Stakeholder Comment Review is broken down as follows:

1. Draft Regulatory Guide DG-5022 Stakeholder Comments from 7-18-2008 (Pages 2-53)

2. Draft Regulatory Guide DG-5022 Stakeholder Comments from 12-12-2008 (Pages 54-64)

3. Draft Regulatory Guide DG-5022 Stakeholder Comments from 1-14-2009 (Pages 64-66)


**CYBER SECURITY**

**STAKEHOLDER ANALYSIS**

**STAKEHOLDER COMMENTS FROM JULY 18, 2008 MEETING ON DRAFT REGULATORY GUIDE DG-5022 "CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES"**

January 27, 2009

## 0. GENERAL

0.0 Introduction

The following document provides an overview forum for the discussion of the recent public comments on the draft Regulatory Guide DG-5022. The structure of the document filters and resolves the comments in to the proper overview venue as related to the draft guide. The comments are assessed in comparison to core values of DG-5022.

0.1 How to use this document:

The working areas are divided into a number of **Venue**(s). The total number of venues is part of the initial review process. Comments under a certain Venue are again review and moved into one of the following working areas: **NRC Positions, Assumptions, Best Practices and Questions**. The feedback comments are then reviewed for their feature value. The working areas have the following definitions and rules:

**NRC Position:** This area is reserved the Regulatory Guide's firm position and primary purpose. The stated requirement provides a core value that either the comments will match or disagree with.

**Best Practices:** This area is for comments that will assist with the creation of the NUREG. The public comment could also disagree with a future approach and opens the issue for discussion.

**Stakeholder Assumptions:** Are rumored directions and open comments with limited rigor for design or knowledge of that venue. The comments in this area are under challenge and are resolved as part of the Requirements / Best Practices or rebuked with supporting conclusions.

**Stakeholder Questions:** This area provides a place for stated concerns and possible solutions that the Regulatory Guide or NUREG can resolve for the stakeholder with further feedback from the staff.

The staff reviewed the comments and defined the required resolution from the past stakeholder meeting. The over all outcome provides an opportunity to improve the Regulatory Guide with the stakeholder's participation.

0.2 The Participants:

Stakeholders Comments - (NEI, STARS, FPL, & TVA)
The NRC staff

0.3 Comment Summarization:

The comments varied through the draft guide from questions / assumptions to direct statements. There are heavy levels of cynicism and at the same time several good

questions/concerns. Below in Table A there are approximately 208 comments from NEI, TVA, FPL and STARS broken in too the 6 categories that are woven in the analysis document.

Table A

| | DG-5022 Document Sections | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Features | A | B | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | D | Gls | App. A | App. B | Totals |
| Questions | 3 | 2 | 7 | 4 | 7 | 32 | 16 | 4 | 16 | 2 | 7 | 1 | 0 | 7 | 1 | 0 | 3 | 2 | 114 |
| Assumptions | 6 | 5 | 2 | 18 | 14 | 20 | 6 | 3 | 3 | 1 | 4 | 2 | 4 | 4 | 0 | 1 | 1 | 1 | 95 |
| | 9 | 7 | 9 | 22 | 21 | 52 | 22 | 7 | 19 | 3 | 11 | 3 | 4 | 11 | 0 | 1 | 4 | 3 | 208 |
| Scope | 4 | 0 | 4 | 12 | 5 | 16 | 5 | 5 | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 55 |
| Move | 0 | 0 | 0 | 0 | 0 | 11 | 10 | 1 | 9 | 2 | 5 | 1 | 0 | 0 | 0 | 0 | 2 | 1 | 42 |
| Delete | 0 | 0 | 0 | 0 | 2 | 17 | 0 | 0 | 0 | 0 | 0 | 1 | 3 | 4 | 0 | 0 | 0 | 0 | 27 |
| Terminology | 4 | 0 | 3 | 3 | 0 | 6 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 18 |
| Organization | 0 | 0 | 0 | 0 | 7 | 2 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 11 |
| Technical | 0 | 0 | 0 | 0 | 0 | 6 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 8 |

The first 3 areas (Scope, Move & Delete) have the highest number of comments. The comments were over all a repeated request to move the detail into the appendix or a NUREG. The next category - Terminology explains the miss understanding of certain words and phrasing in which the Stakeholder did not understand requirements of the draft guide.

The Organization comments are mostly in response to the draft guide's request to review the licensee's cyber security program as part of their physical security program. There are a limited number of Technical type questions/assumptions and these low numbers again demonstrate that the Stakeholder would rather create their own scope and reject the requirements under DG-5022.

**1. DG-5022; A. Introduction** **Tactical Rating: Low**

**1.1 Venue** - A. Introduction

| NRC Positions | Who | Touch Points | Priority |
|---|---|---|---|

NRC Response: Not Applicable (N/A)

**1.2 Best Practices:** N/A

**1.3 Stakeholder Questions:**

1. (NEI - p5) DG 5022, p1 - "…interface systems and networks…"

   NEI - asks for a definition of this term.

2. (NEI - p5) DG 5022, p2 - "... high assurance…"

   NEI - asks for a definition of this term.

3. (NEI - p6) DG 5022, p6 - "This initiative culminated in the submittal by NEI of NEI 04-04 Rev. 1, *"Cyber Security Program for Power Reactors,"* (Ref. 10), to the NRC. At that time, the NRC's Digital Instrumentation and Control research and development program elements regarding cyber security were not yet completed. However, the NRC staff evaluated the NEI submittal and communicated in a letter to NEI dated December 23, 2005, that NEI 04-04 provided an acceptable approach for licensees to formulate their cyber security programs."

   NEI asks is NEI 04-04 still an acceptable approach or not?

**1.4 Stakeholder Assumptions:**

1. (TVA - p1) DG 5022, p1 - "nuclear critical system and networks", however 10CFR73.54 say: "important-to-safety."

   TVA - This term could be interpreted to include systems that do not impact the ability to shutdown the plant and maintain the plant in a safe shutdown condition.

   NEI asks if the term "Nuclear Significant" or "nuclear significant systems and networks" be used instead of "nuclear critical systems and networks".

2. (TVA, p1) DG 5022, p2 - "Cyber attacks may arise from internal source,… " & Cyber attacks may also involve physical attacks…"

TVA - claims they already mitigate by existing programs.

NEI - Ditto

NEI - believes that "inadvertent actions" are not considered a cyber threat.

NEI - believes physical protection of hardware from theft is not a cyber security issue and is covered by the physical security program.

**2. DG-5022; B. Discussion** **Tactical Rating: Low**

**2.1 Venue -**

| NRC Positions | Who | Touch Points | Priority |
|---|---|---|---|

NRC Response to Comment 7:

Although there is no definitive proof that "Many nations" are investing resources to develop capabilities to allow them to mount cyber attacks, there is plenty of inferred evidence (e.g. the attack on Georgian cyber infrastructure immediately before the Russian attack). However, to be fully accurate, this statement can be reworded to: "Many entities, both large and small…"

**2.2 Best Practices:** N/A

**2.3 Stakeholder Questions:**

1. (NEI, p2) DG 5022, p7 - "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage."

   NEI questions which systems meet the standard of radiological sabotage?

2. (NEI, p9) DG 5022, p7 - ""Insiders," such as site employees, contractor employees, and vendors, may intentionally or unintentionally damage digital assets or data."

   NEI asks shouldn't DG 5022 explicitly reference RG 5.69 on Insiders, since it provides guidance on Insider Mitigation Programs?

**2.4 Stakeholder Assumptions:**

1. (NEI, p8) DG 5022, p6 - "Among the measures identified within the order, a specific requirement mandated nuclear power plant licensees to identify those digital systems determined to be critical to the operation of the facility. In addition to identifying the critical systems, licensees were also required to evaluate the potential consequences to the facility if any of the identified systems were compromised."

NEI - The order gave general requirements and used the word “consider”.

2. (NEI, p8) DG 5022, p6 - “In Section 73.55 of the Code of Federal Regulations the NRC established performance objectives and requirements for licensee physical protection programs. The incorporation of critical digital systems into the site physical protection program requires that the “high assurance” standard for physical protection is also applicable to the protection of such critical digital assets. Specifically, such digital assets are to be protected through the establishment and maintenance of an on-site physical protection system and security organization which will have as its objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to public health and safety. The material aspects of NRC Orders EA-02-026 and EA-03-086 are withheld from public disclosure in accordance with 10 CFR Part 73, Section 73.21, “Requirements for the Protection of Safeguards Information.”

   NEI - Claims there is no basis for this.

3. (NEI, p9) DG 5022, p8 - “Many nations, both large and small, are currently investing resources to develop capabilities that would allow them to mount successful cyber attacks and to disrupt or damage an adversary’s critical infrastructure. “

   NEI - Does not believe there are facts on so called cyber attacks thus remove this sentence.

4. (NEI, p8) DG 5022, p7 - “Cyber attacks that may impact control systems can come from a variety of sources (i.e., threat agents), including but not limited to

- insiders (e.g., employees, contractors, vendors);
- hackers;
- criminals;
- terrorists; and
- espionage and cyber warfare. “

   NEI assumes the insider threat is addressed by another Regulatory Guide and there is no value list a venue called “Criminals” thus NEI believes this listing should be removed.

   (STARS, p3 #9) For and insider threat RG 5.69 and NEI 03-01 are sufficient for all plant assets within the Protected Area.

## 3. DG-5022; C. Regulatory Position — Tactical Rating: Med

**3.1.1 Venue** - 1. Requirements and Application of Cyber Security Program

| NRC Positions | Who | Touch Points | Priority |
|---|---|---|---|

NRC Response to Comment 7:

Technically, "state of the art" is not suitable as a protective strategy, since these technologies typically have insufficient field testing. As such, these technologies may not be "better" as mitigating cyber attacked, as compared with established technologies. As such, it would be preferable to require the "most up-to-date industry best practices".

**3.1.2 Best Practices:** N/A

**3.1.3 Stakeholder Questions:**

1. (FPL, p2) DG 5022, p9 - "Each *licensee subject to the requirements of this section shall provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks…"*

   FPL comments that neither the Reg nor the DG-5022 provides a definition of "high assurance". FPL suggests adding a new definition to the glossary. (See their recommendation: page 2 comment 1.)

   (NEI, p18) - Define "high assurance" please.

   FPL also would like the DG 5022 term "nuclear critical asset" be changed to NEI 04-04 term "critical digital asset".

   (NEI, p20) - Ditto

2. (NEI, p13) DG 5022, p9 - FOOT NOTE: "A "nuclear critical asset" is an asset that must itself be protected against cyber attack to provide high assurance that nuclear critical systems and assets are adequately protected from cyber attack. A nuclear critical asset is part of, directly connected to, or indirectly connected to a nuclear critical system or network."

   NEI requests clarification of this ambiguous statement.

3. (NEI, p18) DG 5022, p11 - "*The cyber security program shall be audited as a component of the physical security program and will be subject to the same requirements and controls."*

   NEI - How deep is deep? Need clarity. "What is expected?" and "what we understand" based on current ISGs and experience from the physical security lessons learned?

4. (NEI, p18) Dg 5022, p11 - "Cyber Security Plan"

NEI - Is the Cyber Security Plan going to be safeguards information?

**3.1.4 Stakeholder Assumptions:**

1. (TVA -p1) DG 5022 p10 - "apply state of the art in depth protective strategies to ensure the capability to detect and respond to cyber attacks in a timely manner, "

   TVA claims that State-of-Art techs are too stringent and cannot be updated with in outage cycle of 18 months to 2 years and this could be an expense for unproven technology.

   NEI - Ditto

**3. DG-5022; C. Regulatory Position** **Tactical Rating: Med**

**3.2.1 Venue** - 2. Identification of Nuclear Critical Assets

| NRC Positions | Who | Touch Points | Priority |
|---|---|---|---|

NRC response to comment 3:

It should be specified that not "all" disks and thumb drives are classified as "nuclear critical". However, if such a device is ever used to interface with a nuclear critical asset, it must also be classified as nuclear critical.
NRC response to comment 7:

With regards to the "(NEI, p23)" comment: A lack of direct connectivity does not always equate to the system being zero risk (i.e. immune from cyber attacks). Such devices may still be susceptible to EMI, indirect connectivity and/or insider attacks.

