INSPECTION MANUAL CHAPTER 0308 ATTACHMENT 3 APPENDIX E

TECHNICAL BASIS FOR THE BASELINE SECURITY SIGNIFICANCE DETERMINATION PROCESS

Effective Date: XX/XX/XXXX

03083E-01 INTRODUCTION

The security significance determination process (SDP) is designed to identify declining performance in a timely manner so that increased regulatory oversight can be applied before performance becomes unacceptable. Inspection Manual Chapter (IMC) 0609, Appendix E, "Baseline Security Significance Determination Process for Power Reactors," is the assessment tool through which the U.S. Nuclear Regulatory Commission (NRC) evaluates findings that impact the Security Cornerstone of the Reactor Oversight Process (ROP) an d the Construction Reactor Oversight Process.

IMC 0609, Appendix E, is divided into four parts with each part containing objective tools for the assessment of deficiencies pertaining to different program areas within the Security Cornerstone. Part I, "Baseline Security Significance Determination Process (BSSDP) for Power Reactors," is used to evaluate the significance of most physical protection findings in the Security Cornerstone and contains additional tools for specialized program areas such as Material Control and Accountability (MC&A), target sets, and protection of Safeguards Information (SGI). Part II, "Force-on-Force (FOF) Physical Protection Significance Determination Process for Power Reactors," is used to evaluate the significance of findings related to FOF exercises conducted as a part of the NRC triennial FOF program. Part III, "Construction Fitness-For-Duty (CFFD) Significance Determination Process for New Reactors", is used to evaluate the significance of CFFD program findings at new reactors under construction. Part IV, "Cyber Security Significance Determination Process (CSSDP) for Power Reactors", is used to evaluate the significance of findings related to licensee cyber security programs.

01.01 Material Control and Accountability (MC&A) Significance Determination Process (SDP)

The purpose of MC&A is to provide for the detection and deterrence of loss, theft, or diversion of special nuclear material (SNM). The requirements for MC&A at power reactors are found in 10 CFR Part 74 and apply to all SNM, regardless of location, in the licensee's possession. The MC&A SDP provides an assessment tool that evaluates a number of objective factors to determine the significance of deficiencies related to MC&A programs at power reactors.

01.02 Decision Tree for Unsecured SGI

The requirements for the protection of SGI are found in 10 CFR 73.22. The purpose of these requirements is to prevent unauthorized disclosure of SGI and prescribe how the information is protected in various forms. Previous revisions of the BSSDP used qualitative considerations and management discretion to determine the significance of findings involving unsecured SGI. This process; however, did not produce consistent or repeatable outcomes. The Decision Tree for Unsecured SGI was developed to establish an objective set of criteria for the evaluation of unsecured SGI findings to produce more predictable and repeatable outcomes.

01.03 Unattended Opening (UAO) Significance Determination Process (SDP) Flowchart

The UAO SDP flowchart is used to evaluate the risk significance of deficiencies associated with the protection of UAOs. Previous use of the BSSDP worksheet and the Significance Screening Process for physical protection to evaluate deficiencies associated with UAOs either did not accurately capture the significance of the finding or did not produce consistent or repeatable outcomes due to subjectivity associated with the tools. The UAO SDP flowchart was developed to address these issues by using objective criteria based on location, time duration, and existing layers of defense-in-depth to reach an appropriate significance determination.

01.04 Target Set Significance Determination Process (SDP) Flowchart

The Target Set SDP Flowchart is used to evaluate deficiencies related to the identification and protection of target set equipment. Previous use of the Significance Screening Process for physical protection to evaluate findings related to target sets resulted in inconsistent and unpredictable outcomes. The Target Set SDP Flowchart was developed to risk-inform the significance of deficiencies related to the process of identifying and analyzing target sets and to risk-inform the significance of target set deficiencies that have the potential to affect the licensee's protective strategy or cyber security plan. Deficiencies that affect the strategy or cyber security plan are assessed in conjunction with the BSSDP Flowchart and Cyber Security SDP to appropriately inform significance based on the deficiency's adverse impact(s) to a licensee's physical protection and/or cyber security programs.

