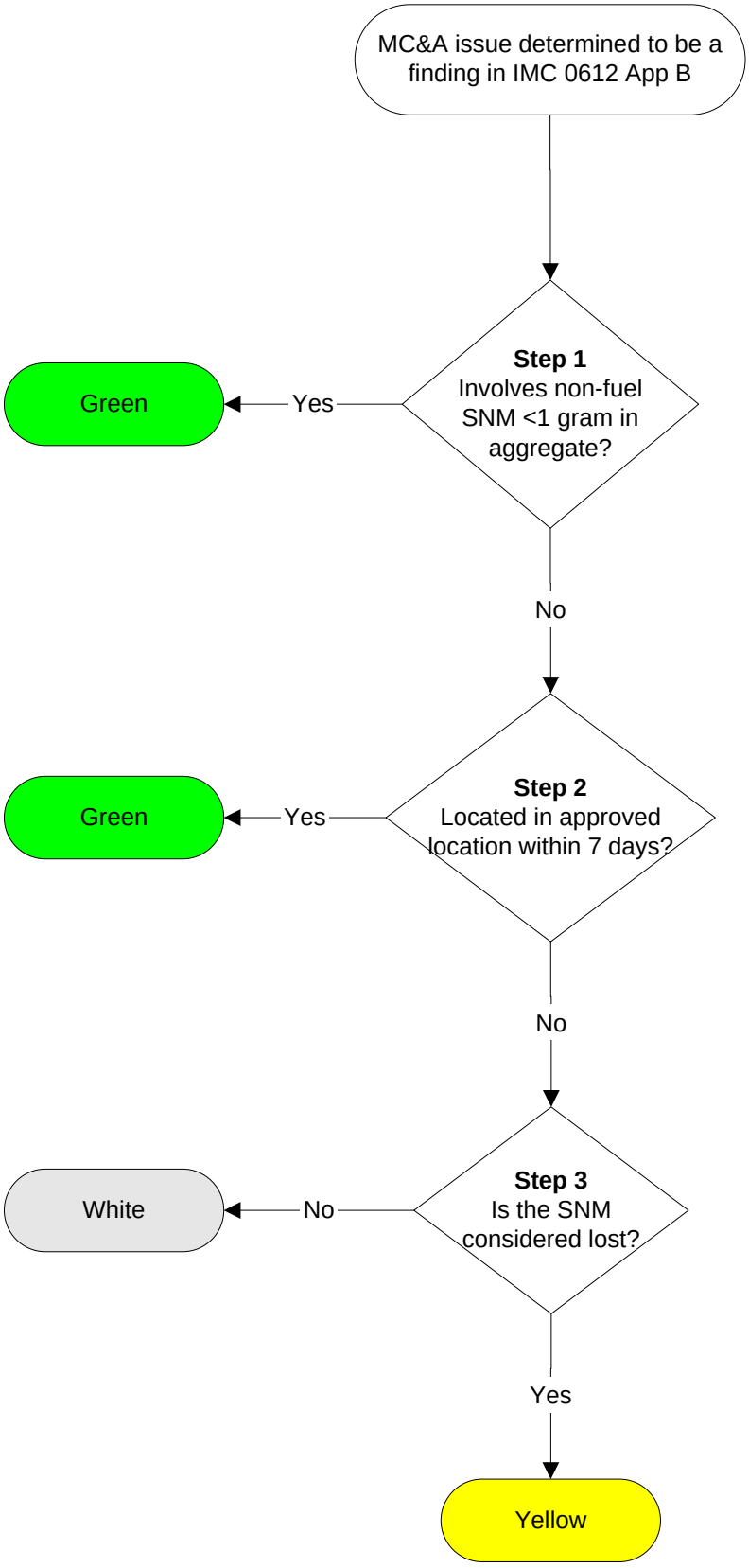


Figure 3 – Decision Tree for Unsecured Safeguards Information