**3.2.2 Best Practices:** N/A

**3.2.3 Stakeholder Questions:**

1. (NEI, p21) DG 5022, p12 -"A nuclear critical asset may be a component of a nuclear critical system or network, or it may be directly or indirectly connected to a nuclear critical system or network. The connection may be through a wired or wireless pathway (involving a chain of connections) or involve a *sneaker net* by which data or software is manually carried from one digital device to another and transferred using physically transportable storage medium, such as disks or thumb drives, or other modes of data transfer."

   NEI questions the expanded indirect digital devices such as disks or thumb drives or other modes or data transfer becoming a critical asset.

2. (FPL, p4, 7) DG-5022, p13 - "The licensees can group closely related and interconnected digital assets together to form an individual nuclear critical asset. However, the security controls applied to that nuclear critical asset must apply to every digital asset that makes up the identified nuclear critical asset."

   FPL states that NRC has endorsed the both NUREG/CR-6847 and NEI 04-04. Based on the NEI 04-04 use of the "weakest link" theory shouldn't this assessment process allow more flexibility in determining the appropriate protection? FLP states that COTS products may not be capable of the security controls as required. Other compensation measures maybe used to satisfy the risk category such as: locking a cabinet with the device inside to prevent access.

   (NEI, p19, p26) questions this paragraph and believes it is "an unjustified expansion of scope; not every component that makes up a safety-related SSCX is itself safety-related."

3. (NEI, p19) DG 5022, p12 - Figure C1: Hierarchy of Plant Digital Systems shows a bubble with the wording "Continuity of Power."

   NEI asks is this term stated without a definition? Please add to the definition area of the document.

**3.2.4 Stakeholder Assumptions:**

1. (TVA, p2 & p3) DG 5022, p13 - "The licensees can group closely related and interconnected digital assets together to form an individual nuclear critical asset. However, the security controls applied to that nuclear critical asset must apply to every digital asset that makes up the identified nuclear critical asset."

   TVA claims this is not addressed in 73.54 and NIST 800-53, and security controls are applied to the entire system and not a specific asset. DG 5022 does not agree with NIST.

   (NEI, p26) NEI repeats the above TVA comment on how NIST 800-53 states how a set of defined security controls are applied to the entire system and not a specific asset. Specified controls are either applied or not applied. If not applied, explain why.

   TVA also claims this is not in 73.54 and an unjustified expansion of scope and not analogous to SR equipment. Large cost for documentation and disposition for all digital sub components.

   (FPL, p2, 3) FPL assumes that the NRC has already endorsed NEI 04-04's CDAS (Identify Critical Digital Assets) methodology. The addition grouping would require rework.

   (NEI, p19) NEI requests acknowledgement of the NEI 04-4 term: "critical digital asset".

(NEI, p22) NEI claims the claims the Regulatory Guide security controls "that may be instituted for a digital controller may not be the same for a digital converter."

2. (TVA, p2) DG 5022, p13 - "The NRC staff recognizes that some control and data acquisition systems within a nuclear plant are autonomous (i.e., have no data connections to any other system). The cyber security posture for autonomous systems or networks is greatly enhanced due to the lack of connectivity with other plant systems. This lack of connectivity results in a reduced possibility of compromise from cyber threats originating from sources external to the plant. However, such systems still are vulnerable to cyber attack originating from internal sources. In addition, due to the abundance of off-the-shelf devices and peripherals that support communication technology, the architecture of an autonomous system is altered when such communication devices are intentionally or inadvertently introduced into the system. 10 CFR Part 73, Section 73.54, makes no distinction between autonomous and non-autonomous systems. The security posture of an autonomous system therefore needs to be evaluated with the same diligence that is applied to interconnected systems. "

*"(b) To accomplish this, the licensee shall:*
*(b)(1) conduct a site-specific analysis of digital computer and communication systems and networks to identify those assets that must be protected against cyber attacks to satisfy paragraph (a) of this section,*
*(b)(2) establish, implement, and maintain a cyber security program for the protection of the assets identified through site-specific analysis, and;*
*b)(3) incorporate the cyber security program as a component of the physical protection program."*

TVA does not believe that an autonomous system(s) pose the same risk as a non autonomous system and do not need to be elevated with the same diligence. Autonomous systems are protected under physical security plan.

(FPL, p2, 4) FPL has the same comment as TVA. This change is late and would require substantial additional work.

(FPL, p4, 7) FPL assumes that RG 5.69 provides a good insider mitigation program that can mitigate the effects of active and active-violent insiders.

(NEI, p20) - Ditto

(NEI, p15) NEI believes that the word "autonomous" should be changed to "standalone".

(NEI, p23) NEI states that the NRC gives no credit for the NEI 04-04 and NISTL toolkit, which can show there is no direct connectivity and thus the risk is zero and thus a full assessment and mitigation is not required.

(NEI, p27) NEI comments that the Guide is treating a Nuclear Plant like a data center. Presently autonomous systems are currently protected under the physical security

plan not the cyber security plan. "Part 73, Section 73.54 does not state that there should be no distinction between autonomous and non-autonomous system." Thus assessed autonomous systems should be excluded from further assessment.

(STAR, P2, #4) The RG treats autonomous systems the same as network-connected systems. This is a departure from the NRC's own NUREG/CR 6847 for isolated and non-networked systems and assets.

3. (TVA - p3) DG 5022, page 13 - "After nuclear critical systems and networks are identified, 10 CFR Part 73, Paragraph 73.54(b)(1) requires the licensee or applicant to identify the digital assets that:…"

   TVA claims that 73.54(b) does not require what the DG lists.

   (NEI, p19) - Ditto

   (NEI, p26) - Ditto

   (FPL - p3, 5) FPL claims that the Critical Systems should therefore be associated with systems that contain the already identified equipment.

**3.0 DG-5022; C. Regulatory Position - Tactical Rating: Med**

**3.3.1 Venue** - 3.1 Frame Work of a Cyber Security Program
3.2 Integration into the Physical Security Program
3.3 Cyber Security Roles and Responsibilities

| NRC Positions | Who | Touch Points | Priority |
|---|---|---|---|

NRC Response to Comment 7:

Although the restoration of the plant may be delayed due to Forensic actions, such actions are still required to mitigate future attacks. Also, in response to the "(NEI, p37)" comment: It may not be necessary to dedicate an FTE to cyber security. However, some full-time group must be qualified to handle cyber-related issues. The members of this group must be capable of handling cyber events until an expert can be called in.

NRC Response to Comment 12:

In response to the "(NEI, p34)" comment: The statement "…there is no conflict of mission between security and engineering/IT" is not necessarily true. In general, it is IT's mission to enable communication, and security's mission to limit communication.

**3.3.2 Best Practices:** N/A

### 3.3.3 Stakeholder Questions:

1. (NEI, p36) DG 5022, p16-19 - "3. Cyber Security Program Framework & Integration"

   NEI asks if these 4 pages can be deleted & FSAR should be called USFSAR.

2. (NEI, p31) DG 5022, p14 - 3.1 Framework of a Cyber Security Program"

   NEI questions why life cycle is not addressed in the rule?

3. (NEI, p31) DG 5022, p16 - "The NRC staff position is that cyber security program elements, resources, and personnel should be aligned with the licensee or applicant's commitment to Part 73. Within the physical security organization, cyber security program elements should be created, implemented, and maintained to provide protection of nuclear critical assets that will ensure appropriate cyber security responses to cyber attacks."

   NEI questions the NRC's position in this paragraph. It is not required by the regulation and is a "back fit".

4. (NEI, p30) DG 5022, p14 - "Licensees should use a common cyber security programmatic framework based upon the requirements in 10 CFR Part 73, Section 73.54, to ensure a consistent approach when implementing cyber security programs. The framework should identify the minimum set of components to be addressed by the licensee when developing a cyber security program. These components should include the:

   - cyber security framework and roles;

   NEI questions if the word framework is redundant with the first bullet item?

5. (NEI, p16) DG 5022, p17 Table C1 - "Preserve evidence collected during cyber security investigations to prevent loss of evidentiary value."

   NEI asks wouldn't the restoration of the plant be delayed because of the Forensic actions?

   (NEI, p37) NEI asks wouldn't it be prudent not to require a Cyber Security group as part of the security organization? There is not a full time position in this field and the person would spend their careers learning all the systems they were responsible for.

   (STARS, p2 #7) STARS questions the authority of the NRC to specify an organizational structure for a licensee. The present roles that handle configuration management, design and cyber security cans formally be coordinated with the physical security.

(STARS, p2 #7) STARS questions the authority of the NRC to specify an organizational structure for a licensee. The present roles that handle configuration management, design and cyber security can formally be coordinated with the physical security.

**3.3.4 Stakeholder Assumptions:**

1. (FPL - p4, 8) DG 5022, p13 - "To meet the high assurance criteria, the licensees must protect critical systems and networks so that design-basis functions and capabilities of these critical systems can be maintained both during and after a cyber attack. This means that these systems should be designed such that a failure due to a compromise or failed security measure, the system/function/or capabilities fail in a safe and secure mode. "

   FPL assumption is that after a device is compromised or a security measure is lost there is no known way hardware or software to ensure the compromise will not adversely effect the output of the device and the adverse effects to the system.

   (NEI, p25) "This statement expands the requirements of the rule."

   (NEI, p29) "This statement is not supported by the draft final rule."

   (NEI, p30) "Most systems are autonomous if a network system they would disconnect from the network or if its safety related then rely on the alternate train for the safety function. "This is an absurd expectation for legacy systems for which worst case scenarios have been considered where applicable."

2. (NEI, p28) DG 5022, p13 - "This means that these systems should be designed such that a failure due to a compromise or failed security measure, the system/function/or capabilities fail in a safe and secure mode."

   NEI - "This statement is not supported by the draft final rule."

3. (NEI, p29) DG 5022, p13 - "10 CFR Part 73, Paragraph 73.54(b)(2), requires that the licensee establish, implement, and maintain a cyber security program for the protection of all critical safety-related, security-related, and emergency preparedness assets, including the assets of interfacing systems and networks, which, if compromised, may adversely affect these assets. 10 CFR Part 73, Paragraph 73.54 (b)(3), requires that the licensee incorporate the cyber security program as a component of the physical protection program."

   NEI assumes that "this statement draws an inference from 73.54(b)(2)."

   (NEI, p31) "Clarify component."

   (NEI, p32) "Keep first two sentences and delete the remainder of the section including footnote #2 and figure C.2 The Cyber Security Program"

4. (NEI, p35) DG 5022, p15 - "A *cyber attack* is an additional attack vector described in early orders and actions and is included in the design basis threat final rule. As such, according to 10 CFR Part 73, Paragraph 73.1(a)(1)(v), a cyber attackF[1]F is commensurate of *attributes, assistance, and equipment* of NRC-recognized adversarial acts and capabilities. Further, Section 73.55 in 10 CFR Part 73, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage," defines objectives that support the protection against such adversarial acts and capabilities. In accordance with Section 73.55(a), "*General performance objective and requirements*," one such requirement is the establishment of a physical security organization.[2]F This organization encapsulates the functions and capabilities required to protect against radiological sabotage. These functions and capabilities stand as chartered responsibilities separate from any other nuclear or non-nuclear organization within the plant or facility.

   NEI believes the Regulatory Guide should be used by the QA department for an oversight of the program.

5. (TVA, p4) DG 5022, p15 - "An important key attribute of the security organization is the separation of the plant or facilities operational responsibilities. Security controls that are selected and deployed for the protection of nuclear critical assets are designed to provide the separation of conflicts that may arise between organizations that have different missions. For example, engineering and information technology organizations typically have economic and service-level commitments that include delivering computer-based solutions that are intended to reduce costs, gain efficiencies, and focus on providing increasing economic value or more efficient processes. In contrast, the security organization is tasked with meeting regulatory expectations and providing appropriate levels of protection for plant/facility assets and public safety even if this causes substantial programmatic impacts for other licensee organizations. The mission of the security organization therefore differs from, and may at times be in conflict with, the missions of a licensee's engineering or information technology organization."

