



NUCLEAR ENERGY INSTITUTE

Stephen D. Floyd
VICE PRESIDENT, REGULATORY
AFFAIRS
NUCLEAR GENERATION DIVISION

July 28, 2004

Mr. Roy P. Zimmerman
Director
Office of Nuclear Security and Incident Response
U.S. Nuclear Regulatory Commission
Washington, DC 20006

Dear Mr. Zimmerman:

We appreciated the participation of Dr. Ralph Way, Mr. Barry Westreich and Mr. Peter Prescott in the NEI Significance Determination Process (SDP) Task Force Meeting held on July 1, 2004. They provided a comprehensive overview of the NRC developed SDP process which allowed for constructive follow-on dialogue. We also shared a copy of the industry developed SDP; a copy is enclosed for consideration.

One of the discussions centered on the idea of industry applying the NRC SDP on findings that NRC also evaluated. Using the same findings enables us to compare results and where differences exist, understand the reason. In the meeting we asked if the NRC staff would be able to share a dozen or so findings but now understand that may not be possible. Therefore, we have accumulated findings from various licensees and will analyze them using the NRC SDP and the industry SDP. We believe this approach will still produce results that will be useful in future discussions.

We do have a few first blush comments on the NRC Physical Protection SDP Worksheet. The chart has an "exploitable" decision block in Section C. We believe that decision block is misplaced and that it should apply to all findings before entering Section A. If a finding is not predictable and exploitable then it is not risk significant and need not be evaluated further.

We also have concerns with the Force-On-Force SDP. We view the triennial NRC witnessed exercise as part of the continuum of annual exercises now an aspect of each plant's security training regimen. Also, it is our understanding that the SDP is focused on single findings. This being the case, it is not clear that a loss of more than one target set is a single finding. We would appreciate further dialogue on this topic.

Mr. Roy P. Zimmerman
July 28, 2004
Page 2

Finally, the enclosed industry SDP uses the successful principles developed in the Emergency Preparedness SDP to provide a simple, suitable performance-based approach to characterizing the significance of Physical Protection Findings. It includes:

- use of a performance based approach to characterize the significance of findings.
- distinction between risk significant physical protection functions and standard physical protection functions.
- determination of the predictability and exploitability of finding issues.
- a focus on adequate critique of exercises.
- avoidance of unintended consequences, such as degrading public confidence with a new and complex process, artificially increasing or decreasing significance of performance weaknesses, or inconsistent applications or interpretation of issues.
- coverage of all aspects of Physical Protection for nuclear power plants in one SDP.

We believe an effort should be made to integrate the industry process into the NRC developed approach.

We will contact your office to set-up a meeting to discuss the results of our applying the NRC process to sample findings.

Please contact John Rycyna, Doug Walters or me if you have any questions.

Sincerely


Stephen D. Floyd

Enclosure

c: Mr. Glenn M. Tracy, NRC

APPENDIX E

PHYSICAL PROTECTION SIGNIFICANCE DETERMINATION PROCESS

1.0 INTRODUCTION

The Significance Determination Process (SDP) is a major element in the NRC's Reactor Oversight Process (ROP). The framework for the Physical Protection Cornerstone is described in SECY-99-007 (*Recommendations for Reactor Oversight Process Improvements*), SECY-99-007a (*Recommendations for Reactor Oversight Process Improvements (Follow-up to SECY-99-007)*), and NRC Manual Chapter 0308. The oversight process is comprised of seven cornerstones. The physical protection cornerstone objective and performance expectation are the bases for the physical protection inspection program, the ROP performance indicators and the significance determination process.

The Physical Protection Cornerstone objective is to ensure activities do not constitute an unreasonable risk to the public health and safety.

The performance expectation is to demonstrate that there is reasonable assurance that the licensee can effectively implement its physical security program in a manner that satisfies the objective.

To meet the objective and performance expectation for physical protection, the U.S. Nuclear Regulatory Commission (USNRC) assesses licensee performance in the following programs and activities:

- Access Authorization Program
- Fitness-for-Duty Program
- Security Program
 - Safeguards Equipment (intrusion detection, alarms, weapons, communication, and barriers)
 - Safeguards Contingency Plan and Program
 - Training and Qualification Plan and Program, including the evaluation of drills and exercises
 - Actual events involving the activation of the Safeguards Contingency Plan

NRC Inspection Program elements are:

- Access Authorization (IP 71130.01)
- Access Control (IP 71130.02)
- Response to Contingency Events (IP 71130.03)*
- Security Plan Changes (IP 71130.04)
- Protective Strategy Evaluation (IP 71130.05)
- Inspection of Security Plan Changes (IP 71130.06)
- Security Training (IP 71130.07)
- Fitness-for-Duty Program (IP 71130.08)
- Owner-Controlled Area Controls (IP 71130.09)
- Information Technology Security (IP 71130.10)*

- Material Control and Accounting (IP 71130. 11)**

*This baseline activity is still being developed and has been deferred.

** This baseline activity will be initially satisfied by Temporary Instruction.

Licensee performance is also assessed through licensee self-assessments and by meeting predetermined ROP performance indicators. The Physical Protection SDP, when coupled with the physical protection performance indicators, is the basis for determining the level of future NRC interactions with a licensee on physical protection.

To meet the Cornerstone Objective and Performance Expectation, the staff of the U.S. Nuclear Regulatory Commission (USNRC) assesses licensee performance in this cornerstone by considering the relationship of performance indicators (PIs) with regard to thresholds and the significance of inspection findings. The significance determination process (SDP) provides a method to place inspection findings in context for risk-significance in a manner that allows them to be combined with PI results. This information is used to determine the level of NRC engagement in accordance with (IAW) the Reactor Oversight Process Action Matrix (found in Inspection Manual Chapter 0305, "Power Operating Reactor Assessment Program").

[Note: Defined terms are capitalized throughout the remainder of the text of this Appendix. See Section 2 for Defined Terms.]

Inspection Manual Chapter 0612, "Power Reactor Inspection Reports", Appendix B "Screening Criteria", contains criteria for determining which inspection issues are FINDINGS that the staff should evaluate through this SDP. This SDP is structured such that any FINDING that enters the SDP will be at least GREEN. This SDP is designed such that the significance of a finding reflects the impact on public health and safety, the potential impact on the public health and safety should an accident occur, or the impact on the efficacy of the licensees PI response band.

During the development of this SDP, the most Risk-Significant PHYSICAL PROTECTION FUNCTIONS (RSPPF) were identified as being distinct from other "standard" PHYSICAL PROTECTION FUNCTIONS (SPPF). These development efforts were performed by a group of Security subject matter experts. On that basis, this Physical Protection SDP methodology recognizes some FINDINGS in the identified risk-significant elements as being more significant than FINDINGS in other PROGRAM FUNCTIONS (i.e., a YELLOW finding rather than a WHITE finding).

While the SECURITY SDP assigns color-coded safety significance to FINDINGS, it should be understood that a GREEN FINDING (very low safety significance) does not mean that the performance is acceptable. Such a finding may, in fact, represent a violation of a REGULATORY REQUIREMENT. The GREEN determination simply means that the safety significance of the finding is very low and correction of the item is considered to be within the "licensee response band" and is to be corrected within the licensee's corrective action program.

2.0 DEFINITIONS AND GENERAL GUIDANCE

The following terms, those listed in Section 2.1, and the guidance provided in Section 2.2 are essential to understanding this appendix. The two categories are:

STANDARD PHYSICAL PROTECTION FUNCTIONS (SPPF)

FINDINGS in these areas, listed below as FUNCTIONS #1, # 2, # 3 #4, and #5 may result in a challenge to the protective strategy, yet the FINDING is of such a nature that the licensee would still retain a degree of defense-in-depth in relation to physical protection of the plant.