01.05 Baseline Security Significance Determination Process (BSSDP) Flowchart

The BSSDP Flowchart provides an evaluation tool to address physical protection performance deficiencies that are not screened by the other processes. This tool assesses the significance of a performance deficiency through a risk-informed process based on the assessed likelihood an adversary would be able to identify and exploit deficiencies in licensee performance and the associated impact on of a performance deficiency on the licensee's physical protection program.

01.06 Force-on-Force (FOF) Significance Determination Process (SDP)

The FOF SDP is used to evaluate the significance of FOF exercise outcomes during the implementation of Inspection Procedure (IP) 71130.03, Contingency Response – Force-on-Force Testing. The FOF SDP uses a points-based system based on exercises outcomes and other pre-determined performance inputs, known as performance threshold criteria (PTC), to determine significance and assign follow-up inspection activities when warranted.

01.07 Construction Fitness-for-Duty Significance Determination Process (CFFDSDP)

New reactors under construction are subject to unique Fitness-For-Duty (FFD) requirements in accordance with 10 CFR Part 26. The CFFDSDP evaluates the potential impacts of FFD program deficiencies on the safe and reliable construction of safety and security-related systems, structures, and components (SSCs) and assigns a risk significance using points-based model.

01.08 Cyber Security Significance Determination Process (CSSDP)

The requirements for cyber security are found in 10 CFR 73.54. The purpose of these requirements is to provide assurance that digital computer and communication systems and networks are adequately protected against cyber-attacks. The CSSDP process is used to

assign significance based on the actual and potential adverse impacts to safety, security, and emergency preparedness (SSEP) functions if an identified cyber security deficiency were to be exploited by a specific attack scenario.

03083E-02 SPECIFIC TECHNICAL BASES

02.01 Material Control and Accountability (MC&A) Significance Determination Process (SDP)

Calculating significance using the MC&A SDP (IMC 0609, App E, Fig. 2) relies on the evaluation of several contributing factors. First, the SDP considers whether the SNM involved was fuel or non-fuel SNM. A finding involving any quantity of spent nuclear fuel is processed, whereas the aggregate quantity of non-fuel SNM related to a finding must be greater than or equal to one gram to be further processed through the SDP. The quantity of one gram is derived from the requirements of 10 CFR 74.15, which do not require reporting nuclear material transactions that involve less than one gram of SNM.

If the SNM involved in the finding is any quantity of spent nuclear fuel or is a quantity of non-fuel SNM greater than or equal to one gram, then the inspector must determine whether or not the material was still within the licensee's control to some degree while it was unaccounted for. This step accounts for time and location being important characteristics of risk in the MC&A area. The likelihood of loss of SNM is decreased if the SNM is in an approved location, because this reduces the potential for inadvertent removal of SNM. It is the licensee's responsibility to maintain control over all SNM to prevent its loss. As such, the ability to locate the SNM in a timely manner is a factor in assessment of the finding.

The 7-day timeframe was selected as a reasonable time for the licensee to conduct a search of records and all approved locations. The 7 days takes into account operational safety considerations for infrequently performed evolutions that would be required if the search involved the spent fuel pool. Industry experience has indicated that searches exceeding 7 days typically extended for several months. The 7-day period begins when the licensee has in place the operational capability to support the search. It is expected that licensees will make a reasonable effort to begin the search in a timely manner. Additionally, if more than 7 days is required to recover unaccounted for SNM, this reflects more significant issues with the licensees MC&A program, as it is typically indicative that multiple issues exist with the licensee's MC&A program.

If the SNM was discovered outside an approved storage location or was not recovered within the 7-day timeframe described above, then the SNM is considered lost.

02.02 Decision Tree for Unattended SGI

The Decision Tree for Unattended SGI (IMC 0609, Appendix E, Figure 3) includes several factors used to assist in significance determination. These contributing factors are: the type of SGI that was left unattended, the conditions under which it was left unattended, and the duration of time that it was unattended.