   10 CFR Part 73, Paragraph 73.54(b)(3), requires the licensee to "*incorporate the cyber security program as a component of the physical protection program."*

   TVA assumes there is no conflict of mission between security and engineering/IT. Supporting statement is: "Implementation of security measures at the site is highly dependent on both the engineering and IT organization." Thus the NRC's has poorly characterized the roles of engineering and IT organization.

---

1 10 CFR 73.1(a)(1)(v) provides a *cyber attack* as one of several threat vectors related to *attributes, assistance, and equipment*.

2 *(b) Physical Security Organization. (1) The licensee shall establish a security organization, including guards, to protect his facility against radiological sabotage.*

TVA second assumption is that the expertise is located in the engineering and/or IT organization and that security has no background in this type of technical work. The individual utility should determine where the cyber security function is to be managed

(NEI, p16, p33) NEI states there is no plan to have Physical security drive cyber security and such a change would have to be well understood and procedural interface.

(NEI, p34) NEI assumes there is no conflict of mission between security and engineering/IT.

**3.0 DG-5022; C. Regulatory Position - Tactical Rating: Med**

**3.4.1 Venue -** 4. Defensive Strategies and Security Controls
4.1 A Defensive Model in Support of Defensive-in-Depth Protective Strategies

| NRC Positions | Who | Touch Points | Priority |
|---|---|---|---|

NRC Response to Comment 6:

See response to Comment #7, Section 3.1 (i.e. "state of the art" comment).

NRC Response to Comment 11:

Both the section quote and stakeholder comment are confusing. In general, "logs" serve two functions: tracking potential attacks (e.g. honeypots, failed login attempts, etc) and past attack forensics (e.g. packet sniffer logs, to see what information was sent during an attack). In either case, the compilation of logs should be automated, and periodically reviewed (automatic and/or manual reviews are acceptable, depending on the particular log and purpose of the review). However, "logs" are never used for on-the-fly protection (as may be inferred from stakeholder comments).

NRC Response to Comment 17:

A non-reroutable network protocol may still be considered a cyber threat, due to potential insider attacks and/or malicious injected traffic.

**3.4.2 Best Practices:** N/A

**3.4.3 Stakeholder Questions:**

1. (NEI, p38) DG 5022, p18 Figure C3. & Paragraph above and below.

   NEI asks if this section be deleted? Replace with the new improved NEI version.

   (NEI, p47) NEI repeats request to delete pyramid. Claims it has no value.

2. (NEI, p39) DG 5022, p18 - "10 CFR Part 73, Paragraph 73.54 (c)(1), calls for implementation of "*security controls"* to protect nuclear critical assets from cyber attack. This requires that the licensees adopt effective security controls to block unauthorized or inappropriate access to nuclear critical assets. Effective security controls must block viruses, worms, malware, denial-of-service attacks, and other forms of cyber attack from reaching nuclear critical assets. Security controls must also protect these assets from inappropriate or unauthorized use of, or modification to, hardware or software; including physical damage to digital assets and communication pathways. The NRC staff position is that simply detecting attacks *after* they have reached these assets and then taking steps to mitigate potential damage does not meet the requirement of Section 73.54(c)(1).

   NEI asks: Can this section be deleted? Replace with the new improved NEI version.

   (NEI, p43) NEI asks to use the new improved NEI version of DG. The statement uses a negative connotation. This should be used as a KPI by the inspectors.

   (NEI, p47) NEI asks to delete this section, because "This would make any future attack methodology, if successful, a violation."

3. (NEI, p40) DG 5022, p19 - " Defense in depth is achieved also by not relying solely on multiple security boundaries but by instituting a robust program that includes the following components:

   - protection;
   - prevention;
   - detection;
   - mitigation; and
   - recovery.

   For example, if there is a failure in prevention (e.g., a violation of policy) or protection and detection mechanisms are bypassed (e.g., by a new virus that is not yet identified as a cyber attack), mechanisms are still in place to detect an unauthorized alteration in an impacted nuclear critical asset, mitigate the impacts of this alteration, and recover normal operations of the impacted critical system before any adverse impact can occur."

   NEI asks: Can this section be deleted? It goes beyond the scope of the rule. Replace with the new improved NEI version.

4. (NEI, p41) DG 5022, p19 - "State-of-the-art"

   NEI requests this terminology be removed because it is inappropriate for the use in rule space in ever changing environment. Licensee can not keep up with on going technology changes.

(NEI, p44) NEI asks to go back to the NEI 04-04 and NUREG approach because the term "State-of-the-art" does not add value or increase protection. It complicates the systems configurations and has a potential to have a high percentage of safety issues from a plant reliability and performance stand point. This is because a large part of the installed digital systems are not "State-of-the-art" and would require different mitigation strategies based on the assessments.

5. (NEI, p42) DG 5022, p19 - "a. Be cognizant of evolving cyber security threats and vulnerabilities. b. Be cognizant of advancements in cyber security protective strategies and security controls. c. Conduct appropriate analyses of the effects each advancement could have on the security and operation of the nuclear critical assets, systems, and networks at their facility. d. Ensure that appropriate actions are taken to minimize the time it takes to deploy new and more effective protective strategies and security controls to safeguard nuclear critical assets, systems, and networks from potential cyber attacks."

   NEI asks: Can this section be deleted? Replace with the new improved NEI version.

6. (NEI, p43) DG 5022, p19 - "…when a cyber attack has reached a nuclear critical asset…"

   NEI asks if this can be reworded to say "..when a cyber attack has reached a nuclear critical asset where technically feasible:…"?

7. (NEI, p43) DG 5022, p19 - "Respond" in this application refers to protection, prevention, mitigation, and recovery activities.

   NEI claims this definition includes items beyond the requirements of the rule. Replace with new improved NEI version.

8. (NEI, p44) DG 5022, p19 - " 10 CFR Part 73, Paragraph 73.54(c)(3) requires the licensees to '*prevent adverse impacts from a cyber attack.*' If a cyber attack successfully propagates through a security mechanism (e.g., a zero-day attack for which a virus signature is not yet available) and reaches a nuclear critical asset, the licensees must have security controls in place within the asset to prevent adverse impacts on design basis functions of that nuclear critical asset."

   NEI asks for clarification; "current D3 strategy is to detect and isolate in advance."

9. (FPL - p5, 9) DG 5022, p20 - "It is the NRC staff position that security logs and related information will be reviewed with sufficient frequency to identify cyber attacks or their precursor activity in time to mount an effective security response."

   FPL states that past experience shows that manual logs do not provide effective means for identification of events or intrusions, and that only automated log review

systems provide a timely response. (So what was the intent of the DG 5022 statement?)

(NEI, p45) NEI asks can the NRC delete this section above and the following: "However, the NRC staff acknowledges that adequate time is needed for the licensee's staff to review information from intrusion detection systems to identify a potential cyber attack and dismiss *false positive* readings. Automated security controls that provide a protection function should act in a time frame that prevents the attack from penetrating or bypassing security mechanisms. Security measures put in place to delay attacks should act fast enough and be of sufficient capability to delay the attack until other security controls can be brought into play. If automated protection and delaying mechanisms fail, it is the NRC staff position that licensees will ensure that actions are taken to mitigate adverse effects before the potential consequences are realized."

(NEI, p47) NEI asks to delete because the ID of a cyber attack will never be the result of a security log review and IT will respond not Security.

10. (NEI, p46) DG 5022, p20 - " It is noted that if a virus, worm, malware, or other form of cyber attack reaches a critical system, the requirement specified in 10 CFR Part 73, Paragraph 73.54(c)(1), has not been fully met. However, the defense-in-depth specification requires that the licensee have security controls in place to delay, prevent, mitigate, and recover from adverse impact if there is a failure of the deployed protection mechanisms. "

    NEI asks to delete this wording because it is not consistent with the Commission's wording in the rule.

11. (NEI, p46) DG 5022, p20 - "Automated security controls that provide a protection function should act in a time frame that prevents the attack from penetrating or bypassing security mechanisms."

    NEI asks that this sentence be clarified.

    (STARS , p2 #6) Does the RG consider the failure modes and effects introduced by an overlay of independent security devices/networks in an intrusive manner on a control system?

12. (NEI, p50) DG 5022, p20 - "The implementation of multiple security levels provides a defense-in-depth protective mechanism that is analogous to what is currently implemented by the licensees for physical security."

    NEI asks that "a defense-in-depth" should read "engineering defense-in-depth."

13. (NEI, p50) DG 5022, p20 - "(i.e., no communication pathways between the nuclear critical system and any other digital asset)"

NEI doesn't believe the example accounts for the difference between digital control and data acquisition, and one-way verses two-way communications. What about the Plant Process Computer?

14. (NEI, p50) DG 5022, p21 - "4.1.1 Application of the Defensive Model"

    NEI asks this entire section be moved to NUREG.

    (NEI, p51) NEI claims the Figure C-4 is an artificial was to rationalize and embed C-S into physical security. NEI asks to use model from NEI 04-04.

    (NEI, p51) In figure C-4 please delete the physical boundaries.

    (NEI, p51) In figure C-4 some plants may be designed as such but not all control systems are located in the vital area. Please use alternative DG 5022.

    (NEI, p51) In figure C-4 please remove level 3 does not add value.

15. (NEI, p51) DG 5022, p21 - "C. 4.1.1.b.ii Limit or eliminate bidirectional data flow between Levels 4 and 3 (Figure C.5)."

    NEI asks: Is a non re-routable network protocol considered a cyber threat? ERGO: RS 232, RS 422. Most operation plant data links fall in this category for safety systems interface to the plant computer.

16. (FPL - p5, 10) DG 5022, p22 - "d. Depict the location of each nuclear critical asset, connected digital assets, and communication/data transfer within the defensive model. This should include the assets that are part of all critical systems and networks, including those systems and networks that are autonomous."

    FPL asks whether describing in words would be more representative verses a visual map with thousands of digital instruments.

17. (NEI, p52) DG 5022, p22 - "4.1.2 Exceptions to the Defensive Model"

    NEI request that this section be moved to the NUREG.

**3.4.4 Stakeholder Assumptions:**

1. (NEI, p50) DG 5022, p20 - "In this way, the defensive model can identify where communication and data transfer pathways cross security boundaries and pinpoint where logical or physical security measures are needed to protect the digital assets that should be maintained at a higher security level."

NEI assumes that the defense model does not identify anything and the CDA/COP assessment does. Delete the sentence.

2. (TVA - p5) DG 5022, p21 - Figure C.4 - Simplified Cyber Security Defensive Model shows level4 to be in the vital area.

   Not addressed in 73.54

   TVA made comments that figure C.4 should be noted as an example of a defensive model. It should not be portrayed as the required model. TVA believes that a control system may be located outside of a vital area, ERGO: a condensate demineralizer system installed in the Turbine Building.

3. (NEI, p50) DG 5022, p21 - "In particular, digital isolation is preferred whenever feasible for safety-related and important-to-safety systems."

   NEI would like other reference other NRC guidance in this area such as ISG.

   (NEI, p50) NEI assumes that the term "digital isolation" is consistent with IEEE 7.4.3-2 definition.

**3.0 DG-5022; C. Regulatory Position - Tactical Rating: Med**

**3.5.1 Venue** - 4.2 Security Control

| NRC Positions | Who | Touch Points | Priority |
|---|---|---|---|

NRC Response to Comment 9:

In response to the "…nuclear critical systems using transmitters with EPROMS with no connectivity or control function should not require a cyber security plan" comment: even in this case, a cyber plan should exist, claiming that the asset is either non-exploitable, or the asset's cyber vulnerability is covered by the physical security plan.