RISK SIGNIFICANT PHYSICAL PROTECTION FUNCTION (RSPPF)

FINDINGS that are directly related to protecting against the DESIGN BASIS THREAT, in the event an ADVERSARY gains access to TARGET SETS sufficient to permit a release in excess of 10CFR100 limits. FINDINGS in these areas, listed below as FUNCTIONS #6, #7, #8 and #9, may result in a significant reduction in protective margin.

2.1 Definitions

Note: Defined terms (listed in alphabetical order) are capitalized throughout the text of this appendix.

1. **ACCESS CONTROL**: All elements necessary to ensure that access of vehicles, material and personnel into the protected area and vital areas is properly implemented.
2. **CATEGORY**: The Significance Determination Process (SDP) categorizes the safety significance of FINDINGS into four (4) general categories of escalating significance as defined in NRC MC 0609:
 - **GREEN** - A finding of very low safety significance. The GREEN band is characterized by acceptable performance in which cornerstone objectives are being met with performance attributes and risk indications in the normal range. Performance problems would not be of sufficient significance that escalated NRC engagement would occur. Licensees would have maximum flexibility to "manage" corrective action initiatives. The threshold for this band would involve performance that would be outside the normal range of industry historical performance and risk.
 - **WHITE** - A finding of low to moderate safety significance. The WHITE band would be entered when licensee performance is outside the normal performance range, but would still represent an acceptable level of performance. Performance is still considered to be within the objectives of the cornerstone, but there is indication of declining performance with a minimal reduction in safety margin.
 - **YELLOW** - A finding of substantial safety significance. The YELLOW band involves a decline in licensee performance that is still acceptable with cornerstone objectives met, but represents a significant reduction

in safety margin. These threshold characteristics and required regulatory response are also selected to be consistent with risk-informed regulatory applications and mandatory actions for regulatory compliance.

- **RED** – A finding of high safety significance. The RED band is typified by changes in performance considered to be significantly outside the design basis, with unacceptable margin(s) to safety, with an accompanied loss of confidence that public health and safety would be assured with continued operation. Further decline in performance would result in operation in a state inconsistent with the NRC safety goals.
3. **CRITIQUE:** All formal and/or documented assessments of a **DRILL/EXERCISE**.
 4. **CRITIQUE PROBLEM:** Indicates that a CRITIQUE did not identify a **DRILL/EXERCISE WEAKNESS**. A finding in this area means that licensee evaluators failed to identify a WEAKNESS in a DRILL/EXERCISE.
 5. **DEGRADATION OF THE FUNCTION:** PROGRAM ELEMENTS are not adequate or are noncompliant, but the FUNCTION, although degraded, is still met. It may be that (1) certain Plan commitments are not met, (2) implementing procedures are not effective, or (3) the program design is not fully adequate. However, if the PROGRAM ELEMENT is implemented as designed, it would meet the intended **FUNCTION**. DEGRADATION OF THE FUNCTION has been incorporated into the PHYSICAL PROTECTION SDP to allow an intermediate level of significance (i.e., a white finding rather than yellow) to be determined, where appropriate. Section 4.0 presents examples of DEGRADATION OF THE FUNCTION for each SPPF/RSPPF.
 6. **DESIGN BASIS THREAT (DBT):** Defined in NRC Order EA-03-086 Dated April 29, 2003 which imposed a revised Design Basis Threat from that described in 10CFR73.1(a). The fundamental principle is that the licensee must protect the plant from adversary action that would cause a 10CFR100 release.
 7. **DRILL/EXERCISE:** NEI 03-09 has two types of drills and exercises. Force-on-Force Tactical Exercises are required annually for each section while Tactical Drills must be performed quarterly. For the purposes of this SDP they are grouped together as DRILL/EXERCISE. The definitions from NEI 03-09 are:

Force-on-Force Tactical Exercise — A force-on-force simulation used to evaluate and demonstrate the capability to defend TARGET SET against selected attributes and characteristics of an adversary.

Tactical Drill — A structured training tabletop or field activity that evaluates at least one key PROGRAM ELEMENT of the protective strategy. The element(s) to be evaluated must be clearly identified

before conducting the drill, and intervention or coaching must be limited so as not to interfere with evaluation of the designated criteria.

8. **FAILURE TO COMPLY**: A program is noncompliant with a **REGULATORY REQUIREMENT**.
9. **FAILURE TO IMPLEMENT**: **FAILURE TO COMPLY** with **REGULATORY REQUIREMENTS** during an actual event in which the failure precluded effective implementation of **PROGRAM ELEMENTS**. Most likely, the failure is a result of a performance problem. In this case, the **PROGRAM ELEMENT** is adequate as designed and, if implemented as designed, the program would meet the **FUNCTION**. However, a **FAILURE TO IMPLEMENT** is not always a result of a performance problem and may, in fact, reveal that a **PROGRAM ELEMENT** is not adequate. In this case, inspection is appropriate to determine whether there is a **LOSS OF FUNCTION**. Resulting issues would be assessed for significance IAW this SDP.
10. **FINDING**: As defined in NRC Manual Chapter 0609.
11. **FUNCTION**: There are nine (9) physical protection **FUNCTIONS**:
 - **FUNCTION # 1 – Administrative (SPPF)** – The licensee has developed and implemented programs for administrative duties including information technology controls, outlined in the Physical Security Plan that are not covered in another **FUNCTION**. (IP 71130.06)
 - **FUNCTION #2 – Training and Qualification (SPPF)** – (Appendix B – Training and Qualification Plan, NEI 03-09) (IP 71130.07)
 - **FUNCTION #3 – Drill and Exercise (including Force-on-Force) Program (SPPF)** – The licensee has developed and implemented a drill, exercise, and force-on-force exercise program in accordance with the site's training and qualification plan. (IP 71130.03)
 - **FUNCTION #4 – Access Authorization/Fitness for Duty (SPPF)** – The licensee has established pre-access and ongoing access authorization, fitness for duty, and behavioral observation for all personnel granted unescorted access. (IP 71130.01 and 71130.08)
 - **FUNCTION #5 – Personnel and Materials ACCESS CONTROL Process (SPPF)** – The licensee has established procedures and equipment for **ACCESS CONTROL** for personnel and entering the protected and vital areas, and for material controls and accountability. (IP 71130.02 and 71130.11)
 - **FUNCTION #6 – Barrier Defense in Depth (RSPPF)** – Barrier defense in depth is design, installation, and maintenance of protected and vital area barriers, keys locks and combinations. (IP 71130.09 and 71130.10)

- **FUNCTION #7 – Vehicle Barriers and Searches (RSPPF)** – The licensee has designed, installed, and maintains vehicle barrier systems. This includes vehicle searches and controls at the vehicle barrier system to address specific vehicle threats. (IP 71130.09)
 - **FUNCTION # 8 – Assessment and Detection (RSPPF)** – The licensee has designed, installed and maintains equipment used to detect and assess unauthorized entrance into the Protected and Vital Areas so that the protective strategy may be initiated in a timely manner. (IP 71130.04)
 - **FUNCTION # 9 – Protective Strategy (RSPPF)** – The licensee has performed an analysis of **TARGET SETS** and has developed a protective strategy to defend those **TARGET SETS** against the **DESIGN BASIS THREAT**. (IP 71130.05)
12. **INTRUSION:** An act of entering a protected or vital area, by an individual who does not possess authorized unescorted access to the protected area.
13. **LOSS OF FUNCTION:** FUNCTIONS are not adequate, not compliant with the provisions of 10CFR Parts 26 & 73 and applicable Orders, or otherwise not performing to such an extent that the FUNCTION is not available. It may be that the Plan commitments are not met, implementing procedures are inadequate, program design is inadequate, training is inadequate, etc. The result is that if the suspect PROGRAM ELEMENT was implemented as designed, or personnel are not capable of implementing the PROGRAM ELEMENT as intended, the FUNCTION would not be met.
14. **PREDICTABLE AND EXPLOITABLE:** Based on the manner in which a FUNCTION and/or PROGRAM ELEMENT was implemented, or how equipment or systems were operating:
- a. It could be credibly determined in advance that a specific vulnerability would be likely to occur [PREDICTABLE].