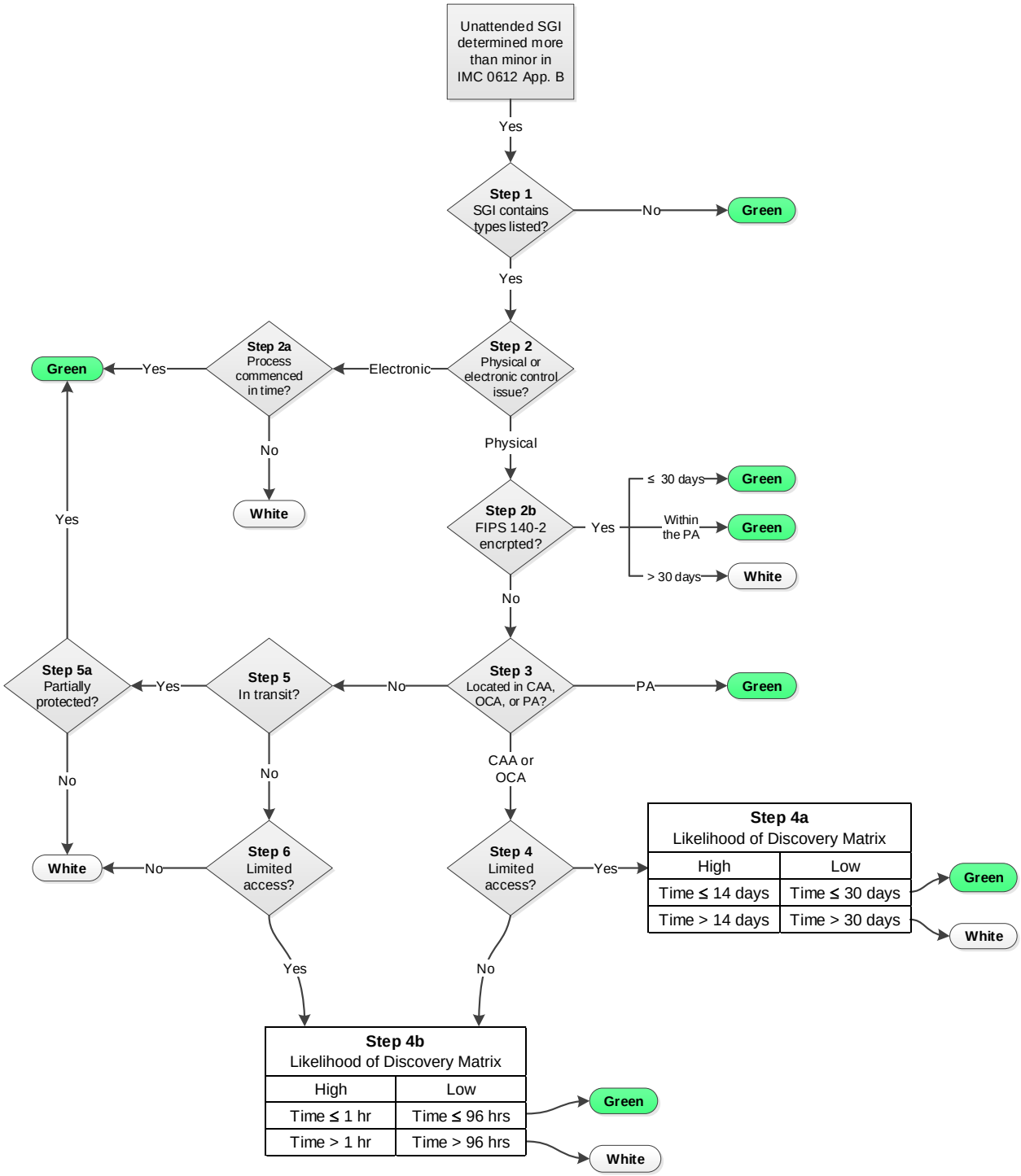
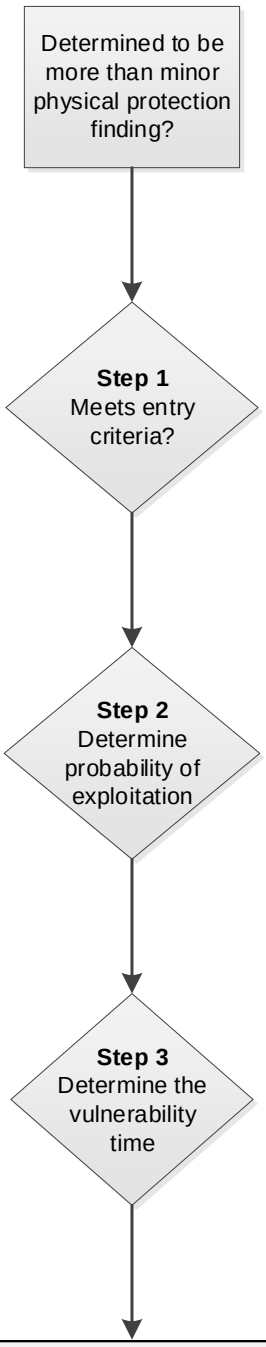