While SGI is a single type of sensitive information and is not tiered based on significance like classified information (Confidential, Secret, Top Secret), a wide variety of sensitive unclassified information meets the criteria for designation as SGI. Therefore, as some SGI that contains a greater level of detail about the licensee's physical protection system and protective strategy, certain types of SGI would provide a greater advantage to a potential adversary than other

types. The decision tree takes this into consideration, and as a result, only certain types of information designated as SGI are processed through the decision tree. Other types of SGI that would not provide an advantage to an adversary that are left unattended result in a Green finding only.

When evaluating a failure to physically control SGI, the decision tree considers the amount of time the material was left unattended, and the conditions it was left unattended. The combination of these factors establishes the overall likelihood that it could have been compromised while unattended. Conditions that could make the SGI more easily discoverable by an unauthorized person (e.g., on a desktop versus in a closed desk drawer), as well as a longer time the material was left unattended both increase the overall likelihood of compromise. The only exception to the above time consideration is when SGI is left unattended in a Protected Area (PA). In these cases, the amount of time the SGI was left unattended is not a factor and the finding will always screen to Green. The decision to cap the significance at Green in these cases is based on the mitigation measures associated with the licensee's implementation of the insider mitigation program (e.g. stringent access control and background screening requirements, behavior observation program implementation, and security patrols). Additionally, because individuals with unescorted access also meet the requisite background investigation requirements for access to SGI, any discovery of unattended SGI within a PA would only potentially violate the specific requirements for a need--to--know which decreases the overall risk significance of the finding.

A number of specific factors are considered in the decision tree when evaluating the overall likelihood of compromise. The likelihood of discovery is a combination of the actual location of the SGI (such as the owner-controlled area (OCA), a controlled access area (CAA), or in an open public space), and the specific conditions under which it was left unattended (on a desk, in a drawer, on a copier, out in the open). The likelihood of discovery is then combined with the duration of time the material was left unattended. The time threshold at which the finding would move from Green to White is dependent on the conditions under which the material was stored. For example, SGI left unattended on a desk in an unlocked building in the OCA would move from Green to White significance more quickly than a document left unattended in a drawer inside a CAA.

In addition to the physical conditions under which the SGI was left unattended, the decision tree assessment process includes an evaluation of whether or not the information was encrypted (if it was an unattended electronic storage device and not a paper document). Encryption of electronic data, although not approved as a method of securing SGI data, still provides an increased level of protection when compared to an unencrypted storage device. If the material was encrypted using Federal Information Protection Standard (FIPS) 140-2 protection, it must be left unattended for a longer period of time before increasing in significance when compared to a paper document left unattended under similar conditions.

The SDP does not consider whether the information was compromised (i.e., disclosed to an individual who is not authorized to access it) when left unattended. Whether SGI is compromised is not necessarily within a licensee's control, therefore, the compromise of information is not used in evaluating significance. However, inspectors should consider whether the compromise of SGI constitutes an "actual consequence" of the SGI being left unattended and pursue traditional enforcement in addition to an ROP finding.

02.03 Unattended Opening Significance Determination Process Flowchart

The UAO SDP flowchart was developed as a tool to evaluate deficiencies related to the

protection of UAOs. The flowchart examines the location of the inadequately protected UAO, the duration of accessibility, and other physical security features along the UAO pathway to a complete target set to arrive at a significance determination. These considerations, which can be commonly assessed in any situation involving an inadequately protected UAO, reduce the subjectivity of the tool and increase both predictability and repeatability.

The location of entry to and exit from the UAO in relation to established layers of security represents one objective data point in the overall significance of the finding. Specifically, UAOs originating in the OCA and exiting within the PA or VA are of greater concern than those originating within the PA for multiple reasons. While site-specific OCA controls vary between licensees, in general, the access control and surveillance measures for OCAs are less stringent than those associated with a PA, increasing the likelihood of undetected exploitation. Additionally, UAOs originating in the OCA and terminating in a PA or VA provide a means to completely bypass the PA and VA layers of intrusion detection and assessment equipment which could adversely impact the licensee's ability to initiate a timely and effective response to the threat. For these reasons, inadequately protected UAOs originating in the OCA carry the potential for a higher significance depending on other factors considered later in the evaluation tool. Conversely, UAOs originating in the PA will always screen to a Green significance determination because there is reasonable assurance that the PA intrusion detection system (IDS), the licensee's Insider Mitigation Program (IMP), and/or the licensee's Behavior Observation Program (BOP) would enable detection of an adversary and initiation of a timely response prior to an adversary or insider entering the ingress point.