AND

- b. Adversaries could credibly take advantage of the vulnerability to defeat an aspect of the security plan. [EXPLOITABLE]

PREDICTABLE AND EXPLOITABLE must both be satisfied before the **FINDING** associated with a **FUNCTION** and/or **PROGRAM ELEMENT** can be concluded to be more than a low risk-significant event (**GREEN**). Hence, **FINDINGS**, which do not meet the **PREDICTABLE AND EXPLOITABLE** criteria, will be categorized as **GREEN**.

For example:

Predictable but not exploitable could be every time there is a large rain

gravel washes out under the PA fence at microwave Zone 15. The microwave system would detect the INTRUSION.

Exploitable but not predictable could be a random microwave failure discovered during a weekly test.

PREDICTABLE AND EXPLOITABLE could be every time there is a large rain gravel washes out under the PA fence in an area with failed lighting which would inhibit night time assessment and response even if IDS were functioning properly..

15. PROGRAM ELEMENT: Items that comprise the implementation aspects of a PHYSICAL PROTECTION FUNCTION. These items, discussed in detail in NEI 03-09, provide specific acceptable methods for complying with the RSPPF or SPPF. Note that the failure of a single PROGRAM ELEMENT does not usually constitute a LOSS OF FUNCTION.
16. REGULATORY REQUIREMENT: As used in this appendix, any PHYSICAL PROTECTION related requirement, including the provisions of 10CFR26 and 73, the Physical Security Plan, Safeguards Contingency Plan, or Training and Qualification Plan, Commission Orders, and other regulatory commitments.
17. RISK SIGNIFICANT PHYSICAL PROTECTION FUNCTION (RSPPF): FUNCTIONS that are directly related to protecting against the DESIGN BASIS THREAT, to prevent an adversary from causing a release in excess of 10CFR100 limits. FINDINGS in these areas, listed above as FUNCTIONS #6, #7, #8 and #9, may result in a significant reduction in protective margin.
18. SAFEGUARDS INFORMATION: See 10CFR73.21 for the definition.
19. STANDARD PHYSICAL PROTECTION FUNCTIONS (SPPF): Listed above as FUNCTIONS #1, # 2, #3, #4 and #5, may result in a challenge to the protective strategy, yet the FINDING is of such a nature that the licensee would still retain a degree of defense-in-depth in relation to physical protection of the plant.
20. TARGET SET: the 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 disruption) barring extraordinary action by plant operators. A TARGET SET with respect to spent fuel sabotage is draining the spent fuel pool leaving the spent fuel uncovered for a period of time, allowing spent fuel heat up and the associated potential for release of fission products.
21. WEAKNESS: A WEAKNESS is a level of performance demonstrated during a drill or exercise that could have precluded effective implementation of the FUNCTION in the event of an actual emergency.

WEAKNESSES are not confined to performance problems that result in a **LOSS OF FUNCTION**. A **WEAKNESS** may also exist if a performance problem occurs associated with unsuccessful implementation of requisite actions anticipated by the scenario. Licensees are expected to identify and **CRITIQUE** performance problems as **WEAKNESSES** associated with **SPPF** and/or **RSPPF** during **DRILLS/EXERCISES**, self assessments, audits, management reviews or other opportunities.

2.2 Guidance

- (1) The NRC Policy Statement on “Safety Goals for the Operations of Nuclear Power Plants”, states that Safeguards is a defense-in-depth measure. Safeguards and many other elements of reactor safety (e.g., remote siting and containment) are implemented as a matter of prudence, rather than in response to a quantitative analysis of accident probabilities. Consequently, the probability of implementing a licensee’s Security Contingency Plan has no relevance in determining the significance of a Safeguards problem. Rather, in determining the significance of a Safeguards problem, it is assumed that the licensee’s Security Contingency Plan is being implemented in response to an emergency and the impact of the problem will be assessed against the licensee’s ability to effectively implement adequate measures to protect the public health and safety for the DESIGN BASIS THREAT.**
- (2) This SDP is preceded by the requisite screening of an issue, in accordance with NRC Manual Chapter 0612, Appendix B, to determine if the issue is an actual FINDING. Manual Chapter 0612, Appendix B is included in this SDP after section 5.3 for information.**
- (3) Once the issue is categorized as a FINDING in accordance with MC0612 Appendix B, the Significance Determination Process as described in MC 0609 and 0609.02 is implemented. In accordance with this SDP, the FINDING will then be evaluated as to whether it is PREDICTABLE AND EXPLOITABLE. For example, a LOSS OF FUNCTION can occur without it being PREDICTABLE AND EXPLOITABLE – hence, a GREEN FINDING characterization would be appropriate. However, licensees must place such items into their corrective action program as described below in Section 5.**
- (4) This SDP has two distinct branches for “FAILURE TO COMPLY” (Sheet 2) and “ACTUAL EVENT IMPLEMENTATION PROBLEM” (Sheet 3). When a FINDING has been confirmed to be PREDICTABLE AND EXPLOITABLE, it shall be assessed through both paths, where applicable, and the most significant FINDING issued. Additionally, some FINDINGS have multiple contributing issues, and the significance of each issue should be assessed. Parallel issues (i.e., more than one issue associated with a given FINDING), shall be noted in the inspection report, but only the most significant FINDING shall be issued. For example, an implementation problem during an actual event may also reveal a LOSS OF SPPF/RSPPF. If the LOSS OF FUNCTION is more significant, it would dictate the color of the**

FINDING. Alternatively, a **FAILURE TO COMPLY** with a **SPPF** may accompany a **FAILURE TO COMPLY** with an **RSPPF**. Inclusion of all associated issues in the inspection report provides a complete record and is particularly important when additional information from the licensee causes the staff to reconsider its preliminary **FINDING** (e.g., the **FAILURE TO COMPLY** with the **RSPPF** but not the **FAILURE TO COMPLY** with the **SPPF** in the above example).

3.0 ACTUAL EVENT IMPLEMENTATION PROBLEMS

3.1 Background

This branch of the SDP is used when a **FAILURE TO COMPLY** with **REGULATORY REQUIREMENTS** occurs during an actual event.¹ Performance problems exhibited during an actual event should be noted as opportunities to improve; however, they do not raise a regulatory issue unless they involve a **FAILURE TO COMPLY**.

As defined in Section 2.1 of this appendix, a **FAILURE TO IMPLEMENT** is a **FAILURE TO COMPLY** with **REGULATORY REQUIREMENTS** during an actual event in which the failure precluded effective implementation (only) of **PROGRAM ELEMENTS**. Generally, a **FAILURE TO IMPLEMENT** occurs as a result of a performance problem. In such instances, the **PROGRAM ELEMENT** is adequate as designed and, if implemented as designed, the Plan meets the **FUNCTION**.