**3.5.2 Best Practices:** N/A

**3.5.3 Stakeholder Questions:**

1. (FPL - p6, 11) DG 5022, p23 - "Security controls, as discussed in detail in NIST Special Publications 800-53, *Recommended Security controls for Federal Information Systems* (Ref.14) and 800-82, "*Guide to Industrial Control Systems (ICS) Security*," (Ref. 15) are divided into three classes: management, operational, and technical controls. "

   FPL asks if the NRC endorses the NIST standard in whole or parts?

(NEI, p53) NEI asks to remove this paragraph because NIST 800-53 refers to information systems while 800-82 refers to control systems and neither is applicable here.

2. (NEI, p52) DG 5022, p22 - " 4.2 Security Controls "

   NEI requests that this section be moved in to the NUREG.

   (NEI, p54) NEI asks to have the NIST 800 standards removed from C.4.2 Security Controls.

3. (FPL - p6, 12) DG 5022, p24 - "Licensees should review NIST SP 800-82, (Ref. 15) and NIST SP 800-53, (Ref. 15) when adopting security controls. NIST SP 800-82 provides a detailed discussion of security controls for control systems. NIST SP 800-53 provides guidelines for selecting and specifying security controls. Although the focus of NIST SP 800-53 is on information systems, Appendix I of SP-800-53 focuses on control system security. The NRC staff recommends a thorough review for the applicability of NIST SP 800-53, NIST SP 800-82, or other applicable NIST guidance on security controls for industrial control systems when licensees adopt their own comprehensive set of security controls as part of their cyber security program. NIST SP 800-53 presents three levels of baseline security controls that correspond to low-impact, moderate-impact, and high-impact consequences. The use of the high-impact level category is recommended for developing appropriate security controls for all critical systems and networks. Any departure from the high-impact level should be justified in detail as part of the licensee's cyber security program for NRC staff review."

   FPL requests why this paragraph does not recognize the security controls in NEI 04-04?

   (NEI, p55) NEI wants consensus for these current classification levels.

4. (NEI, p55) DG 5022, p25 - "7. ***Monitor*** **t**he selected security controls and update them, as warranted, to address changes to the critical systems and networks. Changes can occur during any phase of the system's life cycle. Results of the security assessment should be used to determine if the selected security controls need to be enhanced or expanded beyond their baseline (NIST SP 800-82) to meet the high assurance requirement (10 CFR Part 73, Paragraph 73.54(a))."

   NEI states that high assurance is subjective and can we obtain a clear definition?

**3.5.4 Stakeholder Assumptions:**

1. (TVA - p6) DG 5022, p24, "NIST SP 800-53 presents three levels of baseline security controls that correspond to low-impact, moderate-impact, and high-impact

consequences. The use of the high-impact level category is recommended for developing appropriate security controls for all critical systems and networks. Any departure from the high-impact level should be justified in detail as part of the licensee's cyber security program for NRC staff review."

Not addressed in 73.54

TVA's assumption is that the NRC is incorrect by virtue of NIST SP 800-53 to automatically assign all digital systems in a high impact category.

(NEI, p54) NEI believes that a control system does not meet the high impact level category as it is defined in FIPS 199. This section should be removed.

2. (NEI, p55) DG 5022, p24 - "***Supplement*** the initial set of tailored security controls after an in-depth cyber security assessment of risk is conducted. This should include a consideration of the threat environment and the potential use of *attack vectors scenarios* (see Section C.6). Security controls must reflect NRC security requirements and guidance."

   NEI current NISTL Guidance does not address this and thus this section should be removed.

3. (TVA - p7) DG 5022, p25, "***Document*** the agreed-upon set of security controls in each a security plan developed for each nuclear critical system and network, including the rationale for any refinements or adjustments to the initial set of security controls or departures from NRC regulatory guidance."

   Not addressed in 73.54

   TVA's claims the assumption that not all nuclear critical systems have digital assets that perform a control function. ERGO: nuclear critical systems using transmitters with EPROMS with no connectivity or control function should not require a cyber security plan.

   (NEI, p55) NEI claims this would add another 50 to 70 systems with 163 security controls by NIST 800-53. Remove this section because it would require many FTE s to cover.

**3.0 DG-5022; C. Regulatory Position - Tactical Rating: Med**

**3.6.1 Venue** - 4.3 Policies and Procedures

| NRC Positions | Who | Touch Points | Priority |
|---|---|---|---|

NRC Response: N/A

**3.6.2 Best Practices:** N/A

**3.6.3 Stakeholder Questions:**

1. (NEI, p57) DG 5022, p25 - " 4.3 Policies and Procedures"

   NEI requests this section be removed because NEI 04-04 does not mandate Cyber Security as an independent organization under security.

   NEI also requests 3rd paragraph be removed under 4.3 Policies and Procedures.

2. (TVA - p7) DG 5022, p25, "Policies (and the procedures that act to enforce those policies) should be based on, where applicable, Homeland Security Advisory System Threat Levels, thereby allowing for the deployment of increased security postures in response to declared increases in threat levels."

   Not addressed in 73.54

   TVA does not understand the statement.

   (NEI, p56) NEI requests this section be removed, and added to NUREG.

3. (TVA - p7) DG 5022, p26, " Topical areas to be addressed by site-specific cyber security policies include, but are not limited to: Responding to Department of Homeland Security Threat Level Advisories."

   Not addressed in 73.54

   TVA does not understand the statement.

   (NEI, p57) NEI requests that this section be removed and added to a NUREG.

**3.6.4 Stakeholder Assumptions:**

1. (TVA - p7) DG 5022, p25 & 26, Entire Section.

*"(f) The licensee shall develop and maintain written policies and implementing procedures to implement the cyber security plan and ensure that the cyber security requirements of this section are met.*

*(f)(1) Policies, implementing procedures, site-specific analysis, and other supporting technical information used by the licensee need not be submitted for Commission review and approval as part of the cyber security plan; but are subject to inspection by NRC staff on a periodic basis."*

TVA's assumes that plant safety significant systems are considered instrument and control systems and should comply with the IEEE standard and not the NIST standard.

**3.0 DG-5022; C. Regulatory Position - Tactical Rating: Med**

**3.7.1 Venue -** 4.4.2 DMZ or Screened sub net servers
4.4.4 Intrusion Detection and penetration systems
4.4.5 Honeypots and Honeynets
4.4.6 Packet Sniffers
4.5 Security Boundary

| NRC Positions | Who | Touch Points | Priority |
|---|---|---|---|

NRC Response to Comment 6:

Instead of removing these sections, these sections should be expanded to provide high-level guidance in the use of these security mechanisms.

NRC Response to Comment 7:

How does this assumption relate to the associated section? The original text seems to discuss the DMZ between systems/networks. The NEI's comment seems to be addressing application servers, which is unrelated to this.

**3.7.2 Best Practices:** N/A

**3.7.3 Stakeholder Questions:**

1. (NEI, p58) DG 5022, p28 - "C. 4.4.4 Intrusion Detection and Prevention systems"

   NEI requests this section be deleted because it adds no value.

2. (NEI, p58) DG 5022, p28 - " C. 4.4.5 Honeypots and Honeynets"

   NEI requests this section be deleted and add to NUREG.

3. (NEI, p58) DG 5022, p28 - " C 4.4.6 Packet Sniffers"

   NEI requests this section be deleted and add to NUREG.

4. (NEI, p58) DG 5022, p29 - "C 4.5 Security Boundaries"

   NEI requests this section be deleted and add to NUREG.

**3.7.4 Stakeholder Assumptions:**

1. (NEI, p58) DG 5022, p25 - "Servers containing the data from a critical control system that needs to be accessed by another control system, plant network, or other network connection, are put on a DMZ."

   NEI believes there is no reason to segregate the new builds that have one network with multiple servers (applications). Access to these is already in place for engineering and maintenance.

**3.0 DG-5022; C. Regulatory Position - Tactical Rating: Med**

**3.8.1 Venue** - 4.6 Security Monitoring Network

| NRC Positions | Who | Touch Points | Priority |
|---|---|---|---|

NRC Response to Comment 6:

This section should more clearly state that the purpose of physically and logically securing the CDA is to prevent internal unauthorized access (i.e. decrease likelihood of insider attacks).

NRC Response to Comment 7:

See response to Comment #7, Section 3.1 (i.e. "state of the art" comment).

NRC Response to Comment 8:

See response to Comment #7, Section 3.1 (i.e. "state of the art" comment).

NRC Response to Comment 9:

The original statement does not preclude IT, nor does it dictate who's "first". Also, the term "security personnel" is misleading (maybe "cyber-security personnel"?). Due to NEI's apparent confusion regarding this statement, it may be useful to clarify this statement.

NRC Response to Comment 12:

It is critical for patches and virus signatures to be up-to-date, and the method described for accomplishing this is the least expensive method. It may be useful to recommend an update procedure and/or update frequency to alleviate concerns over "cost".

**3.8.2 Best Practices:** N/A

### 3.8.3 Stakeholder Questions:

1. (FPL, p7, 13) DG 5022, p30 to 33 - " 4.6 Security Monitoring Network"

   FPL asks can the word "should" be changed to "may" for section 4.6 and subsections 4.6.1 thru 5. "The determination of which components are to be included in the security monitoring system is dictated by the defensive strategy and site specific architecture."

2. (NEI, p58, p60) DG 5022, p30 to 33 - " 4.6 Security Monitoring Network

   NEI asks that the entire section be moved to the NUREG.

3. (NEI, p31) DG 5022, p31 - " C4.6.1 Licensees should use NIDS or NIPS to monitor and analyze network traffic along key communication pathways that traverse each security boundary, regardless of whether firewall or data-diode technologies are used."

   NEI asks that the section be moved to NUREG.

4. (NEI, p62) Dg 5022, p31 - " a. Be physically and logically secured (e.g., hardened) to prevent unauthorized access or manipulation."

   NEI says the CDAs are already within a substantially hardened envelope (the plant) What additional standard needs to be met?

5. (TVA - p10) DG 5022, p32 - "Network devices requiring virus signature updates or patches should be configured to "pull" the signatures or patches from the designated server management server. Patch scanning tools that scan systems for missing security patches or updates should be installed on a node existing in the security monitoring network."

   Paragraph 73.54(c) in 10 CFR Part 73 describes required elements in the cyber security program. It includes requirements to apply for defense-in-depth protective strategies, implement security controls to protect assets, prevent adverse impacts, and ensure the function of nuclear critical assets is maintained. It states:

   > *"(c) The cyber security program must be designed to:*
   > *(c)(1) implement security controls to protect the assets identified by paragraph (b)(1) of this section from cyber attacks,*
   > *(c)(2) apply state-of-the-art defense-in-depth protective strategies to ensure the capability to detect and respond to cyber attacks in a timely manner,*
   > *(c)(3) prevent adverse impacts from a cyber attack, and;*

*(c)(4) ensure that the functions or tasks required to be performed by the assets identified by paragraph (b) (1) of this section are maintained and carried out as intended."*

TVA assumption is that the guidance is over prescriptive and costly to maintain.

(NEI, p16) NEI would like to replace "state-of-the-art" with "commensurate with the criticality of the digital asset, maintain defense-in-depth."

**3.8.4 Stakeholder Assumptions:**

1. (TVA - p9) DG 5022, P31, "Security devices (e.g., firewalls, network intrusion systems) should have dedicated interfaces on the security monitoring network. When establishing a security-monitoring network, the licensee should ensure that security interfaces with each affected security boundary or critical system are both physically and logically protected from compromise. If this is not accomplished, it may be possible for a threat agent to circumvent the established security architecture through a compromise of the security-monitoring network itself. In general, in-band security monitoring and software updates should not be permitted. If in-band techniques are used to notify the site or corporate security personnel of cyber security events, the interface between the security monitoring network and other networks should be at least as secure as the interface that the security network monitors. The security monitoring network is considered to be a plant-centric network. Remote access or remote control to the security-monitoring network should not exist.