The flowchart process includes the duration of accessibility to the UAO pathway in the evaluation of the risk significance. While most UAOs are constantly configured, some can become exposed or temporarily created due to changes in plant configuration or emergent work activities. While these conditions provide a means to bypass layers of security, the less predictable and transitory nature of UAOs of this type present a higher degree of planning difficulty for an adversary to successfully exploit and are therefore less attractive. The flowchart recognizes these circumstances by establishing a time threshold for the licensee to discover and adequately compensate for or correct these conditions. UAOs below this time threshold would result in a Green finding regardless of the entry and egress location while UAOs above this time threshold carry the potential for a higher risk significance.

The last consideration in the flowchart is the total number of physical barriers and/or IDS an adversary would need to defeat prior to reaching a complete target set. Because the objective of a DBT adversary would be to cause significant core damage or spent fuel sabotage through the destruction of a complete target set, the flowchart sets access to a complete target set as the endpoint for the purpose of risk significance evaluation. The determination to examine the number of physical barriers and IDS along a given pathway was established on the basis that any overt actions to defeat these features along a given pathway would provide an opportunity for security to identify the potential threat through audible and/or visual means and initiate a response. In this final assessment step, higher levels of risk significance, up to Yellow, are assigned to pathways that bypass more layers of security with fewer barriers along the route in recognition of there being less of an opportunity for a licensee to initiate an effective response to the threat prior to reaching a complete target set.

02.04 Target Set Significance Determination Process (SDP) Flowchart

The Target Set SDP Flowchart was developed to evaluate deficiencies associated with the identification and protection of target set equipment. In previous revisions of the BSSDP, deficiencies associated with target sets were processed using qualitative criteria in the

Significance Screen which resulted in inconsistent and unrepeatable outcomes. Additionally, with the increased use of digital technology and the development and implementation of licensee cyber security programs, it became apparent that target set deficiencies with a cyber security impact should be assessed in conjunction with the Cyber Security SDP to appropriately risk-inform the significance. The Target Set SDP Flowchart was developed to address these concerns and assigns a risk-informed significance based on adverse impacts to the licensee's physical protection or cyber security programs.

Licensee programs associated with target set equipment include administrative processes associated with the identification, documentation, and continued review of target set equipment. When these processes fail to account for equipment or components that require protection, vulnerabilities in the design of the licensee's protective strategy or cyber security controls may be present that could challenge the licensee's ability to successfully prevent acts of radiological sabotage. The flowchart makes an early distinction in the significance between different types of target set deficiencies by assessing first through a set of descriptive criteria whether changes to the licensee's protective strategy or cyber security plan would be necessary to correct the deficiency. Issues that do not require changes to either the protective strategy or cyber security plan are screened against various administrative criteria for very low significance in recognition that no underlying vulnerability or exploitable condition associated with maintaining adequate protection existed. Conversely, deficiencies that require changes to either the licensee's protective strategy or cyber security plan require additional evaluation because they represent a vulnerability or exploitable condition that may have challenged the licensee's ability to adequately protect target set equipment.