Figure 4 – Significance Screen Process



Step 4 Impact to Physical Protection Program/Time Matrix			
	High	Medium	Low
< 30 Days	WHITE	GREEN	GREEN
< 1 Year	WHITE	WHITE	GREEN
≥ 1 Year	YELLOW	WHITE	WHITE

Figure 5 – Unattended Opening Significance Determination Process Flowchart

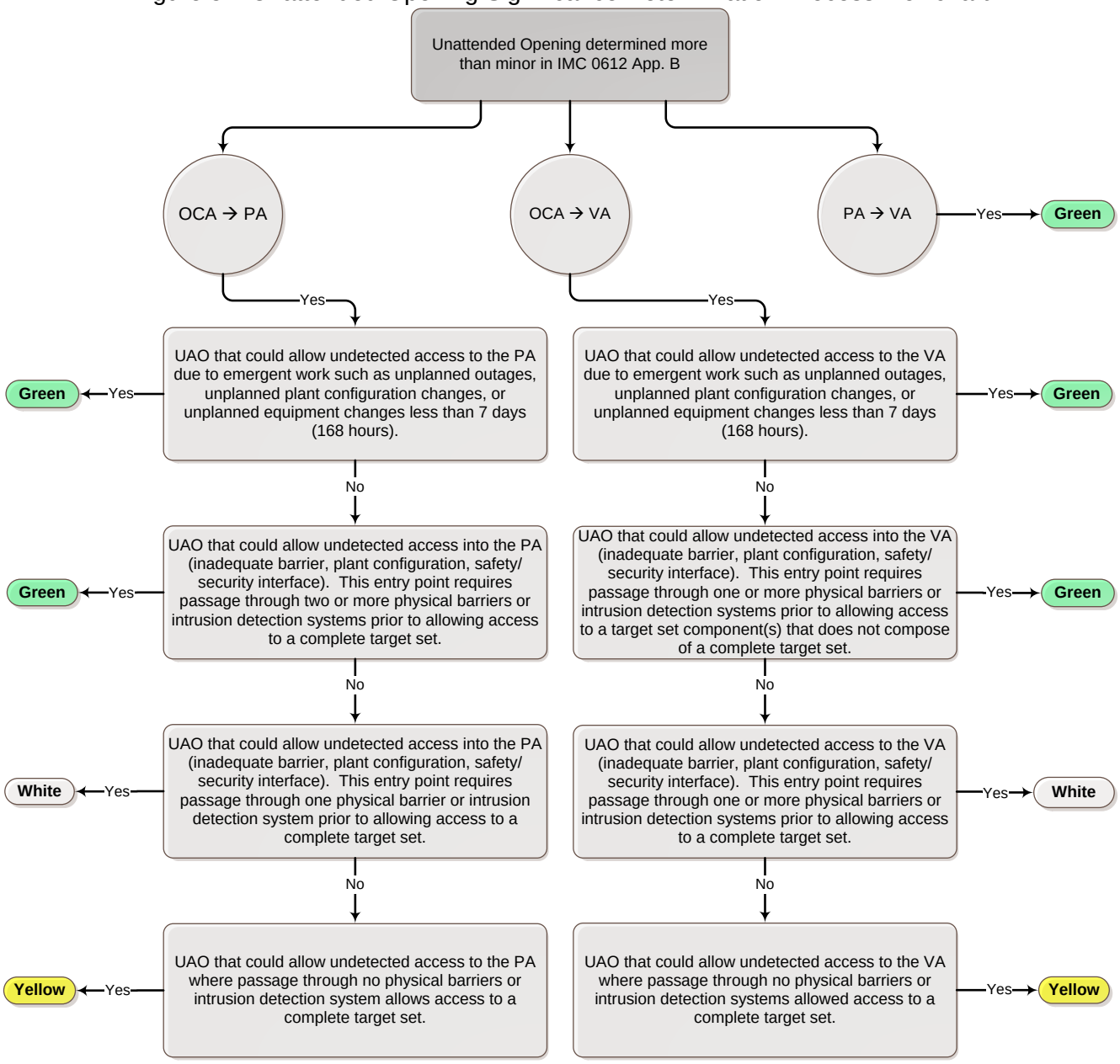