A **FAILURE TO IMPLEMENT** is an item of noncompliance. It is important to note, however, that some performance problems that occur during an actual event may not rise to the level of a **FAILURE TO IMPLEMENT**

However, a **FAILURE TO IMPLEMENT** is not always a result of a performance problem and may, in fact, reveal that a **PROGRAM ELEMENT** is not adequate. In this case, inspection is appropriate to determine whether there is a **LOSS OF RSPPF/SPPF FUNCTION**. Resulting issues would be assessed for significance in accordance with the criteria for a **LOSS OF FUNCTION**.

3.2 Criteria

The Plan(s) were not implemented as appropriate for the security condition . This is generally determined by reviewing licensee performance during an actual event for compliance with regulations and Plan commitments.

3.3 Considerations

Review the affected **FUNCTION**. If the poor performance had little impact on the affected **FUNCTION**, it may be appropriate to note the performance problem as an opportunity to improve (or perhaps a minor violation), rather than a **FAILURE TO IMPLEMENT**.

¹ Flowchart Sheet 3 is used when determining the significance of an actual event implementation problem.

4.0 FAILURE TO COMPLY

As defined in Section 2.1 of this appendix, FAILURE TO COMPLY means that a program is noncompliant with a REGULATORY REQUIREMENT². LOSS OF FUNCTION means that PROGRAM ELEMENTS are not adequate, not compliant with REGULATORY REQUIREMENTS, or otherwise not functional to such an extent that the FUNCTION is not available for a security response.

It may be that the Plan commitments are not met or are inadequate, implementing procedures are inadequate, program design is inadequate, training is inadequate, etc. The result is that if the suspect PROGRAM ELEMENT was not implemented as designed, or personnel are not capable of implementing the PROGRAM ELEMENT, the specific FUNCTION would not be met. Compliance with REGULATORY REQUIREMENTS is necessary. However, the FUNCTION is identified for the purpose of determining the significance of a FAILURE TO COMPLY. This Section provides examples of the LOSS OF FUNCTION.

A LOSS OF FUNCTION is more significant than a FAILURE TO COMPLY with individual requirements. However, functionality does not require compliance with every requirement. The failure of a program to comply with one or even a few of the associated requirements does not necessarily mean a LOSS OF FUNCTION. Consequently, it must be determined whether the FUNCTION is met, even with the noncompliance. If the FUNCTION is met, there is a FAILURE TO COMPLY without a LOSS OF FUNCTION.

A LOSS OF RSPPF FUNCTION results in either a WHITE or YELLOW FINDING. However, there may be instances in which the RSPPF FUNCTION is degraded, but not lost. These cases warrant a FINDING, but a FAILURE TO COMPLY that does not rise to the level of a degraded RSPPF would result in a GREEN FINDING.

[Section References in FUNCTION bullets below are from NEI 03-12, Template for the Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, [and Independent Spent Fuel Storage Installation Security Program]]

Standard Physical Protection FUNCTIONS (SPPF)

1. FUNCTION # 1 -- Administrative

The licensee has developed and implemented programs for administrative duties outlined in the Physical Security Plan that are not covered in another Function.

DEGRADATION OF THE FUNCTION (GREEN) would include:

FAILURE TO IMPLEMENT administrative requirements as described in the physical security program

LOSS OF FUNCTION (WHITE) would include:

None

² Flowchart Sheet 2 is used when determining the significance of a FAILURE TO COMPLY.

FUNCTION Includes: (Security Plan References)

- ❑ Review, Evaluation & Audit of Security Program – 12.0
- ❑ Records – 17.0
- ❑ Digital Systems Security – 18.0
- ❑ Temporary Suspension of Security Measures – 19.0
- ❑ Work Hour Controls – 5.5
- ❑ Testing and Maintenance of Firearms – 15.6
- ❑ **SAFEGUARDS INFORMATION**
- ❑ Security Personnel Equipment – 5.4
- ❑ Testing and Maintenance of Personnel Equipment – 15.5

2. FUNCTION #2 -- Training and Qualification -- (Appendix B – Training and Qualification Plan, NEI 03-09)

The licensee has developed and implemented a training program for Security Force personnel to implement the requirements of the plant physical security plan and contingency plan.

DEGRADATION OF THE FUNCTION (GREEN) would include:

Training program is not consistent with training requirements.

LOSS OF FUNCTION (WHITE) would include:

None

FUNCTION Includes: (Security Plan References)

- ❑ Employment Suitability and Qualification – Appendix B – 2.0
- ❑ Individual Training and Qualifications – Appendix B – 3.0
- ❑ Team Training – Appendix B – 4.0
- ❑ NEI 03-09
- ❑ Quarterly Tactical Drills
- ❑ Correctly identifying requalification requirements using the Difficulty, Importance and Frequency Analysis.

3. FUNCTION # 3: DRILL/EXERCISE (including Force-on-Force) Program

The licensee has developed and implemented a DRILL/EXERCISE program in accordance with the site's training and qualification plan.

DEGRADATION OF THE FUNCTION (GREEN) would include:

Non- licensee identified **WEAKNESSES** in implementation of a valid protective strategy.

FUNCTION Includes: (Security Plan References)

- ❑ Training and Qualification Plan
- ❑ NEI 03-01
- ❑ A force-on-force exercise program is established in accordance with the Training and Qualification Plan
- ❑ Annual exercises are assessed via a formal CRITIQUE process in order to identify WEAKNESSES.
- ❑ Identified WEAKNESSES are corrected.

- Periodic drills are performed to test the protective strategy and to identify WEAKNESSES for corrective action.

4. **FUNCTION #4 Access Authorization/Fitness for Duty – 9.1**

The licensee has established pre-access and ongoing access authorization and fitness for duty for all personnel granted unescorted access.

DEGRADATION OF THE FUNCTION (GREEN) would include:

A deficiency which has lead to unescorted access being granted to personnel, who under the provisions of NEI 03-01 or Part 26, should not have been granted unescorted access and an entry to the PA was achieved.

LOSS OF FUNCTION (WHITE) would include:

A programmatic deficiency, that is PREDICTABLE AND EXPLOITABLE which has lead to unescorted access being granted to personnel, who under the provisions of NEI 03-01 or Part 26, should not have been granted unescorted access and an entry to the PA was achieved.

FUNCTION Includes: (Security Plan References)

- Insider Mitigation Program – 9.2
- NEI 03-01
- Fitness for Duty Program

5. **FUNCTION # 5 Personnel and Material ACCESS CONTROL Process – 9.0**

The licensee has established procedures and equipment for ACCESS CONTROL for personnel and vehicles entering the protected and vital areas. The licensee has established procedures for material control and accountability. Degradations are compensated in accordance with the site's physical security plan.

DEGRADATION OF THE FUNCTION (GREEN) would include:

Failure of search equipment not compensated for in accordance with the physical security plan and associated procedures

LOSS OF FUNCTION (WHITE) would include:

PREDICTABLE AND EXPLOITABLE non-compensated degradation of search and ACCESS CONTROL equipment that resulted in weapons or explosives entering the protected area.

FUNCTION Includes: (Security Plan References)

- Picture Badge System – 9.3
- Searches – 9.4
- PA Packages and Materials Search – 9.4.2
- PA Vehicle Search – 9.4.3
- PA Personnel Search – 9.4.4
- PA ACCESS CONTROL – 9.5
- Escort and Visitor Requirements – 9.5.1
- Vital Area ACCESS CONTROL – 9.6

- Testing and Maintenance of Special Purpose Detectors (metal detectors, explosives detectors, and package X-ray examination devices) – 15.3
- Material controls and accountability

Risk Significant Physical Protection FUNCTIONS (RSPPF)

1) FUNCTION #6. Barrier Defense in Depth

Barrier defense in depth is design, installation, and maintenance of owner controlled area, protected area and vital area barriers, keys locks and combinations. Degradations are compensated in accordance with the site's physical security plan.