Issues that necessitate a change to the licensee's protective strategy are transitioned to the BSSDP Flowchart while issues that necessitate a change to the cyber security plan are transitioned to IMC 0609, Appendix E, Part IV, "Cyber Security Significance Determination Process for Power Reactors," for further evaluation. The decision to transition issues to the BSSDP Flowchart or the Cyber Security SDP for further evaluation was made because those tools represent assessment options that are more closely related to the specific area requiring evaluation. Both the BSSDP Flowchart and cyber security SDP are tools that were in place and in use at the time the Target Set SDP Flowchart was created with both providing an objective means to assess the vast range of performance deficiencies related to their respective programs. Because the most risk significant target set related deficiencies would manifest as specific degradations or vulnerabilities relative to the licensee's protective strategy or cyber security plan, both tools were viewed as an acceptable means for evaluating issues with potentially higher risk significance. Additionally, attempting to incorporate specific elements and criteria into a unified tool specific to target sets had the potential to result in an overly complex process that would be redundant to the other SDP tools already available. For these reasons, the BSSDP Flowchart and Cyber Security SDP were viewed as the most appropriate means to produce objective and repeatable outcomes for target set issues that carry the potential for a higher level of risk significance.

02.05 Baseline Security Significance Determination Process (BSSDP) Flowchart

The BSSDP Flowchart provides an evaluation tool to assess the significance of performance deficiencies. A performance deficiency is assessed for the likelihood an adversary would be able to identify and exploit deficiencies in licensee performance and the associated impact of a performance deficiency on the licensee's physical protection program, by comparing the performance deficiency to criteria in two tables. The outcome of that assessment is used to identify the appropriate cross point in a significance matrix to determine the security risk significance of the performance deficiency.

In the first table, the performance deficiency is assessed for the likelihood an adversary would be able to identify and exploit deficiencies in licensee performance and the associated impact of a performance deficiency on the licensee's physical protection program. The examples in the table are based on a progression of exploitability from level I to level III. Each level corresponds to an increasing likelihood that an adversary would be able to identify the performance deficiency and to exploit it through focused surveillance of the site in accordance with the design basis threat.

Likelihood of exploitability incorporates guidance to inspectors to assist them in determining whether an issue is programmatic in nature or the result of a human performance error. Programmatic issues are performance deficiencies that are incorporated into the licensee's training, procedures, or processes and as a result are predictable and identifiable through surveillance of licensee activities or through access to procedures, records, or documentation available to an insider. The likelihood that a programmatic issue may be identified and exploited increases the longer the vulnerability exists. Generally, a finding that is programmatic is more exploitable by an adversary than a finding related to a human performance error within an otherwise adequate program or process. Specifically, a human performance error is generally not predictable if all procedures and processes are followed appropriately.

Multiple criteria in the likelihood of exploitability table may be applicable to the performance deficiency. In these cases, an average of the identified levels will be used to identify the most appropriate level of exploitability. Consideration of multiple criteria and averaging them adds additional realism to the determination by recognizing that factors that increase exploitability could be offset by factors that reduce exploitability.

The second table of the BSSDP Flowchart is used to evaluate the performance deficiency for the impact that the particular condition could have on a licensee's physical protection program if it were exploited by an adversary to commit an act of radiological sabotage. The examples in the table are based on a progression of consequences to which the licensee's physical protection program would be challenged to respond. The impact to the physical protection program takes into consideration several factors and rates the PD as low, medium, or high. Each factor relates to the general risk posed by the vulnerability or the impact the vulnerability would have if it were exploited by an adversary. The rating increases as the effectiveness of the licensee's physical protection program is more challenged.

02.06 Force-on-Force (FOF) Significance Determination Process (SDP)

The FOF SDP considers the outcome of all exercises conducted during an NRC evaluated triennial FOF inspection. The significance of findings resulting from exercise performance relies on a number of factors related to the outcome of the exercise. Any findings identified during an FOF exercise or inspection, other than those specific to the outcome of the exercise, are processed through the BSSDP, not the FOF SDP.

The FOF SDP uses a point-based system with predetermined significance thresholds to arrive at a single significance determination for the performance-based exercises. The SDP assigns an outcome of Effective, Indeterminate, Marginal, or Ineffective to each exercise with each outcome carrying a specific point value based on its relative significance. Ineffective exercises, which are assigned when a licensee fails to provide adequate protection of a complete target set during the conduct of the exercise, is assigned the highest point value followed by decreasing point values for Marginal and Indeterminate outcomes based on their relative significance to the licensee's protective strategy. Effective outcomes are assigned zero points in recognition of the successful implementation of the licensee's protective strategy during the

conduct of the exercise.