Figure 6 – Target Set Significance Determination Process Flowchart

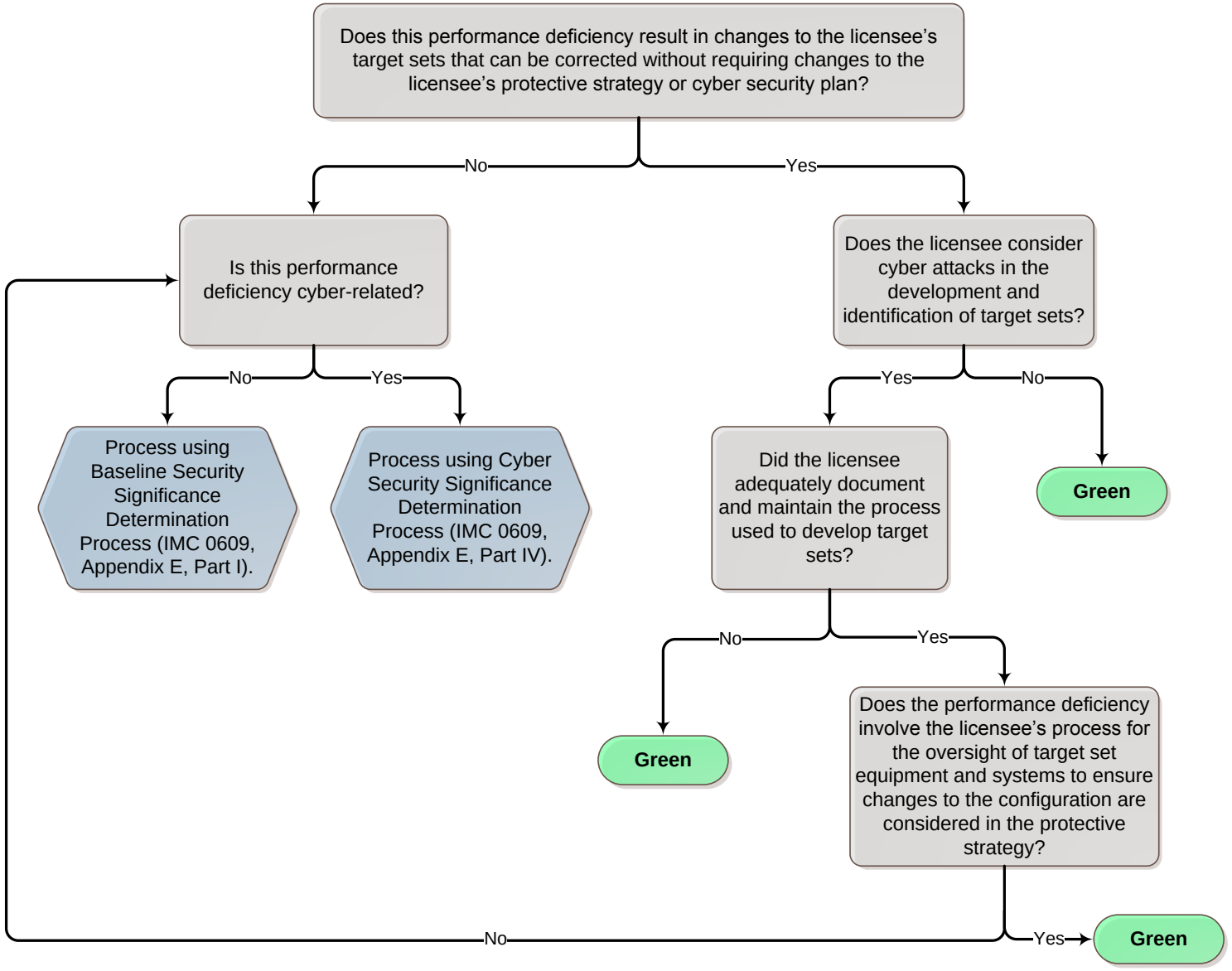
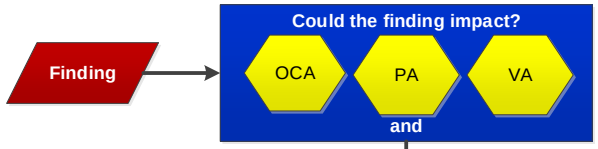


Figure 7 - Baseline Security Significance Determination Process Worksheet, “Access Authorization”



Finding impacts the Access Authorization attribute?