DEGRADATION OF THE FUNCTION (GREEN) would include:

Degradation of a owner controlled area, protected area or vital area physical barrier not compensated in accordance with the Physical Security Plan and associated procedures.

SIGNIFICANT DEGRADATION OF THE FUNCTION (WHITE) would include:

A PREDICTABLE AND EXPLOITABLE degradation of a owner controlled area, protected area or vital area physical barrier not compensated in accordance with the Physical Security Plan and associated procedures.

LOSS OF FUNCTION (YELLOW) would include:

A PREDICTABLE AND EXPLOITABLE failure in barrier defense-in-depth caused by a non-compensated degradation of multiple barriers that would have allowed concurrent access to protected and vital area TARGET SETS sufficient to permit a release in excess of 10CFR100 limits.

Discovery of design deficiencies that would allow unauthorized vehicles or personnel to proceed beyond the stand-off distances, or access the protected area, or vital areas or TARGET SET equipment sufficiently to permit damage to equipment which could allow a release in excess of 10CFR100 limits.

A PREDICTABLE AND EXPLOITABLE non-compensated degradation of one or more delay barriers that would render the protective strategy ineffective.

FUNCTION Includes: (Security Plan References)

- 1) Keys, Locks and Combinations
- 2) Protected Area Barriers – 6.2
- 3) Vital Area Barriers – 6.3
- 4) Delay Barriers in accordance with the Site's Protective Strategy– 6.4
- 5) Compensatory Measures for PA – 16.1
- 6) Compensatory Measures for VA Barriers– 16.2

- 7) Compensatory Measures for VA Portals – 16.5
- 8) Compensatory Measures for Protected Area Control Device (i.e. Turnstile System) – 16.8

2) **FUNCTION #7: Vehicle Barriers**

The licensee has designed, installed, and maintains vehicle barrier systems and performs searches at VBS checkpoints to protect against the DBT bomb. Degradations are compensated in accordance with the site's physical security plan.

DEGRADATION OF THE FUNCTION (GREEN) would include:

Degradation of a physical vehicle barrier not compensated in accordance with the Physical Security Plan and associated procedures.

SIGNIFICANT DEGRADATION OF THE FUNCTION (WHITE) would include:

A PREDICTABLE AND EXPLOITABLE degradation of a physical vehicle barrier not compensated in accordance with the Physical Security Plan and associated procedures..

LOSS OF FUNCTION (YELLOW) would include:

Non-compensated PREDICTABLE AND EXPLOITABLE degradation of one or more vehicle barriers such that a **DESIGN BASIS THREAT** vehicle could enter and damage TARGET SETS sufficient to permit a release in excess of 10CFR100 limits.

Discovery of design deficiencies that would allow unauthorized vehicles or personnel to enter the stand-off distances, protected area, or vital area TARGET SETS sufficient to permit a release in excess of 10CFR100 limits. [See IMC 0305 for design deficiencies].

FUNCTION Includes: (Security Plan References)

- Vehicle Barrier System - 6.1
- VBS Checkpoint Search – 9.4.1
- Compensatory Measures for Vehicle Barrier System – 16.9
- Vehicle Barrier Inspection

3) **FUNCTION # 8 Assessment and Detection**

The licensee has designed, installed and maintains equipment used to detect and assess unauthorized entrance into the Protected and Vital Areas. Degradations are compensated in accordance with the site's physical security plan.

DEGRADATION OF THE FUNCTION (GREEN) would include:

Degradation of the IDS or assessment capabilities, which are not compensated for, in accordance with the Physical Security Plan and associated procedures.

SIGNIFICANT DEGRADATION OF THE FUNCTION (WHITE) would include:

A PREDICTABLE AND EXPLOITABLE degradation of the IDS or

assessment capabilities, which are not compensated for, in accordance with the Physical Security Plan and associated procedures.

LOSS OF FUNCTION (YELLOW) would include:

A PREDICTABLE AND EXPLOITABLE non-compensated degradation of one or more IDS and assessment system capabilities at the PA and Vital Area boundary concurrently such that there would be undetected access to TARGET SETS sufficient to permit a release in excess of 10CFR100 limits.

FUNCTION Includes: (Security Plan References)

- Illumination – 10.1
- Surveillance – 10.2
- Perimeter INTRUSION Detection
- Closed Circuit Television
- Alarm/Annunciation Equipment – 10.3
- Central Alarm Station/Secondary Alarm Station – 10.4
- Patrols – 10.5
- Compensatory Measures for Protected Area Lighting – 16.4
- Compensatory Measures for Closed Circuit Television/Non-Fixed Camera Systems – 16.6
- Compensatory Measures for Security Computer System – 16.7
- Waterborne Threat Measures – 9.7

4) FUNCTION # 9: Protective Strategy – 13.0

The licensee has performed an analysis of TARGET SETS and has developed a protective strategy to defend TARGET SETS against the Design Basis Threat.

DEGRADATION OF THE FUNCTION (GREEN) would include:

Inadequate documentation of protective strategy that does not accurately reflect strategy being implemented.

SIGNIFICANT DEGRADATION OF THE FUNCTION (WHITE) would include:

Licensee strategy is invalid due to facility procedures, systems or equipment which create a condition such that protection of a TARGET SET would not be achievable which could result in a release in excess of 10CFR100 limits.

LOSS OF FUNCTION (YELLOW) would include:

Licensee strategy is invalid due to facility procedures, systems or equipment which create a condition such that protection of multiple TARGET SETS would not be achievable which could result in a release in excess of 10CFR100 limits. .

FUNCTION Includes: (Security Plan References)

- TARGET SET Analysis
- Contingency Response – Safeguards Contingency Plan (Appendix C)
- Site Protective Strategy

- Response Protocol with Law Enforcement Responders – 5.3
- Delay barriers -6.4, and defensive fighting positions -7.0
- Communications -11.0.

4.1 GUIDANCE ON DRILL AND EXERCISE CRITIQUE PROBLEMS

Background

This section provides guidance regarding issues that inspectors may identify through the baseline program inspection of licensee DRILLS AND EXERCISES. Inspection Procedures instruct inspectors to observe DRILLS AND EXERCISES, and identify WEAKNESSES (i.e., a demonstrated level of performance that could preclude effective implementation of the Safeguards Contingency Plan in an actual emergency). A CRITIQUE PROBLEM occurs when the licensee fails to identify the WEAKNESS(ES) observed by the inspector.

The SDP stratifies the significance of a failure to CRITIQUE a WEAKNESS as either GREEN or WHITE, as follows:

- A CRITIQUE that fails to identify a WEAKNESS associated with an RSPPF that is determined to be a failure during a DRILL OR EXERCISE, represents a LOSS OF FUNCTION that is potentially a WHITE FINDING.
- A CRITIQUE that fails to identify a WEAKNESS resulting from a performance problem, associated with an SPPF during a DRILL OR EXERCISE is potentially a GREEN FINDING.

RSPPF performance problems should be given the highest priority in the CRITIQUE process. Thus, a licensee's ability to observe, evaluate, and CRITIQUE a WEAKNESS associated with an RSPPF is critical. The overall expectation is that the licensee's CRITIQUE will emphasize evaluation of performance in the RSPPF areas. When the CRITIQUE identifies a WEAKNESS and it is appropriately corrected, it should be considered a strength of the CRITIQUE process.