The point values for all exercises are totaled and increased or decreased depending on inputs associated with specific PTC. With the artificialities, limitations, and safety constraints present during the conduct of an FOF exercise, the inclusion of the PTC recognizes that a single demonstration of the licensee's protective strategy during an exercise may not be completely indicative of the overall effectiveness of the licensee's physical protection program. Therefore, the licensee's performance during an NRC evaluated exercise is considered in the context of the licensee's overall Security Cornerstone performance. The PTC considers conditions related to open risk significant findings and open substantive cross-cutting issues and increases or decreases the overall exercise outcome point value. For programs that have no additional weaknesses as determined by the PTC, the overall point value of exercise outcomes is slightly reduced. For programs that have other identified risk significant deficiencies, the overall point value for an exercise outcome evaluated as other than effective is slightly increased.

The FOF SDP uses point value tabulation tables as an efficient and predictable means to calculate the significance of exercise outcomes with different tabulation tables provided to assess one scheduled exercise or two scheduled exercises. Each table carries a different maximum significance determination of White for one scheduled exercise and Yellow for two scheduled exercises. This difference in potential significance determination outcome is based on multiple factors. First, due to the simulations and artificialities associated with conducting FOF exercises, ineffective outcomes across two separate scenarios with different pathways and objectives gives more weight to the presence of a potential programmatic issue with the licensee's protective strategy as a whole. Comparatively, a single ineffective demonstration might only be indicative of a weakness specific to a single pathway. Because observing two NRC evaluated exercises provides greater depth of evaluation through an additional data input, the potential to reach a Yellow significance determination is present when two scheduled exercises are evaluated versus a cap of White for one scheduled exercise. In both tabulation tables, the maximum significance is only attainable if the PTC is not met, reserving the highest levels of regulatory oversight for programs with already present risk significant deficiencies in other areas of the Security Cornerstone.

In addition to assigning an overall risk significance determination for the exercise outcomes, the tabulation tables for the initial exercise week also assign specific re-visit actions to most negative exercise outcomes. These actions can range from a Corrective Actions Measures (CAMs) review to the conduct of multiple NRC evaluated exercises as a separate follow-up inspection activity referred to as a re-inspection. In general, the rigor and resource requirements of the follow-up actions increase as the number of indeterminate, marginal, and ineffective exercises increase. The licensee's overall performance as measured by the PTC can have a minor impact on the type of follow-up activity but the SDP functions such that an Ineffective exercise combined with any outcome other than an Effective outcome will result in the observation of two additional NRC evaluated exercises. This relationship is reflective of the increased level of concern associated with licensees who fail to demonstrate in at least one exercise that their protective strategy, as designed, is capable of providing adequate protection for target set equipment through an effective exercise outcome. The type of follow-up action is dependent solely upon different combinations of exercise outcomes and does not depend on the overall point value accumulated at the end of the inspection.

A separate tabulation table for re-inspections is used only when the re-visit action from the initial inspection activity requires the conduct of two additional NRC evaluated exercises. The tabulation table for re-inspection activities slightly increases the point values for indeterminate, marginal, and ineffective exercise outcomes during re-visit exercises and does not consider the

PTC in the overall point value calculation as in previous tabulation tables. Because the licensee's performance during the initial activity consisted of one ineffective demonstration coupled with an outcome other than effective, there is an increased focus on ensuring that the licensee appropriately identified and corrected the deficiencies that led to the initial less-than-effective exercise outcome(s). Elimination of the PTC during re-inspection activities ensures the risk significance of less-than-effective exercise outcomes are not mitigated based on adequate security program performance outside of the licensee's performance evaluation program. The slight increase in point values for indeterminate, marginal, and ineffective exercises also opens a pathway to reach a Red significance determination through two ineffective exercise outcomes. This pathway to a Red significance determination is commensurate with the increased level of concern associated with programs that do not demonstrate the ability to effectively identify and correct protective strategy related deficiencies after previously identified risk significant exercise failures.