Tier I	
Implementing Procedures (01-02.01.a)	Granting Unescorted Access (01-02.02.e)
Implementing Procedures (01-02.01.b)	Information Sharing (01-02.04.a,b)
Implementing Procedures (01-02.01.c)	Reinvestigations (01-02.02.j)
Granting Unescorted Access (01-02.02.a)	Insider Threat and Mitigation (01-02.03.b,c)
Granting Unescorted Access (01-02.02.b,c,d)	Insider Threat and Mitigation (01-02.03.d)
Granting Unescorted Access (01-02.02.i)	Insider Threat and Mitigation (01-02.03.e)
Granting Unescorted Access (01-02.02.k)	Behavior Observation Program (01-02.03.a)
Granting Unescorted Access (01-02.02.f,g,h)	Behavior Observation Program (08-02.03.a,b)
Policy and Procedures (08-02.01.a) Test Results Reviews (08-02.02.a)	SAE Interviews (08-02.04.a,b,c)

Tier II	
Implementing Procedures (01-02.05.a,b,c,d)	Reinvestigations (01-02.06.d)
Granting Unescorted Access (01-02.06.a)	Behavior Observation Program(01-02.07.a,b)
Granting Unescorted Access (01-02.06.b)	Policy and Procedures (08-02.05.a,b,c,d,e,f,g,h)
Granting Unescorted Access (01-02.02.d,e)	Granting and Maintaining Authorization (08-02.06.a,b,c,d)
Granting Unescorted Access (01-02.02.f)	Test Results Review (08-02.07.a,b,c,d,e) SAE Interviews (08-02.09.a,b)
Granting Unescorted Access (01-02.02.h)	Test Results Review (08-02.07.f.g)
Maintaining Authorization (01-02.06.c)	Collection Site Inspection (08-02.08.a,b,c,d,e)
Information Sharing (01-02.08.a,b,c)	Licensee Testing Facility and/or HHS-Certified Laboratory(08-02.10.a,b,c,d,e)
Granting Unescorted Access (01.02.02.i)	

Tier III
Reviews (01-02.09)
Granting Unescorted Access (01-02.02.k)
Information Sharing (01-02.12.a,b)
Behavior Observation Program (01-02.11.a)
Personnel Information Management (01-02.10.a,b,c)
Reviews (08-02.11)
Policy and Procedures Review (08-02.12.a)
Test Results and Medical Review Officer (MRO) Interview (08-02.13.a)
Record Keeping and Reporting (08-02.14.a,b,c,d,e)
Managing Fatigue-Security Force Work Hours (08-02.15.a,b,c)

Figure 8 - Baseline Security Significance Determination Process Worksheet, “Access Control”