Licensees perform CRITIQUES in many different ways and the baseline inspection instructs inspectors to be flexible in accepting mechanisms for problem identification. The critical feature of any CRITIQUE is that a WEAKNESS is captured and entered into a corrective action system with appropriate priority. If the WEAKNESS is entered into a corrective action system, prior to disclosing a FINDING, the CRITIQUE should be considered successful.

A WEAKNESS that was missed by the CRITIQUE must be a demonstrated level of performance that could preclude effective implementation of the Safeguards Contingency Plan in an actual emergency. Some missteps in performance may not rise to the level of a WEAKNESS and/or were corrected by subsequent actions. An example would be the coaching of an individual due to the individual's performance failure.

CRITIQUE processes differ among licensees, and a licensee should be given credit if the WEAKNESS was entered into a corrective action process, regardless of whether the WEAKNESS was verbalized at a CRITIQUE meeting.

The disposition of CRITIQUE FINDINGS also varies among sites. The licensee must evaluate numerous evaluator observations and prioritize resources for correction. Indeed, some evaluator suggestions may be counterproductive, as determined by responsible management. Care should be taken to understand the logic underlying the suggested disposition before identifying it as a CRITIQUE PROBLEM. However, a licensee's disregard for well-founded evaluator-identified WEAKNESSES should be considered to be a CRITIQUE PROBLEM (e.g., if the WEAKNESS would have been a FAILURE TO IMPLEMENT in an actual event, the NRC expects the licensee to capture the WEAKNESS in the CRITIQUE and enter it into a corrective action program).

The Plan contains the licensee's commitments. The implementing procedures are the licensee's methods of implementing those commitments and may be used to judge effective, timely, and accurate implementation. If either the Plan or the procedures are inadequate, it is not a DRILL/EXERCISE CRITIQUE issue. Rather, it is a FAILURE TO COMPLY, and the applicable section should be used to assess significance. Licensee mistakes and missteps that only detract from implementation should not initially be considered WEAKNESSES. Mistakes are likely to happen in the course of an exercise, and when such mistakes are corrected, it reveals an organizational strength rather than a WEAKNESS.

5.0 CORRECTIVE ACTIONS

5.1 Introduction

The Physical Protection Cornerstone of the NRC Reactor Oversight Process is based on the licensee response band established by the PI program and the licensee's Corrective Action Program (CAP). As it relates to physical protection, CAP encompasses the drill and exercise CRITIQUE program, CRITIQUE of actual events and other assessment activities (such as QA audits, self assessments and reviews performed in accordance with 10 CFR, as well as the corrective action program. The NRC's Baseline Inspection Program provides oversight of a licensee's efforts to CRITIQUE drills and exercises and correct WEAKNESSES.

The Safeguards Cornerstone is designed to foster drill and exercise programs that develop and maintain security organization skills. It is the nature of a drill program that performance errors will occur and equipment, facility and procedure problems (WEAKNESSES) will surface. The identification and correction of these WEAKNESSES is a positive and vital aspect of the program. The regulations require licensees to correct any WEAKNESS(ES) identified during training, drills and exercises.

5.2 Timeliness

This section provides guidance regarding the timeliness of a licensee's correction of identified WEAKNESSES. However, this guidance should not be interpreted as a requirement. Rather, this guidance describes when it is appropriate for an inspector to review the timeliness of a licensee's corrective action efforts. Corrective actions may be temporary, such as implementing compensatory measures, or may be long-term such as a plant modification. Licensee corrective action timeliness should be evaluated to ensure that the actions are appropriately prioritized and scheduled, and are commensurate with the safety significance of the issue.

The licensee determines the safety-significance of WEAKNESSES and sets priorities in accordance with commitments and the CAP. The NRC staff assesses the appropriateness of those priorities in the context of the issue. The timeliness guidance may be used as a limit for inspector involvement (e.g., if the WEAKNESS is corrected in a shorter time than that suggested in the guidance, the inspector probably does not need to review the basis for the timeliness of corrective actions).

Root cause analyses, common cause analyses, and other analyses may take 60 days or longer, in some cases, to complete. While immediate corrective actions, such as briefings or lessons-learned summaries may be implemented rapidly, they may not represent actual correction of the WEAKNESS. The licensee must resolve problems in a manner that is appropriate to the risk-significance. While that will often be accomplished in less time than suggested below, there may be times when a licensee should take more time. When the time is longer than that prescribed by the timeliness guidance, the inspector should review the scheduling rationale for reasonableness and any potential to impact public health and safety. Should a corrective action be scheduled in a manner that is not reasonable or potentially impacts public health and safety (in that the Plan can not be implemented effectively), a FINDING may be appropriate for FAILURE TO COMPLY.

Corrective action systems may track enhancement suggestions that result from the drill program. These enhancement suggestions often add value to the program, but are not required and do not address WEAKNESSES. There is no NRC timeliness expectation for resolution of enhancement suggestions.

5.2.1 Criteria

These criteria are to be used when the timeliness of the resolution of a drill or exercise performance WEAKNESS is not appropriate for its risk-significance. If the problem is RSPPF-related, the failure to correct the FINDING in a timely manner should be considered a LOSS OF FUNCTION. Otherwise, it should be considered a FAILURE TO COMPLY with REGULATORY REQUIREMENTS (i.e., a GREEN FINDING).

5.2.2 Considerations

It is not appropriate to consider the timeliness of enhancement items. However delay of corrective actions greatly exceeding suggested guidance and deemed as inappropriate in view of the significance of the WEAKNESS should be considered LOSS OF FUNCTION.

5.3 Failure To Correct DRILL/EXERCISE WEAKNESS

Determination of a failure to correct a DRILL/EXERCISE WEAKNESS requires a detailed review of the WEAKNESS and the associated corrective actions. It is not intended that a single repetition of a DRILL/EXERCISE WEAKNESS should automatically be deemed to be a failure of the CAP. Conversely, success in a drill or exercise (e.g., by one well-drilled team) should not necessarily be considered a demonstration of problem resolution. When an apparent failure to resolve a problem is observed, review specific corrective actions, as well as similar occurrences in response to actual events, and DRILL/EXERCISE. Also consider the status of relevant PIs and review corrective action, self-assessment and inspection records with emphasis on similar problems. In addition, verify completion of corrective actions. Assessment of the effectiveness of the corrective actions should be based on the complete history of the issue. Obtain a reasonably complete picture of the current problem by reviewing previous corrective actions. The intent is to see a pattern of recurring performance problems in similar activities in order to identify ineffective corrective actions.

MC0612 – APPENDIX B
Issue Disposition Screening

Use Figure 1 and the below listed questions to determine if a finding has sufficient significance to warrant further analysis or documentation. The decision points in the process outlined in Figure 1 are discussed in detail below.

A. Performance Deficiency Question

A founding principal of the reactor oversight assessment process is that only those issues that are determined by the staff to be licensee performance deficiencies are entered into the licensee performance assessment process. Therefore, an issue must be a “performance deficiency” before it can be considered a finding.

If the issue is not a performance deficiency, it may still require NRC action outside of the ROP and should be addressed by other agency means as appropriate (e.g., generic communications). However, if the issue is a greater than minor violation of NRC requirements, it must be documented in accordance with applicable Enforcement Policy. These issues are rare and should be evaluated with close management oversight on a case-by-case basis.