   Paragraph 73.54(c) in 10 CFR Part 73 describes required elements in the cyber security program. It includes requirements to apply for defense-in-depth protective strategies, implement security controls to protect assets, prevent adverse impacts, and ensure the function of nuclear critical assets is maintained. It states:

   *"(c) The cyber security program must be designed to:*
   *(c)(1) implement security controls to protect the assets identified by paragraph (b)(1) of this section from cyber attacks,*
   *(c)(2) apply state-of-the-art defense-in-depth protective strategies to ensure the capability to detect and respond to cyber attacks in a timely manner,*
   *(c)(3) prevent adverse impacts from a cyber attack, and;*
   *(c)(4) ensure that the functions or tasks required to be performed by the assets identified by paragraph (b) (1) of this section are maintained and carried out as intended."*

   TVA assumption is that the guidance is over prescriptive and costly to maintain.

   (NEI, p59 & p60) NEI believes that this section be moved to the NUREG.

2. (NEI, p60) DG 5022, p31 - "a. Detect and alert security personnel to malicious or suspicious activity occurring at established defensive level boundaries and within security levels."

   NEI believes that IT should be alerted first not Security.

3. (TVA, p10) DG 5022, p33 - "Anti-virus/anti-malware update servers used to update client signature definitions should be installed on a dedicated DMZ or screened subnet server."

   TVA assumption is that the guidance is over prescriptive and costly to maintain.

4. (TVA, p10) DG 5022, p33, "Patch management and virus update servers deployed on the DMZ or screened subnets located on the security boundaries between security levels 4 and 3 and security levels 3 and 2 should…"

   TVA assumption is that the guidance is over prescriptive and costly to maintain.

5. (TVA, p11) DG 5022, p33, "Install software patches and virus signature updates to the update server using a manual means (e.g., sneaker-net) rather than allowing the update server to automatically pull updates from a source located in a lower security level."

   TVA assumption is that the guidance is over prescriptive and costly to maintain.

## 3.0 DG-5022 C. Regulatory Position — Tactical Rating: Med

**3.9.1 Venue -** 5.1 Physical Security
5.2 Hardened Systems

| NRC Positions | Who | Touch Points | Priority |
|---|---|---|---|

NRC Response: N/A

**3.9.2 Best Practices:** N/A

**3.9.3 Stakeholder Questions:**

1. (NEI, p62) DG 5022, p34 - "5. Security Guidance for Key Topical Areas"

   NEI asks to have this section moved to the NUREG.

2. (NEI, p62) DG 5022, p34 - " 5.2 Hardened Systems"

   NEI asks that this section is moved to the NUREG.

### 3.9.4 Stakeholder Assumptions:

1. (TVA - p12) DG 5022, p34 -"The NRC staff recognizes that substantial requirements for physical access controls and mitigating measures are specified within 10 CFR Part 73, Section 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage," and 10 CFR Part 73, Section 73.56, "Personnel Access Authorization Requirements for Nuclear Power Plants." However, a number of physical security issues are not addressed by these rules, including:

   inappropriate activities conducted by authorized or trusted individuals;
   exposure to physical compromise during the early phases of a critical system life cycle when the system or its components are under the physical control of other organizations (e.g., vendors, suppliers, delivery services); and access to communication ports on digital assets (e.g., connections for USB devices, serial devices, keyboards, monitors, networks). Additionally, some assets also may contain removable media ports that support technologies such as compact flash, SDRAM, floppies, DVD, or compact disks. Many of these ports or input devices can be used bypass logical access controls.

   To reduce the possibility of a physical compromise to critical systems, the licensees should develop supplemental security controls to specifically address the physical security for digital assets during their life cycle. These controls include control system components, network devices, and security devices (e.g., switches, routers, servers, workstations, controllers). The physical security issues to be addressed include:

   assessing the potential security threats and risks that exist at all of the locations of an asset throughout its life cycle;
   limiting access throughout an asset's life cycle to only those authorized individuals. This includes access controls during design, manufacture, shipping/transport, and operation at the licensee's facility;
   physical security mechanisms (e.g., physical port locks, locked cabinets) to limit access to assets; and
   detection of unauthorized access or activities."

   10 CFR Part 73, Paragraph 73.54(b)(3), requires the licensee to "*incorporate the cyber security program as a component of the physical protection program."*

   TVA assumption is that the threat is covered under existing regulations and there is no need for additional requirements.

2. (TVA - p13) DG 5022, p34 - "When hardening nuclear critical assets, the licensee should develop security controls to address the:

   removal of unnecessary default accounts or test accounts,
   removal of unnecessary file shares,

removal of unnecessary operating system services and ports,
installation of access controls on file systems, file shares, registries (if any), and executables (binaries) where possible to limit inappropriate access or misuse of the system,
application of role-based access controls, where appropriate, and their reduction to the lowest level possible to reasonably perform a user's job function,
logging and monitoring of logical access to nuclear critical assets where possible, and ensuring that remote access or remote control to a nuclear critical asset does not exist beyond its defensive level boundary."

Not addressed in 73.54

TVA states that vendors do not tailor their power line to one venue for hardening for nuclear critical assets. The assumption is it would be very hard to motivate vendors towards supporting this requirement.

**3.0 DG-5022 C. Regulatory Position** **Tactical Rating: Med**

**3.10.1 Venue -** 5.3 Identification, Authentication and Access Control
5.4 Positive Control of Portable Computing Devices
5.5 Remote Connectivity
5.6 Modems
5.7 Wireless Networking
5.8 Backups and Disaster Recovery

| NRC Positions | Who | Touch Points | Priority |
|---|---|---|---|

NRC Response to Comment 12:

A physically isolated asset may still be susceptible to EMI, indirect connectivity and/or insider attacks. As such, these systems must still be monitored. This section should be revised to explicitly state this.

**3.10.2 Best Practices:** N/A

**3.10.3 Stakeholder Questions:**

1. (NEI, p62) DG 5022, p35 - " 5.3 Identification, Authentication and Assess Control"

   NEI asks that this section is moved to the NUREG.

2. (NEI, p62) Dg 5022, p37 - "5.4 Positive Control of Portable Computing Devices"

   NEI asks that this section is moved to the NUREG.

3. (NEI, p63) DG 5022, p38 - " 5.5 Remote Connectivity"

   NEI asks that this section is moved to the NUREG.

4. (NEI, p63) DG 5022, p38 - "Remote connectivity refers to the ability to access or control network resources from a distant or remote location. Such ability can be achieved through a variety of connectivity methods, including the use of modems, wireless communications, and the Internet."

   NEI asks to revise the above statement to what the ICM discussed.

5. (FPL, p7, 14) DG 5022, p39 - "For emergency preparedness systems and networks, remote connectivity to an offsite location is only permitted if the cyber security program and security controls for the remote system are equivalent to that of the connected nuclear critical asset."

   FPL states that Physical security controls for the EOFs are addressed under NUREG-0696, section 4.1. Can the phrase "and security controls" be deleted?

6. (NEI, p63) DG 5022, p40 - "5.6 Modems"

   NEI asks that this section is moved to the NUREG.

7. (NEI, p63) DG 5022, p41 - " 5.7 Wireless Networking"

   NEI asks that this section is moved to the NUREG.

8. (NEI, p64) DG 5022, p41 to 44 - " 5.7 Wireless Networking"

   NEI asks: why are there Wireless requirements for level 3 and 4 for plant systems. They are not secure and presently not used there.

9. (NEI, p64) DG 5022, p44 - " 5.8 Backups and Disaster Recovery"

   NEI asks that this section is moved to the NUREG.

**3.10.4 Stakeholder Assumptions:**

1. (NEI, p63) DG 5022, p35 - "When hardening nuclear critical assets, the licensee should develop security controls to address the:"

   NEI assumes that if the assessment shows there is no need for a hardened asset then the user does not have to follow the recommended guidance by NIST. Physically isolated assets are protected by cyber attacks and thus no need to monitor. The RG does not allow for risk consequence based implementation.

2. (FPL, p7, 15) DG 5022, p41 - "At this time, wireless networking is considered by the NRC staff to be an emerging communications technology with limited historical operating experience with respect to nuclear facilities. Although standards do exist that define the various technologies used within wireless networks, the rate at which these standards have experienced change and the rapid evolution of the technology are of particular concern. Many of the amendments to these standards have occurred as a direct result of discovered security vulnerabilities."

   FPL believes that only WPA2 or equivalent is the recognized to provide adequate security for wireless communication. The other technologies mentioned do not provide adequate security for critical digital assets and suggest deleting the discussion of other wireless technologies.

**3.0 DG-5022 C. Regulatory Position** **Tactical Rating: Med**

**3.11.1 Venue** - 5.9 Media Sanitization
5.10 Encryption
5.11.6 Further Definition of Roles and Responsibilities
5.11.8 Provide Other Operational Support

| NRC Positions | Who | Touch Points | Priority |
|---|---|---|---|

NRC Response to Comment 8:

See response to Comment #7, Section 3.1 (i.e. "state of the art" comment).

NRC Response to Comment 9:

See response to Comment #7, Section 3.1 (i.e. "state of the art" comment).

**3.11.2 Best Practices:** N/A

**3.11.3 Stakeholder Questions:**

1. (FPL - p8, 16) DG 5022, p46 - "*Media* identifies materials that can *hold* data in any form or allow data to *pass* through them. Examples of materials that can hold data include paper, magnetic disks, optical disks, random access memory (RAM), read-only memory (ROM), and USB flash drives. Copper conductors, fiber optics, and air are all examples of material that are capable of allowing data to pass through them. "

   FPL requests that this sentence be deleted: "Copper conductors, fiber optics, and air are all examples of material that are capable of allowing data to pass through them."

2. (NEI, p64) DG 5022, p46 -"5.9 Media Sanitization"

   NEI asks that this section is moved to the NUREG.

3. (NEI, p64) DG 5022, p47 - “5.10 Encryption”

   NEI asks that this section is moved to the NUREG.

4. (FPL, p8,17) DG 5022, p48 - “System log management is one component of an effective cyber security program. A *log* is a record of the events occurring within a system or network. Log entries contain information related to a specific event that has occurred. The secure storage, regular review, and prompt analysis of system logs allows for the timely identification and resolution of security incidents, policy violations, fraudulent activity, and operational problems.”

   (Same as 3.4.3 Question) FPL suggests that only automated review can satisfy the timely requirements for response to an attack.

5. (NEI, p65& 66) DG 5022, p48 to 52 -“5.11 System Log Management (all sections)”

   NEI asks that all sections are moved to the NUREG. There is a lack of understanding on how to apply this technology and there is no value added.

**3.11.4 Stakeholder Assumptions:**

1. (TVA, p15) DG 5022, p51 - ”The roles of teams and individuals often involved in log management include the following:

   critical system and network administrators - responsible for configuring logging on individual systems and network devices, analyzing those logs, reporting on the results of log management activities, and performing regular maintenance of the logs and logging software;
   cyber security network administrators - responsible for managing and monitoring the log management infrastructures, configuring logging on security devices (e.g., firewalls, network-based intrusion detection systems, antivirus servers), reporting on the results of log management activities, and assisting others with configuring logging and performing log analysis;
   cyber security incident response teams - access and use log data during potential cyber security incidents;
   cyber security application developers - may need to design or customize applications so that they perform logging in accordance with established logging policies and procedures;
   information security officers - may oversee the log management infrastructures;
   chief information officers (CIO) - oversee the IT resources that generate, transmit, and store logs; and
   auditors - may use log data when performing audits.

*(c)(2) apply state-of-the-art defense-in-depth protective strategies to ensure the capability to detect and respond to cyber attacks in a timely manner,*

TVA assumption is that the guidance is over prescriptive and costly to maintain.

2. (TVA, p16) DG 5022, p53 - "In addition to the operational processes described earlier in this section, infrastructure and system-level administrators need to provide additional types of support for logging operations. They should perform the following actions regularly:

   a. Monitor the logging status of all log sources to ensure that each source is enabled, configured properly, and functioning as expected.
   b. Monitor log rotation and archival processes.
   c. Check for upgrades and patches.
   d. Ensure that the clock for each system is synchronized.
   e. Reconfigure logging as needed based on policy changes, audit findings, technology changes, and new security needs.
   f. Document anomalies detected in log settings, configurations, and processes."