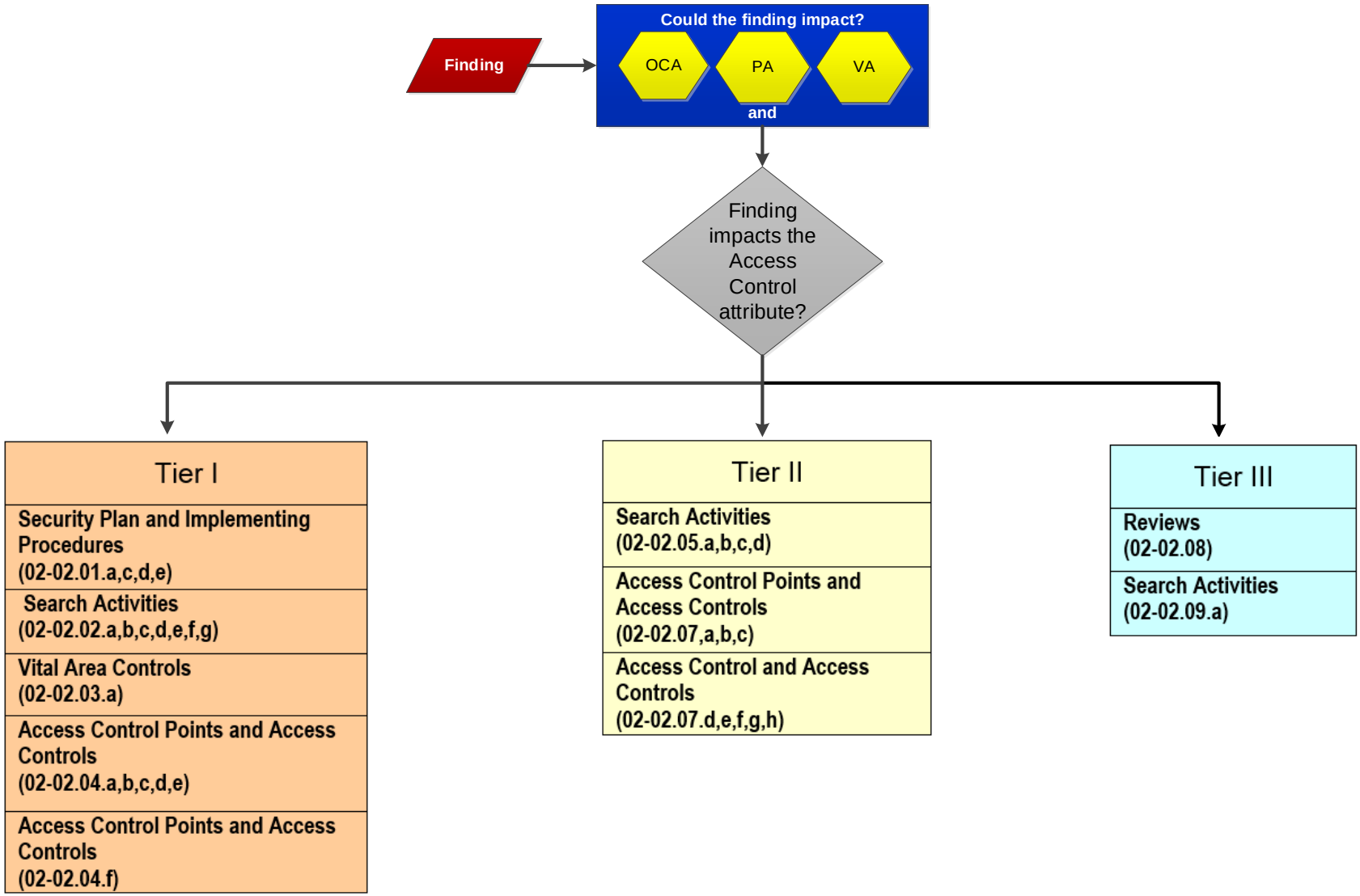
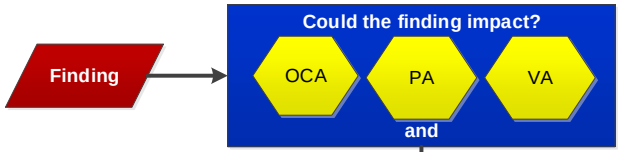


Figure 9 - Baseline Security Significance Determination Process Worksheet, “Physical Protection”



Finding impacts the Physical Protection attribute?

Tier I		
Security Plan and Implementing Procedures (02-02.01.b)	Alarm Stations (04-02.04.b,c)	Components of the Protective Strategy (05-02.02.a)
Security Plan and Implementing Procedures (04-02.01.a)	Communication System (04-02.04.f,g)	Components of the Protective Strategy (05-02.02.b)
Perimeter Intrusion Detection System (04-02.02.a,b,c,d,e,f,g)	Special Purpose Detection System (04-02.05.a,b,c,d)	Initial Training (07-02.02.a,b,c,d,e,f,g,h)
Perimeter Intrusion Detection System (04-02.02.h)	Physical Barriers (04-02.06.a,b,c,d)	Training & Qual. Plan/Implementing Procedures (07-02.01.a)
Perimeter Intrusion Detection System (04-02.02.i)	Physical Barriers (04-02.06.e)	Daylight/Night Fire Qualification (07-02.03.a,b,c,d,e)
Internal Detection and Assessment (04-02.03.a,b,c)	Weapons Maintenance Program (04-02.07.a,b,c,d)	Tactical Qualification (07-02.04.a.b)
Alarm Stations (04-02.04.a,d,e)	Evaluation of Security Systems, Equipment & Measures (04-02.08.a,b,c,d,e)	
Performance Evaluation Program (05-02.04.a,b,c,d)	Performance Evaluation Program (05-02.04.e)	