02.07 Construction Fitness-for-Duty Significance Determination Process (CFFDSDP)

All more-than-minor performance deficiencies related to FFD requirements for nuclear power reactors under construction are evaluated using the CFFDSDP. FFD related performance deficiencies at a reactor under construction are unique in that they do not carry the same immediate consequences as an operating reactor due to the absence of an operating reactor core and/or spent fuel. Deficiencies during construction, however, have a potential to adversely impact various safety-related and security-related structures, systems, and components (SSCs) that may be relied upon at a point in the future to maintain the reactor in a safe and secure condition once it is brought online. The CFFDSDP evaluates risk significance as the potential adverse impact a worker who is not fit for duty may have upon these safety and security significant SSCs.

The CFFDSDP uses a point-based system with key modifications to fit the unique circumstances of construction FFD programs. Because construction licensees may choose to implement the requirements of 10 CFR 26 Subpart K or a full testing program in accordance with 10 CFR 26 Subparts A through H, N, and O, the CFFDSDP was designed to account for deficiencies associated with either program. The overall point values are derived from inspection procedure samples from the applicable inspection procedure. Each inspection requirement is categorized into one of three tiers with Tier I requirements carrying the highest potential point values followed by lower values assigned to Tier II and Tier III based on their relative significance to the licensee's FFD program.

Operating reactor construction projects consist of an extensive amount of work activities that can be categorized into work that involves safety-related and security-related SSCs and work that does not. Because FFD requirements can extend to construction workers across a broad range of disciplines and construction activity, the CFFDSDP considers whether the deficiency was associated with or allowed an unfit individual to work on safety-related and security-related SSCs. FFD program deficiencies that permit an unfit individual to work on SSCs are considered to be more risk significant due to the potential adverse impact to nuclear safety and security once the reactor enters the operational phase. Conversely, FFD program deficiencies associated with work on non-SSC equipment do not carry the same level of risk because there is a minimal underlying impact to nuclear safety and security once the reactor is brought online. While all FFD program related deficiencies must be corrected, the CFFDSDP accounts for differences in work activities by increasing the Tier I, II, and III point values if the FFD program deficiency is associated with or allowed an unfit worker to work on SSCs.

02.08 Cyber Security SDP for Power Reactors

All more-than-minor performance deficiencies related to cyber security controls at nuclear power reactors are assessed using the Cyber Security SDP for Power Reactors. In accordance with 10 CFR 73.54, licensees are required to protect digital computer and communications systems and networks associated with safety-related and important-to-safety functions, security functions, emergency preparedness (EP) functions including offsite communications, and other systems and equipment which, if compromised, would adversely impact a safety, security, or emergency preparedness (SSEP) function. The Cyber Security SDP assesses the potential for deficiencies to enable an adverse impact to SSEP functions as a result of cyber-attack scenarios or actual cyber-attacks.

The Cyber Security SDP consists of an initial screening tool and individual decision trees each for the assessment of Safety, Security, and EP functions respectively. The initial screening tool was developed to distinguish between issues of very low significance and those requiring additional evaluation to reach a significance determination. Deficiencies associated with an actual cyber-attack on a licensee's systems that caused an adverse impact to an SSEP function are of particular concern due to the presence of a tangible consequence. Accordingly, issues involving an actual cyber-attack that adversely impacted an SSEP function bypass the initial screening considerations for very low significance and move directly to a more in-depth evaluation where higher levels of significance are achievable. All other deficiencies that do not involve an actual attack on the licensee's system are assessed within the initial screening tool against a set of qualitative criteria. If the deficiency is determined not to be exploitable or if the licensee has existing controls and measures in place to detect, respond to, and effectively mitigate an attack, then the issue is screened to very low significance in recognition of there being no potential for an adverse impact to occur.

Specific to safety-related or important-to-safety functions, the Cyber Security SDP considers multiple factors associated with initiating events, mitigating systems, and other risk significant systems (RSS). In general, the significance of a finding correlates to the degree to which a licensee would be challenged in maintaining the reactor in a safe condition with the adverse conditions created by the cyber-attack. As a practical example, deficiencies that would enable a Loss of Offsite Power (LOOP) or adversely impact only one RSS would receive a lower risk significance than deficiencies that would enable a complete loss of safe shutdown capability or adversely impact multiple RSS.