   *(c)(2) apply state-of-the-art defense-in-depth protective strategies to ensure the capability to detect and respond to cyber attacks in a timely manner,*

   TVA assumption is that the guidance is over prescriptive and costly to maintain.

**3.0 DG-5022 C. Regulatory Position** **Tactical Rating: Med**

**3.12.1 Venue** - 6. Cyber Security Assessment and Risk Management

| NRC Positions | Who | Touch Points | Priority |
|---|---|---|---|

NRC Comments: N/A

**3.12.2 Best Practices:** N/A

**3.12.3 Stakeholder Questions:**

1. (NEI, p67) DG 5022, p52 - "6. Cyber Security Assessment and Risk Management"

   NEI - Can the risk assessment process defined in NEI 04-04 continue to be used?

   TVA - Ditto

2. (FPL, p9, 19) DG 5022, p54 - "Conduct tabletop review and validation. Perform a detailed examination of each nuclear critical asset. This should include:"

FPL suggests that a formal review process would provide a better access to current documentation and verify equipment setup than in a closed door session. Can the NRC change the word "should" to "may"?

3. (FPL, p9, 20) DG 5022, p55 - "Following selection of the security controls, identify the residual risk that remains for each asset. Determine whether the remaining risk meets the high assurance requirement of 10 CFR Part 73, Section 73.54, and is acceptable without applying additional control measures, or whether additional defense-in-depth security controls are needed."

   FPL - Can the risk assessment processes defined in NEI 04-04 continue to be used?

   (NEI, p68) NEI asks that all sections are moved to the NUREG.

**3.12.4 Stakeholder Assumptions:**

1. (FPL, p8, 18) DG 5022, p54 - "Assess threat information. The licensee should identify and evaluate postulated, credible cyber attacks (and combined physical and cyber attacks) that could impact any nuclear critical asset. The postulated cyber attacks must include outsider and insider attacks, malicious and inadvertent activities, and attacks that are targeted against nuclear critical assets and those that not-targeted against nuclear critical assets. The characterization of the maximum capabilities of threat agents should be available from the design basis threat and adversary characterization documents. The licensee should identify and assess potential attack vectors scenarios that could be used during any phase of a nuclear critical asset's life cycle. The use of attack trees (Schneier 1999) or a comparable method of assessment is recommended to assess and document the attack vector scenarios."

   FPL believes this is inconsistent with the Design Basis Threat presented in the RG 5.69. FPL also suggests removing the reference to a web page document, change "combine physical and cyber attacks" to "combined physical facility attack and critical digital asset cyber attack" and change "must include outsider and insider attacks" to "must include outsider working with an insider attacks."

   FPL believes the DG 5022 exceeds the requirements and guidance that was issued in April 2008 for the implementation of the cyber security design basis threat.

   (NEI, p69) NEI believes that 04-04 helps reduce the number CDAs by screening out the exploitation that would have little or no consequence.

**3.0 DG-5022 Regulatory Position** **Tactical Rating: Med**

---

**3.13.1 Venue** - 7.1 Preparation
7.2 Identification
7.3 Containment
7.4 Eradication

7.5 Recovery
7.6 Post-Incident Analysis
7.7 Forensic Activities
7.8 Reporting Requirements

| NRC Positions | Who | Touch Points | Priority |
|---|---|---|---|

NRC Response to Comment 13:

This section may need to be reworded. It should not imply that "law enforcement agencies" always need to be informed over any suspected cyber infringement. However, such agencies must be informed if a suspected, organized and/or intended cyber attack occurs (e.g. apparent accidental infringements do not need to be reported, and intended amateur infringements may not need to be reported).

**3.13.2 Best Practices:** N/A

**3.13.3 Stakeholder Questions:**

1. (NEI, p70) DG 5022, p56 - "The IRR plan should be an integral part of an overall cyber security plan (CSP). The IRR should also be integrated into the site emergency preparedness (EP) plan so that the EP includes the necessary IRR plan response and recovery activities. Such activities should be used in conjunction with established EP and operational procedures that provide a comprehensive and graded level of escalation consistent with the severity of a potential or actual cyber attack. A *potential attack* is a security event in which it is unknown if the underlying cause is a cyber security problem or some other non-security malfunction. "

   NEI states that the EP plan is not specified in 73.54 (e). Can we revise?

2. (NEI, p71) DG 5022, p56 - "7.1 Preparation"

   NEI asks to change wording to match rule.

3. (NEI, p71) DG 5022, p56 - " 7.1.1 Cyber Security Incident Response Team"

   NEI requests this section be moved to the NUREG.

4. (NEI, p73) DG 5022, p57 - "7.1.2 IRR Security Controls"

   NEI requests this section be moved to the NUREG.

5. (NEI, p74) DG 5022, p57 - " 7.2 Identification"

   NEI requests this section be moved to the NUREG.

(STARS, p3 #10) The requirement of processing new threat assessments is a huge task. Can the NRC consider filtering the United States Computer Emergency Readiness Team released threats to an OE on a daily basis for impact assessment at the plants?

6. (NEI, p75) DG 5022, p58 - " 7.4 Eradication"

   NEI asks to change title to "Mitigation".

   (NEI, p76) NEI requests to move this section to NUREG.

7. (NEI, p77) DG 5022, p58 - "7.5 Recovery"

   NEI requests the name change to "Restoration."

   (NEI, p78) NEI requests to move this section to NUREG.

8. (NEI, p79) DG 5022, p59 - " 7.6 Post-Incident Analysis"

   NEI requests to move this section to NUREG.

9. (NEI, p80) Dg 5022, p59 - " 7.7 Forensic Activities"

   NEI requests to move this section to NUREG.

10. (NEI, p81) DG 5022, p61 - " 7.8 Reporting Requirements"

    NEI asks to remove this section and add to DG-5019 "Reporting of Safeguards Events."

    (NEI, p81) NEI asks is it the NRC's intent to have the reporting requirements in two DGs?

11. (NEI, p81) DG 5022, p61 - " law enforcement agencies"

    NEI requests to delete this requirement to notify law enforcement agencies.

12. (NEI, p81) DG 5022, p62 - "At a minimum, the licensee should use, as a guideline, the following to determine a reportable cyber security event where such an event would adversely impact safety, security, and emergency preparedness:

    - (15 Minutes) Upon confirmed cyber attacks posing imminent threat to, or failures of, computer systems.
    - (1 Hour) Upon the determination of a site-specific imminent threat where cyber security defensive protocols have been established to protect safety, security, and emergency preparedness systems.
    - (1 Hour) Upon any observed malevolent cyber threat or actions being threatened

against a plant, a person or organization where someone claims responsibility of such threats or actions, or there is a pattern of such threats or actions.
- (1 Hour) Upon the discovery of a compromised defined electronic or digital security barrier that is intended to protect or provide a protected environment for any nuclear critical asset, system, or network.
- (4 Hours) Upon the discovery of a postulated or potential threat or activity that could manifest into a significant event.
- (4 Hours) Upon the elevation of security protocols triggered by notification from credible agencies where suspicious activities which may be indicative of potential pre-operational surveillance, reconnaissance or intelligence-gathering activities are directed against the facility.

NEI asks if reporting requirements are covered under the station corrective action program, then will they now be required to implement specific timings in the ABN procedures for reporting issues to the NRC? The NRC should stay within current requirements and not break it down further.

**3.13.4 Stakeholder Assumptions:**

1. (NEI, p71) DG 5022, p56 - "7. Incident Response and Recovery"

   NEI believes this section is consistent with NEI 04-04; however it goes to the nth degree in procedure requirements. The sites corrective action program is sufficient in dealing with the issues accordingly.

   TVA's general assumption is that this guidance section is over prescriptive and costly to maintain.

2. (NEI, p72) DG 5022, p56 - "The CSIRT should include the following roles:
   - team leader (single point of contact)
   - cyber security specialist(s)
   - engineering staff responsible for the affected nuclear critical assets
   - computer engineering/IT staff
   - operations coordinator/staff.

   Additional resources that should be available to participate on the CSIRT on an as-needed basis (depending on the incident) include:
   - IT security
   - site security (physical)
   - senior plant management
   - corporate public relations
   - Corporate legal.

   NEI states it will require 1 FTE at each site and may take advantage of existing IT security.

**3.0 DG-5022 C. Regulatory Position** **Tactical Rating: Med**

**3.14.1 Venue** - 8.1 Formulating Awareness and Training Program
8.2 Levels of Cyber Security and Training
8.2.3 Advance Cyber Security Training
8.3 Post-Implementation Activities

| NRC Positions | Who | Touch Points | Priority |
|---|---|---|---|

NRC Comments: N/A

**3.14.2 Best Practices:** N/A

**3.14.3 Stakeholder Questions:**

1. (NEI, p82 to 85) DG 5022, p63 to 65 - " 8.0, 8.1, 8.2 "

   NEI asks to move these sections to the NUREG, however the last paragraph in 8.2.3 can be completely deleted.

2. (NEI, p85) DG 5022, p65 - "8.3 Post-Implementation Activities"

   NEI requests that this is deleted because it is already covered by the systematic approach to training.

**3.14.4 Stakeholder Assumptions:**

1. (FPL, p10, 21) DG 5022, p65 -"Advanced training should be conducted through recognized IT and control system security training programs. It is the NRC staff position that licensee cyber security specialists receive professional certification for the technical courses they take and that requirements and timetables be established for ongoing participation and training programs and acquiring professional cyber security-related certifications. These certifications should be kept current, and records to reflect competencies and currency reflected in an auditable tracking system.

   FPL suggests that it is up to the site if they would rather out source the technical expertise vs. train within.

**3.0 DG-5022 C. Regulatory Position** **Tactical Rating: Med**

**3.15.1 Venue** - 9.1 Modification of Assets and Introduction of New Equipment
9.2 Design Control

| NRC Positions | Who | Touch Points | Priority |
|---|---|---|---|

NRC Response to Comment 4:

This section should be revised to clearly state when upgrades and patches do and do not need NRC approval. In general, approval should not be required for periodic updates or security patches (e.g. updates to virus signatures, OS security fixes, etc), but should be required for version updates (e.g. updates that alter functionality).

**3.15.2 Best Practices:** N/A

**3.15.3 Stakeholder Questions:**

1. (NEI, p86) DG 5022, p65 - " 9.1 Modification of Assets and Introduction of New Equipment"

   NEI requests that this should be moved to the NUREG.

2. (NEI, p87) DG 5022, p65 - "10 CFR Part 73, Paragraph 73.54(d)(4) states that as part of the cyber security program, the licensee shall *"analyze the introduction of new equipment meeting the criteria of (a)(1) and which must be protected in accordance with (b)(1) for potential conflicts with existing assets."* The introduction of new equipment refers to the following circumstances:

   - new hardware that represents all or part of a new nuclear critical asset, system, or network
   - new software for a nuclear critical asset, system, or network
   - new communication hardware or software."

   NEI asks: Does this mean one would have to get NRC approval to upgrade firmware, apply patch, or virus signatures?

3. (NEI, p88) DG 5022, p66 - "9.1.1 Rapidly Changing Digital Equipment and Communication Technologies"

   NEI requests that this should be moved to the NUREG.

4. (NEI, p88) DG 5022, p67 - "9.1.2 Regulatory Requirements for Configuration Management and Control"

NEI requests that this should be moved to the NUREG. The Commission's requirements are well defined for configuration management & control.

5. (NEI, p88) DG 5022, p67 - "9.1.3 Recommended Elements for Configuration and Control Management"

   NEI requests that this should be moved to the NUREG.

6. (NEI, p88) DG 5022, p68 - " Design Control"

   NEI requests that this should be moved to the NUREG.

**3.15.4 Stakeholder Assumptions: (None)**

**3.0 DG-5022 C. Regulatory Position** **Tactical Rating: Med**

**3.16.1 Venue** - 10 Protection of Security-Related Sensitive Information

| NRC Positions | Who | Touch Points | Priority |
|---|---|---|---|

NRC Comments: N/A

**3.16.1 Best Practices:** N/A

**3.16.2 Stakeholder Questions:**

1. (NEI, p89) DG 5022, p69 - "10 Protection of Security-Related Sensitive Information"

   NEI asks: please delete. This is covered in other regulation and guidance.