Tier II	
Perimeter Intrusion Detection System (04-02.09.a,b) Physical Barriers (04-02.12.a)	Components of the Protective Strategy (05-02.06.d)
Alarm Stations (04-02.11.a,b)	Training & Qualification Plan/Implementing Procedures (07-02.05.a,b,c,d,e)
Communication System (04-02.11.c,d,e)	On-the Job Training (07-02.06.a,b)
Other Security Related Devices & Equipment (04-02.13.a) Components of the Protective Strategy (05-02.06.n)	Firearms Familiarization Training (07-02.07.a)
Components of the Protective Strategy (05-02.06.a,c,e,h)	Requisite Knowledge & Performance (07-02-08.a)
Components of the Protective Strategy (05-02.06.f,g,i)	Re-qualification (07-02.09.a,b)
Components of the Protective Strategy (05-02.06.b)	Performance Evaluation Program (05-02.07.a,e,f)
Performance Evaluation Program (05-02.07.d)	Performance Evaluation Program (05-02.07.b.c)

Tier III
Reviews (04-02.14)
Weapons Maintenance Program (04-02.15.a,b,c)
Reviews (07-02.10)
Training Documentation (07-02.11.a)
Medical Qualifications (07-02.12.a,b)
Physical Fitness Test (07-02.13.a,b,c)
Performance Evaluation Program (05-02.11.a)
Firearms Preemption Authority (07.02.14. a,b,c)

Figure 10 - Baseline Security Significance Determination Process Worksheet, “Contingency Response”