The CSSDP process directs cyber security deficiencies that would enable an adversary to adversely impact a security function that pass the initial screening to the BSSDP Flowchart (IMC 0609, App E, Part I) for further evaluation. Actual or potential cyber-attacks against a licensee's physical protection program would manifest as losses of or degradations to specific physical protection equipment, systems, and components. The resultant condition would have the potential to adversely impact the licensee's ability to adequately implement the requirements associated with each Security Cornerstone attribute, such as controlling access to various security areas, detection and response, and overall control of the licensee's security computer system. Because the BSSDP is a well-established process with a proven capability to evaluate a broad range of deficiencies related to the equipment, systems, and processes related to physical protection programs, the determination was made not to develop a new or unique assessment tool specific to cyber security deficiencies related to security functions. This decision reduces overall redundancy in the SDP tools and promotes consistent SDP outcomes within the Security Cornerstone.

Deficient cyber security performance evaluated through the BSSDP Flowchart represents

exploitable conditions that would manifest as degradations or losses to digital security systems, evaluation of all physical protection program elements that would be adversely impacted by the exploitable condition is necessary to reach an appropriate cyber security program risk significance determination.

The Cyber Security SDP for EP functions evaluates actual or potential adverse impacts in the form of losses of Risk Significant Planning Standards (RSPS) and Planning Standards (PS). Deficiencies that do not represent an actual attack that resulted in the loss of an RSPS or a PS during an EP exercise or actual emergency are screened out as Green in recognition of the licensee's ability to identify and correct the condition before an actual adverse impact to the licensee's EP capability occurred. Conversely, deficiencies that represent an actual loss of RSPS or PS at a time when a licensee must implement the Emergency Plan carries the potential for a higher risk significance commensurate with the adverse impact on the licensee's ability to effectively and accurately manage and respond to the emergency condition. Issues that represent an actual loss of an RSPS or PS during these conditions are transitioned to IMC 0609, Appendix B, "Emergency Preparedness Significance Determination Process," for further evaluation. Because the EP SDP was already designed with the capability to evaluate a broad range of deficiencies associated with RSPS and PS, the decision was made to use the already established and proven tool to avoid redundancy and ensure consistency in the application of significance determination outcomes.

03083E-03 REFERENCES

IMC 0609, Appendix B, Emergency Preparedness Significance Determination Process

IMC 0609, Appendix E, Part I, Baseline Security Significance Determination Process

IMC 0609, Appendix E, Part II, Force-on-Force Significance Determination Process

IMC 0609, Appendix E, Part III, Construction Fitness-for-Duty Significance Determination Process for New Reactors

IMC 0609, Appendix E, Part IV, Cyber Security Significance Determination Process for Power Reactors

FIPS 140-2, Security Requirements for Cryptographic Modules

END

Attachment:
Revision History for IMC 0308, Attachment 3, Appendix E.

Attachment 1: Revision History for IMC 0308, Attachment 3, Appendix E

Commitment Tracking Number	Accession Number Issue Date Change Notice	Description of Change	Description of Training Required and Completion Date	Comment Resolution and Closed Feedback Accession Number (Pre-Decisional, Non-Public Information)
N/A	ML11342A018 07/27/2012 CN 12-016	Initial issuance	None	N/A
N/A	ML21312A432 01/31/2022 CN 22-002	This is a major revision and should be read in entirety. Revised to capture new SDP tools (e.g. UAO SDP, Cyber Security SDP, etc.) incorporated into the BSSDP since initial issuance. Revised to conform terminology throughout the document to changes in SDP terminology since initial issuance. Conducted SUNSI review and determined the “Official Use Only Security-Related Information” designation may be removed upon issuance of the document.	None	ML21312A434
N/A		Revised to capture the discontinued use of the BSSDP Worksheet for calculating PD significance for security related findings and other minor editorial corrections.		