**3.16.3 Stakeholder Assumptions:**

2. (NEI, p17) DG 5022, p69 - "To augment existing requirements contained within 10 CFR 73.21 and establish a common method of identifying security-related sensitive material, the NRC issued and approved for use Designation Guide DG-SGI-1, "Designation Guide for Safeguards Information." Further, the NRC has provided changes to 10 CFR Part 50, Paragraph 50.34(e), that states "*Each applicant for a license to operate a production or utilization facility, who prepares a physical security plan, a safeguards contingency plan, a training and qualification plan, or a cyber security plan, shall protect the plans and other related Safeguards Information against unauthorized disclosure in accordance with the requirements of §73.21 of this chapter, as appropriate."*

   NEI does not believe this above states that "the cyber security plan is safeguards information. "

(STARS, p2 #8) The Cyber Security Plan should be treated as sensitive information and not safeguards. The Cyber security plan should be incorporated by reference in the PSP. (Chapter 18 of the Physical Security Plan (PSP)).

**3.0 DG-5022 C. Regulatory Position** **Tactical Rating: Med**

**3.17.1 Venue -** 11 Cyber Security Plan
11.1 Cyber Security Program Framework and Integration
11.2 Identification of Nuclear Critical Assets, Systems, and Networks
11.3 Site Cyber Security Defensive Strategies and Security Controls
11.4 Evaluation and Management of Cyber Security Risks
11.5 Incident Response and Recovery
11.6 Cyber Security Awareness and Training
11.7 Modification of Assets and the Introduction of New Equipment
11.8 Records, Retention, Auditing, and Protection of Security Related Information
11.9 References
11.10 Appendix A - Glossary/Abbreviations
11.11 Appendices (additional)

| NRC Positions | Who | Touch Points | Priority |
|---|---|---|---|

NRC Comments: N/A

**3.17.2 Best Practices:** N/A

**3.17.3 Stakeholder Questions: (None)**

**3.17.4 Stakeholder Assumptions:**

1. (NEI, p89) DG 5022, p70 - " 11 Cyber Security Plan"

   NEI believes that the Industry will develop a template to address Cyber Security plan.

2. (NEI, p90) DG 5022, p70 to 76 - "Sections 11.1 to 11.11"

   NEI believes that the Industry will develop a template to address Cyber Security plan.

3. (FPL, p10, 22) DG 5022, p71 - "Conforming changes in 10 CFR Part 50 require submission of a formal cyber security plan."

   FPL believes that Utilizing NEI 04-04 would simplify this process if development.

4. (NEI, p89) DG 5022, p71 - "The plan must be site-specific in addressing the computer and network architecture, security plans, workforce characteristics, and

other aspects of the facility and its operations that are covered by this cyber security plan."

NEI believes the information to be included is too specific and the plan can not be a generic document.

**3.0 DG-5022 C. Regulatory Position** **Tactical Rating: Med**

**3.18.1 Venue -** 12.1 Cyber Security Plan Submittal Requirements
12.2 Licensing Submittal Requirements for New Nuclear Facilities
12.3 Licensing Submittal Requirements for Modifications, upgrades, or Replacement of Existing System

| NRC Positions | Who | Touch Points | Priority |
|---|---|---|---|

NRC Response to Comment 9:

This section should be revised to clearly state when upgrades and patches do and do not need NRC approval. In general, approval should not be required for periodic updates or security patches (e.g. updates to virus signatures, OS security fixes, etc), but should be required for version updates (e.g. updates that alter functionality).

NRC Response to Comment 10:

This section should be revised to clearly state when upgrades and patches do and do not need NRC approval. In general, approval should not be required for periodic updates or security patches (e.g. updates to virus signatures, OS security fixes, etc), but should be required for version updates (e.g. updates that alter functionality).

**3.18.2 Best Practices:** N/A

**3.18.3 Stakeholder Questions:**

1. (NEI, p91) DG 5022, p76 - "12 Licensing Submittal Requirements"

   NEI requests that this section be deleted. It is covered in other staff guidance. "The only time we would submit detailed info as delineated in this section is when - we are submitting a Licensing Amendment Request."

2. (NEI, p17) DG 5022, p77 - "Such plans for existing facilities are to be submitted within 180 days after the effective date of this rule."

   NEI - Can we discuss "the timing of the implementation of the rule?

3. (NEI, p92) DG 5022, p77 - " 12.2 Licensing Submittal Requirements for New Nuclear Facilities"

NEI asks that this section be deleted.

4. (NEI, p92) DG 5022, p78 - " 12.3 Licensing Submittal Requirements for Modifications, upgrades, or Replacement of Existing System"

   NEI requests that this section be deleted.

5. (NEI, p93) DG 5022, p78 - " LAR Submittal"

   NEI requests that this section be deleted. "Requiring ALL Aspects to be completed would mean that when the utility is ready to install, this is the point they make their LAR submittal and hope that the NRC finds it acceptable. This is the Oconee experience. No utility in their right mind would do a digital upgrade that requires an LAR if this requirement has to be met since they would have to spend all the money with out any assurance that they have a success path."

   (NEI, 94) If we have to replace a digital recorder with an upgraded digital recorder, do we have to submit an LAR first? Please remove the LAR requirement. The NRC does not take into account emergent modifications. The LAR may take up to a year for the NRC to approve.

   (STARS, p1,#3) There will be delays in the new plants because of this DG. The design certification documents that already have been submitted will be open to review. Can the NRC create a detailed design and configuration control life cycle management (LCM) phased process including documentation to be completed at each phase and make those available for audit? A process-based inspection will be more effective in ensuring compliance with regulatory requirements rather than a snap shop in time review and approval.

**3.18.4 Stakeholder Assumptions:**

1. (TVA, p18) DG 5022, p77, "Such plans are required to be protected against unauthorized disclosure by licensees and applicants and treated as "Safeguards Information" per 10 CFR 73.21."

   TVA believes that a cyber security plan should be treated as business sensitive under the existing federal regulations and not all plans should be considered safeguard.

   (NEI, p91) NEI does not believe the Cyber Security Plan should be treated as Safe Guarded Information.

2. (NEI, p92) DG 5022, p77 - "12.2 Licensing Submittal Requirements for New Nuclear Facilities"

NEI believes that the SAT time period is premature after the licensing submittal. For the attributes required the SAT plans can not be completed until the AE has completed the design and only then the SAT should be considered a COL item subject to audit prior to fuel load.

3. (TVA, p19) DG 5022, p78, "When modifying, upgrading, or replacing nuclear critical systems or networks, the licensee is to submit the following documents with the Licensing Amendment Request (LAR) (as described in Appendix B) to demonstrate that those assets have been adequately protected against the effects of potential cyber attacks throughout their design life cycle (i.e., from concepts phase through decommissioning of those assets):

   10CFR Part 73, Paragraph 73.54(d)(4)

   TVA claims that it is not practical and defeats the purpose of the utilities to make timely improvements to their cyber security program if they follow DG 5022, where they would be required to upgrade and updates to operating systems, patches, firewall rule changes, installation of new firewalls, etc and wait for the NRC to approve before the implementation.

## 4.0 DG-5022 D. Implementation — Tactical Rating: Med

**4.1.1 Venue** - Back fit

| NRC Positions | Who | Touch Points | Priority |
|---|---|---|---|

NRC Comments: N/A

**4.1.2 Best Practices:** N/A

**4.1.3 Stakeholder Questions: (None)**

**4.1.4 Stakeholder Assumptions:**

1. (NEI, 95) DG 5022, p80 - "Back fit"

   NEI does not agree with the NRC back-fit statement, that there is substantial increase in the overall protection of the public health and safety.

## 5.0 DG-5022 Glossary — Tactical Rating: Med

**5.1.1 Venue** -

| NRC Positions | Who | Touch Points | Priority |
|---|---|---|---|

NRC Comments: N/A

**5.1.2 Best Practices:** N/A

**5.1.3 Stakeholder Questions: (None)**

**5.1.4 Stakeholder Assumptions:**

1. (FPL - p10, 23) DG 5022, p81 -

   FPL believes the definition limits the options and is unduly restrictive.

## 6.0 DG-5022 APPENDIX A. CYBER SECURITY ASSESSMENT AND RISK MANAGEMENT Tactical Rating: Med

**6.1.1 Venue** - Appendix A

| NRC Positions | Who | Touch Points | Priority |
|---|---|---|---|

NRC Comments: N/A

**6.1.2 Best Practices:** N/A

**6.1.3 Stakeholder Questions:**

1. (NEI, p95) DG 5022, p96 - " Appendix A"

   NEI requests this section be moved to the NUREG.

   (NEI, p95) A NEI request that the NRC provide what is the considered acceptable risk based on some sort of risk scoring procedure. Recommend CR-6847 be revised and issued along with the RG 5022 or DG 5022 should include an acceptable risk scoring methodology.

2. (NEI, p96 & 97) DG 5022, p96 to 105 - "All sections of Appendix A"

   NEI requests they be moved to the NUREG.

**6.1.4 Stakeholder Assumptions:**

1. TVA assumption is that the guidance is over prescriptive and costly to maintain.

## 7.0 DG-5022 APPENDIX B. CYBER SECURITY GUIDANCE FOR THE INTRODUCTION OF NUCLEAR CRITICAL, ASSETS, SYSTEMS, AND NETWORKS. Tactical Rating: Med

**7.1.1 Venue** - Appendix B

| NRC Positions | Who | Touch Points | Priority |
|---|---|---|---|

NRC Comments: N/A

**7.1.2 Best Practices:**

1. (NEI, p97 to 98) DG 5022, p106 to 117 - "Appendix B"

   NEI requests that all of Appendix B is moved to the NUREG.

**7.1.3 Stakeholder Questions:**

1. (STARS, p2, #4) DG 5022, p106 - "Appendix B"

   STARS asks: Can the NRC add requirements directly to the Vendors?

**7.1.4 Stakeholder Assumptions:**

1. TVA assumption is that the guidance is over prescriptive and costly to maintain.

## 8.0 DG 5022 Document — Tactical Rating: Med

**Venue** - General Comments

The draft Regulatory Guide is inconsistent with respect to the content, basis and interpretation of issued regulation, including 10CFR73.54. (STARS)

The NIST 800-82 standard referenced is a draft standard for control systems and data acquisition system (DASs). Industrial control systems and DASs are vastly different from IT enterprises and large data centers. As such, security considerations are very different based on functionally, criticality and connectivity. (STARS)

The standards should be limited to the NUREG/CR 6847 (the basis for NEI 04-04 Guidance), Regulatory Guide 1.152, IEEE 7.4.3.2 and other already issued orders and rules that pertain to cyber security. (STARS)

The Introduction of Security overlays and new interface organizations will introduce failure modes that will be very hard to analyze and create more opportunity of degradation of safety and plant reliability. (NEI)

Too much guidance is complied from NIST. (NEI)

If the NRC is not responsible for Continuity of power systems, all requirements other than the ones for Safety Systems should be removed from this Regulatory Guide. (NEI)

Currently the NRC NRR I&C Branch is having difficulty dealing with even the less complex systems, imagine what will happen with the failure modes and probabilities of security features comes into play for RPS/ESFAS. (NEI)

The draft guide is overly complex, overly prescriptive for a guidance document and goes beyond the required to ensure adequate protection for nuclear safety. (TVA)

The requirements extend to areas which more closely align with keeping the plant on line. (TVA)

For insider threats this draft guide is contrary to the NRC position stated in Regulatory Guide 5.69. (FPL)

For Autonomous systems the DG-5022 fails to recognize reliance upon the insider mitigation program for protection. (FPL)

A site centric digital communication monitoring system may not be more secure than the implementation of an in-band remotely controlled secured system. (FPL)

NEI recommends the relocation of several sections of the draft guide sections to a NUREG document. (FPL)

Based upon the content of DG-5022, it is recognized that NEI 04-04 Rev 01 may need additional criteria added to completely satisfy the regulation’s requirements. (FPL)

## Stakeholder Comments on Key Guidance in DG-5022

*Presented by the NEI to the NRC at the Stakeholder Meeting on Dec. 12, 2008*

(All NRC comments are in **BLUE** and can be used when addressing NEI.)