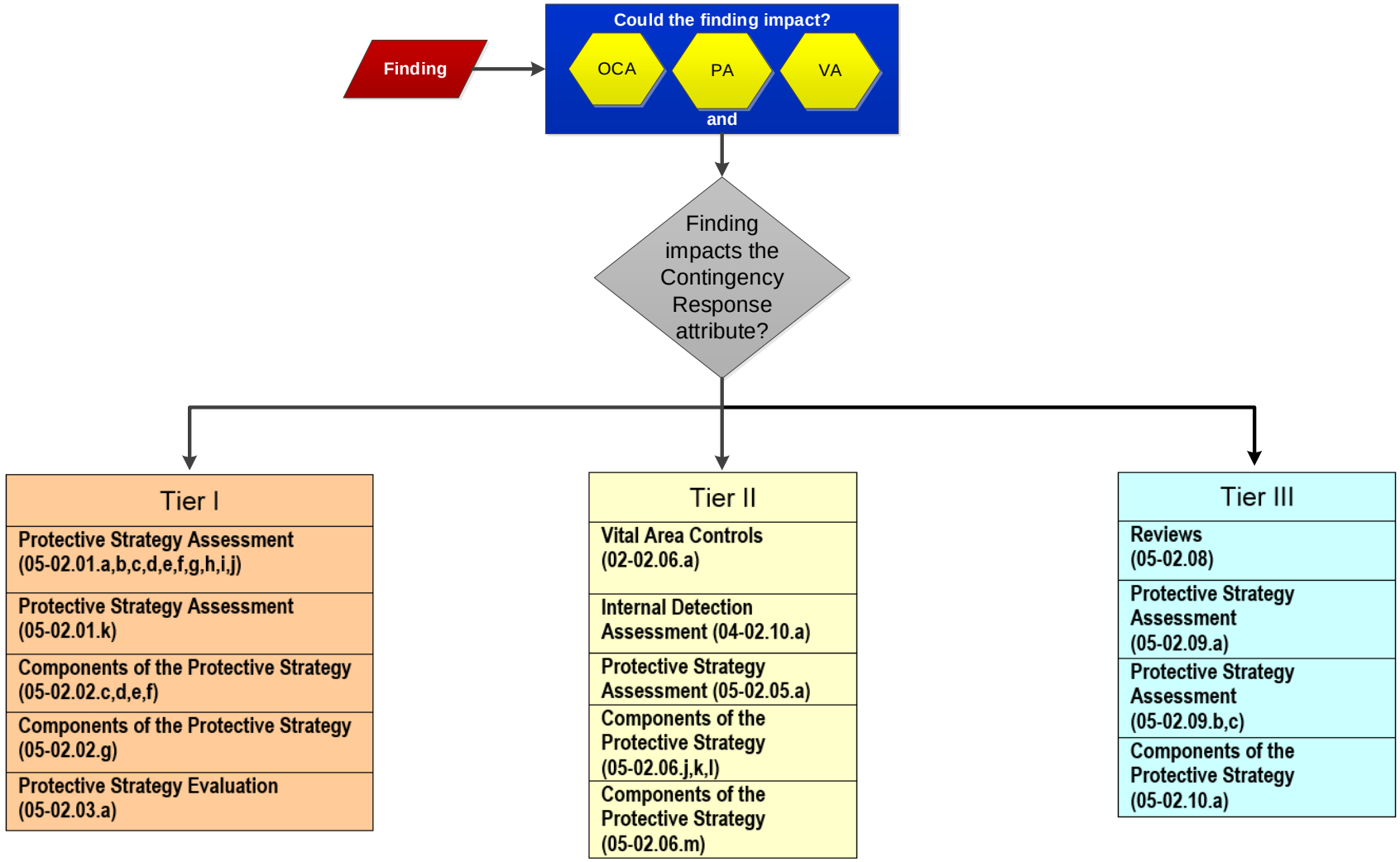


Figure 11 – Baseline Security Significance Determination Process Assessment Table

Range	Color
0 – 6	Green
7 – 15	White
16 – 25	Yellow
26+	Red

Access Authorization	Total Number of Program Elements Impacted																
	TIER I																
Impact Area	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
OCA	0	1	2	3	4	5	6	7	8	8	9	9	9	10	10	10	11	11
PA	1	2	3	4	5	6	7	8	8	9	9	9	10	10	10	11	11	11
VA	2	3	4	5	6	7	8	8	9	9	9	10	10	10	11	11	11	12

Access Authorization	Total Number of Program Elements Impacted															
	TIER II															
Impact Area	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
OCA	0	0	1	2	3	4	4	5	6	6	7	7	8	8	9	9	9
PA	0	1	2	3	4	4	5	6	6	7	7	8	8	9	9	10	10
VA	1	2	3	4	5	6	6	7	7	8	8	9	9	10	10	11	11

Access Authorization	Total Number of Program Elements Impacted									
	TIER III									
Impact Area	1	2	3	4	5	6	7	8	9	10
OCA	0	0	0	1	2	3	4	5	5	6
PA	0	0	1	2	3	4	5	5	6	6
VA	0	1	2	3	4	5	6	6	7	7

Access Control	Total Number of Program Elements Impacted									
	TIER I					TIER II			TIER III	
Impact Area	1	2	3	4	5	1	2	3	1	2
OCA	0	1	2	3	4	0	0	1	0	0
PA	1	2	3	4	5	0	1	2	0	0
VA	2	3	4	5	6	1	2	3	0	1

Physical Protection	Total Number of Program Elements Impacted																					
	TIER I																					
Impact Area	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
OCA	0	1	2	3	4	5	6	7	8	8	9	9	9	10	10	10	11	11	11	12	12	12
PA	1	2	3	4	5	6	7	8	8	9	9	9	10	10	10	11	11	11	12	12	12	13
VA	2	3	4	5	6	7	8	8	9	9	9	10	10	10	11	11	12	12	12	13	13	13

Physical Protection	Total Number of Program Elements Impacted																					
	TIER II																TIER III							
Impact Area	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	1	2	3	4	5	6	7	8
OCA	0	0	1	2	3	4	4	4	5	5	5	6	6	6	7	7	0	0	0	1	2	2	2	2
PA	0	1	2	3	4	4	5	5	5	5	6	6	7	7	7	8	0	0	1	2	3	3	3	3
VA	1	2	3	4	5	5	6	6	7	7	8	8	9	9	9	10	0	1	2	3	3	3	4	4

Contingency Response	Total Number of Program Elements Impacted													
	TIER I					TIER II					TIER III			
Impact Area	1	2	3	4	5	1	2	3	4	5	1	2	3	4
OCA	1	2	3	4	5	0	1	2	3	4	0	0	1	1
PA	2	3	4	5	6	1	2	3	4	5	0	1	1	2
VA	3	4	5	6	7	2	3	4	5	6	1	2	3	4

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