B. Enforcement Questions

Certain issues are documented under all circumstances, even if the issue is minor. A positive response to any of the following questions requires that the issue be documented as a finding. Findings related to traditional enforcement are expected to be a small fraction of all findings. The significance of these findings should be assessed by NRC management. Typically, a Severity Level would be assigned after consideration of appropriate factors for the particular regulatory process violation in accordance with the NRC Enforcement Policy. Therefore, these findings should also be evaluated by the SDP, if applicable, in order to consider the associated risk significance of the finding prior to assigning a severity level. If evaluated by an SDP the significance color should be entered into the IMC 0305 Operating Reactor Assessment Program action matrix in parallel with enforcement actions.

(1) Does the issue have actual safety consequence (e.g.: overexposure, actual radiation release greater than 10CFRPart 20 limits)?

(2) Does the issue have the potential for impacting the NRC's ability to perform its regulatory function? For example, a failure to provide complete and accurate information or failure to receive NRC approval

MC0612 – APPENDIX B Issue Disposition Screening

for a change in licensee activity, or failure to notify NRC of changes in licensee activities, or failure to perform 10CFR50.59 analyses etc. (see Enforcement Policy IV.A.3)

(3) Are there any willful aspects of the violation?

If the answer to any of the enforcement questions is "Yes" the finding should first be discussed with regional management and may be referred to the Office of Enforcement for assignment of a Severity Level. If all answers to the above questions are "No", the inspector should next determine whether the finding is minor.

C. Minor Questions

The inspector should first compare the finding to those findings identified in Appendix E to determine whether the finding is minor. If the finding is similar to the minor findings identified, the issue should be considered minor. If the guidance in Appendix E is not applicable or is not useful for the specific finding, the inspector should then attempt to answer each of the below questions. Answering "Yes" to any of the below questions indicates that the finding should be documented as greater than minor.

- (1) Could the finding be reasonably viewed as a precursor to a significant event?
- (2) If left uncorrected would the finding become a more significant safety concern?
- (3) Does the finding relate to performance indicators that would have caused the PI to exceed a threshold?
- (4) Is the finding associated with one of the below cornerstone attributes and does the finding affect the associated cornerstone objective?

If the answer is "No" to all of the above questions, the finding should be considered minor. If the finding is associated with a below listed attribute, but did not affect the respective cornerstone objective, the finding should be considered minor. If the cornerstone objective is affected, the finding is greater than minor and warrants documenting.

In all cases, minor findings should have no actual safety consequences, little to no potential to impact safety, no impact on the regulatory process, and no willfulness. If the finding is determined to be minor, the inspector should not document the finding.

MC0612 – APPENDIX B Issue Disposition Screening

D. SDP Question

Can the finding be evaluated using the SDP?

If the finding can be processed by the applicable SDP, it should be assigned a color, and documented in the inspection report. Questions for each cornerstone are provided below as an aid in identifying the correct SDP that may be applicable, however the governing SDP guidance is found in IMC 0609.

SAFEGUARDS

CORNERSTONE – Physical Protection

- (1) Is the finding associated with or involve a failure to meet the requirements of 10CFR73.55 (b)-(h), or associated plans, procedure or rules?
- (2) Is the finding associated with or does it impact any key attribute of the Physical Protection Cornerstone to meet its intended function whether in performance, design or implementation?

E. Non-SDP Findings

The non-SDP finding shall, as a minimum, be reviewed by a member of NRC management familiar with NRC requirements in the area inspected to ensure that the finding is greater than minor and not greater than very low safety significance. This review shall ensure that inspector's findings are consistent with NRC policies and requirements and that enforcement-related findings are addressed in accordance with the NRC Enforcement Policy and the NRC Enforcement Manual. Examples of these findings typically involve concerns relating to (1) the collection or reporting of performance indicators that would have caused a PI to exceed a threshold, (2) documenting a finding necessary to close an open item such as a licensee event report, (3) technical information relating directly to an issue of agency-wide concern (i.e., generic safety issues), and (4) other greater than minor findings related to NRC requirements where no SDP exists.

F. Non-Performance Deficiencies

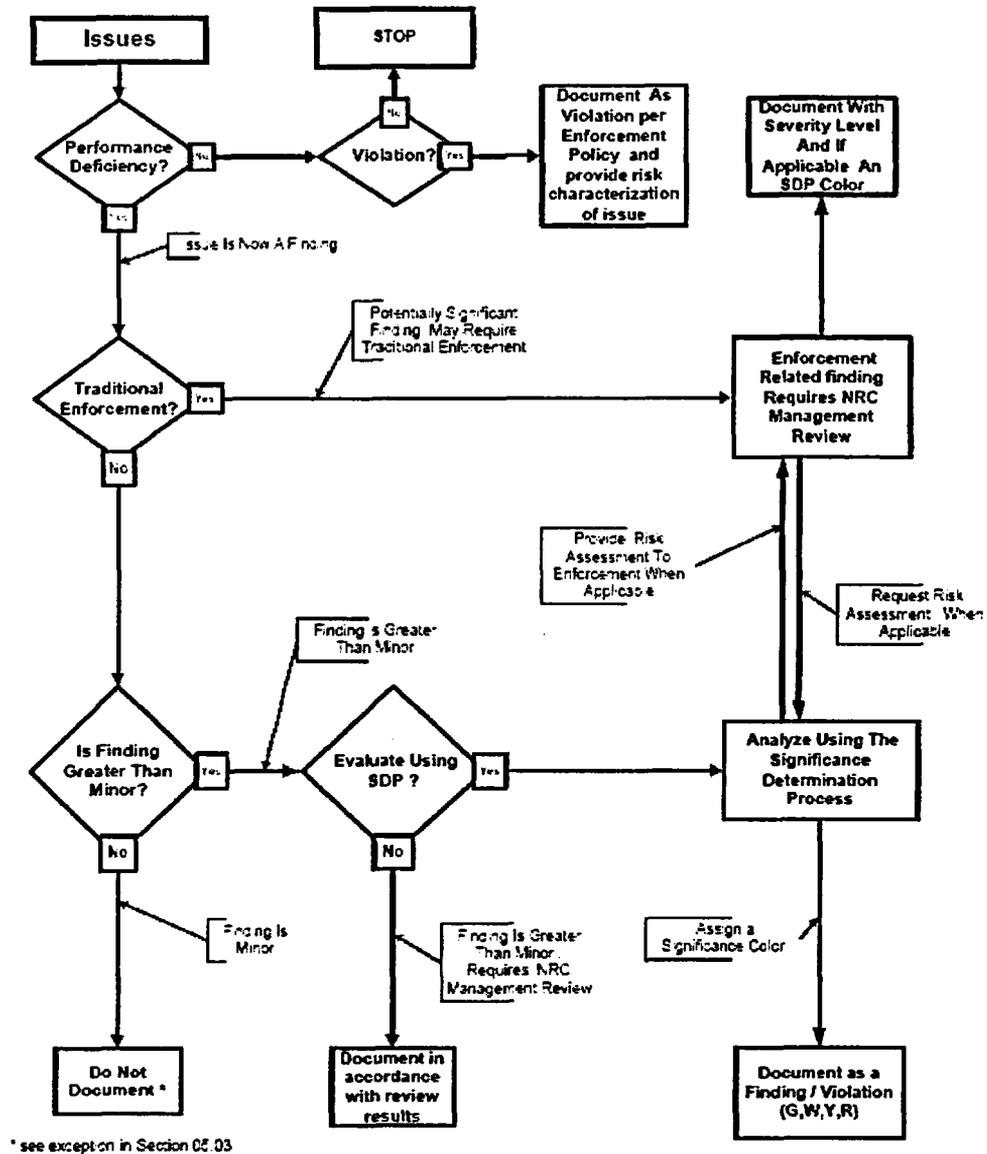
Issues which are determined not to be licensee performance deficiencies, but which constitute a violation of NRC requirements must be documented in accordance with applicable sections of the Enforcement Policy. This includes a determination that

MC0612 – APPENDIX B Issue Disposition Screening

the violation is greater than minor and may also warrant enforcement discretion per Section 06.03.a.4 of this Chapter.

MC0612 – APPENDIX B Issue Disposition Screening

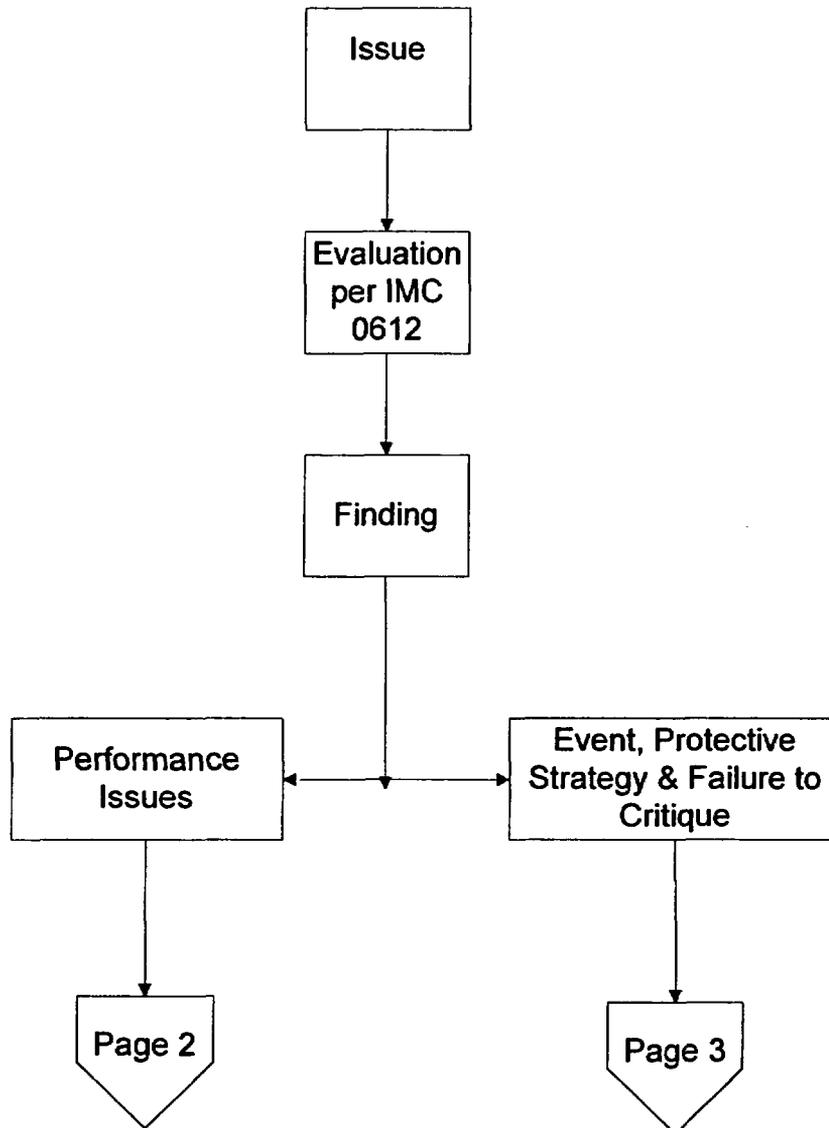
Figure 1



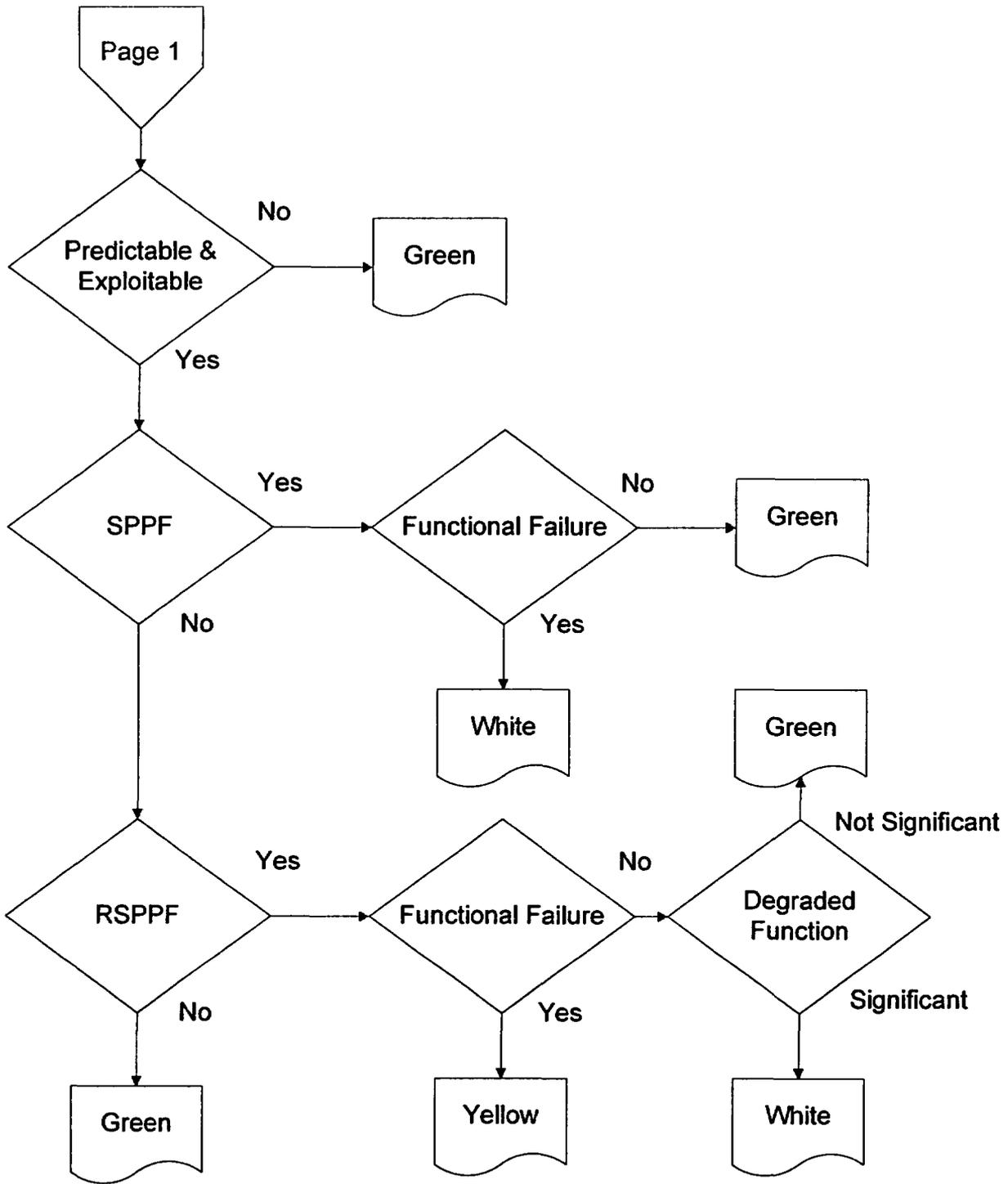
PHYSICAL PROTECTION SIGNIFICANCE DETERMINATION PROCESS

Issue Dispositioning Screening

Flowchart 1



Flowchart 2



Flowchart 3