1. *Cyber Plan*
   a. *DG-5022 should clearly state the overall purpose of the Cyber Security Plan (CSP) as required by 10CFR73.54. DG-5022 should state the regulatory finding that the stall intends to make when they approve the CSP.*

(DO NOT AGREE)
The purpose of the cyber security plan is self-evident in the rule language contained in 10 CFR 73.54 paragraphs (e), (e)(1), (e)(2)(i-iv).

   b. *The CSP should convey a brief description of how a current or future nuclear facility would comply with the requirements 10CFR73.54.*

(DO NOT AGREE)
The material presented within DG-5022 identifies one acceptable method to comply with the requirements of DG-5022. Other methods may also exist.

   c. *Industry understanding is that the Plan to be submitted to the NRC would be a high-level plan.*

(AGREE)
Provide modifications to text in Section 4.0 Cyber Security Plan to alter or remove items that would result in unnecessary submissions of license amendments.

   d. *Level of detail in the CSP should be similar to that in NEI 03-12 (for the Physical Security Plan)*

(AGREE)
Although we agree with this concept, the DG-5022 is not the appropriate place by which to reference NEI 03-12. Rather the modifications to the text provided in Section 4.0 lists the expected level of detail to be provided when submitting a CSP. NEI can elect to provide a modified template of NEI 03-12 to the Commission for review to determine adequacy.

ACTION REQUIRED: Modified Text for Section 4.0 Cyber Security Plan (entire section):

2. *The current draft of the DG-5022 attempts to be a comprehensive guide for cyber security. The guide should leverage existing NRC/industry regulation, program,*

*and processes to address specific cyber security program to minimize overall risk exposure.*

*a. Policies and Implementing procedures*
*b. Self Evaluation (Assessment, OE, & Corrective action Programs)*
*c. Physical Security*
*d. SGI*
*e. Roles and responsibilities*
*f. Nuclear Incident Response*
*g. Radiological Emergency Plan*
*h. Design Control/Configuration Control*

(AGREE)

The components of a cyber security program may be performed as a concurrent engineering activity and integrated into an existing system engineering lifecycle and other regulatory programs, in order to leverage existing policies and implementing procedures.

3. Recognize within the document that the existing programs and processes carry out NRC regulatory requirements or existing NRC endorsements to establish, implement, and maintain cyber security programs. Some of the guidance in DG-5022 is a duplicate of and in potential conflict with existing regulations and endorsements.

a. 10CFR 73.55
b. 10CFR 50 Appendix B
c. 10CFR Part 26
d. Systematic approach to training - 10CFR50.120
e. RG 1.152; 1.168-1.173
f. DBT 5.69
g. DG 5011 - Insider threat mitigation
h. Incident Response/Reporting
i. ISG-1, ISG-4, IGS-6
j. IEEE 7.4.3.2 (DRAFT)
k. NEI 04-04 Revision 1
l. Operating experience program

(UNKNOWN)

NEI needs to clarify how these items apply. The NRC is building a matrix to cover these touch points.

ACTION REQUIRED: NONE

4. *The regulatory guide should map 10CFR73.54 to a graded approach (as found in RG 1.97) for requirements based on informed criteria such as physical security,*

*connectivity, system function (e.g., safety, important-to-safety, security, emergency preparedness) and susceptibility to cyber threat.*

*a. Defensive Strategy*
*b. Design Modification*
*c. Assessment*
*d. Cyber Security Plan*
*e. Should address total risk mitigation*

(AGREE IN PART)

Section 2.2, paragraph 1, sentence 2 on page 10 of DG-5022 already states the following:

"An acceptable method for establishing a cyber security program that complies with these requirements utilizes a graded approach, based on risk-informed processes to systematically maintain security throughout the life -cycle of the critical systems and CDAs."

a. Defensive strategies exist to provide assist in providing defense-in-depth which also represents a graded approach.
b. The graded approach to the protection of critical systems is most closely related to the cyber security assessment process as outlined in NUREG/CR-6847.
c. The design modification process as outlined in Section 3.7 represent items to be addressed in each phase of the design process. Section 3.7.6, paragraph 2, item e identifies that a detailed cyber security assessment on the installed critical system is to be performed. That assessment to be performed is the same process as outlined in NUREG/CR-6847. It is not possible to perform a NUREG/CR-6847 type of assessment without first having an installed system.
d. The cyber security plan is a report to be submitted to the NRC that identifies how a licensee has implemented its site-specific cyber security plan. The report submitted by the licensee may contain information as to the graded approach taken in items (g) and (h) in the newly-modified sections.
e. No cyber security plan can address total risk mitigation. Even with the application of state-of-the-art technologies, there will be some threat vectors that cannot be eliminated or mitigated. That is the reason a graded approach is specified within Section 2.2 as identified above.

ACTION REQUIRED: In the next revision of NUREG-CR-6847, explicit language will be provided that more clearly identifies the graded approach as it applies to safety, security, and EP-related systems. No change is required in DG-5022.

**(5 is the same as 4)**

5. Integrate software of quality assurance, cyber security, Plant Reliability (INPO AP-913) into one set of graded approach criteria.

(AGREE IN PART)
Section 2.2, paragraph 1, sentence 2 on page 10 of DG-5022 already states the following:

"An acceptable method for establishing a cyber security program that complies with these requirements utilizes a graded approach, based on risk-informed processes to systematically maintain security throughout the life -cycle of the critical systems and CDAs."

ACTION REQUIRED: In the next revision of NUREG-CR-6847, explicit language will be provided that more clearly identifies the graded approach as it applies to safety, security, and EP-related systems. No change is required in DG-5022.

6. Throughout the DG-5022, do not interpret 10CFR73.54. Where the rule is cited ensure that language is the same as the regulation.

(AGREE) Provide modifications to text in Section 4.0 Cyber Security Plan to alter or remove items that would result in unnecessary submissions of license amendments.

7. Remove prescriptive guidance that is outside the scope of 10CFR73.54, such as:

   a. DG-5022 prescribes incorporating the cyber security organization within the physical security organization. This is not required because Cyber Security is a component of Physical Security and is Chapter 18 of the Physical Security Plan.

(DO NOT AGREE)

   b. DG-5022 prescribes specific technical details regarding, for example, IDS/IPS, encryption, media sanitization, honey-pots.

(DO NOT AGREE)

   c. Some requirements are not cost-beneficial and have not been reflected in the Commissions regulatory analysis associated with the Final Rule. Therefore they would be considered backfits and would be required to meet the threshold of 10CFR50.109.

(OUT OF NRC's SCOPE)

ACTION REQUIRED: NONE

8. *Presently, it is not technically feasible to implement the full scope of the guidance in DG-5022.* This is an inaccurate comment made by an NEI IT cyber security

specialist that has no prior plant or controls experience (I talked with him at the conclusion of the meeting in December).

a. *For example, the out-of-band security monitoring network would directly violate the requirement to have unidirectional communication between Security Levels 4 and 3.*

b. *The ERDS program would violate the requirements prescribed in DG-5022. In some cases implementing some of the violate vendor license agreements.*

(QUESTION/ASSUMPTION)

ANSWERS:

a. An out-of-band security monitoring network would not violate the requirement to have unidirectional communications between security levels 4 and 3. The requirement for unidirectional communications applies to the data-flow provided to or from critical systems located within a given security level that happens to transition a given security boundary. One reason for the existence of the security monitoring network is to provide a further level of protection by ensuring the control of *security devices* such as firewalls and IDS/IPS occurs through a separate dedicated management interface. Such control is preferable to in-band control as is much more difficult for an adversary to reconfigure such a device when the installed rules prevent such types of traffic from being accepted by the managed interface. Another reason for a security monitoring network is that it allows for consolidation of event data related to an intrusion from a multitude of security-related devices.

b. Communications with ERDS devices should be conducted in the same manner as the data from any critical system that transitions security levels. The data should be made available through controlled interfaces consistent with DG-5022 Sections 3.2.1 *Overall Site-Defensive Strategy*, 3.2.2.5 *Remote Connectivity*, Section 3.2.2.6 *Modems*, and 3.3.1 *Security Boundaries* as applicable. Licensees should not assume that NRC networks are any more trustworthy than any other foreign network. If improperly secured, such connections could provide a potential attack vector to plant critical systems. A relevant example of such a vector of attack was realized when the Davis Bessie plant computer system infected by a worm from a trusted vendor. ERDS data should be properly migrated out from the plant just like any other data that is destined for use in a network located in a lesser security level.

ACTION REQUIRED: NONE

9. *Clarify language where the implementation guidance could cause adverse impact to plant operation and safety:*
   a. *Packet sniffers, active network scanning*
   b. *Automatic mitigation and recovery of plant systems/components*

(DO NOT AGREE)

a. The use of packet sniffing technology is covered in Section 3.3.4 Packet Sniffers. Item (b) of this section identifies that network taps should be used when deploying sniffers. Network taps are commonly used to provide an optically-isolated, unidirectional sampling of streamed data. The use of network taps ensures that the sniffer itself cannot adversely impact the network it is monitoring.

   With regard to active network scanning, Section 3.6.6 Physical Walkdown and Electronic Validation of Critical Systems, items (b)(xiii) and (b)(xiv) explicitly state the following:

   xiii: "Vulnerability scanning. NOTE: It is recommended when performing *active vulnerability scans* of critical digital assets it is performed in an off-line condition where the critical digital asset is not being relied on to perform a required function. *Passive vulnerability scanning* may be performed on critical digital assets while the critical digital asset is being relied on to perform a required function as long as the activity does not result in an adverse effect to the critical system or critical digital asset under assessment."

   xiv: "Penetration testing (optional). NOTE: Penetration testing may cause major disruptions to the critical system being probed. Extreme caution must be exercised in conducting such testing, to preclude any adverse impact on plant safety, security, and emergency preparedness."

   At no time is it suggested that these activities be performed where a condition exists that would result in adverse impact to plant operation or safety.

b. No section of DG-5022 addresses the automatic mitigation and recovery of plant systems/components.

ACTION REQUIRED: NONE

10. *Terminology and definitions need to be consistent. For example, system, critical system, critical digital system are used interchangeably. Definitions within the document must be consistent with those in the Glossary. Definitions should be bounding, unambiguous, and used consistently. Examples of ambiguously defined or used terms include:*
    *a. "Emergency preparedness" is ambiguous.*
    *b. "Important to safety" is ambiguous*
    *c. Critical Systems is defined inconsistently*
    *d. Hardening is defined inconsistently.*

(AGREE)

a. The definition of emergency preparedness is supplied in the glossary which identifies emergency preparedness systems as being:

"Systems, components, and equipment that provide reasonable assurance that adequate protection and mitigation measures can be taken in the event of a radiological emergency at the facility. Systems include those that provide for prompt communications among principal response organizations; onsite facilities and equipment to support the emergency preparedness; and methods and equipment onsite for assessing and monitoring actual or potential offsite consequences."

No other definition exists within the document and the use of the term is provided consistently throughout the document.

b. The term "important-to-safety" is used within the rule text stated in 10 CFR 73.54(a)(1)(i). Its use is consistent within the document; however the glossary does not currently provide a definition.

ACTION: Provide a definition for important-to-safety

c. The definition of a critical system is identified in the glossary to be:

**"critical system** - collectively identifies those systems and networks associated with safety-related and important-to-safety functions; security functions; emergency preparedness functions including offsite communications; and support systems and equipment which, if compromised, would adversely impact safety, security or emergency preparedness functions."

There are a couple of instances in the body of the document where inline definitions exist. The inline definitions themselves are not incorrect given the surrounding context of the paragraph, however, it is not as consistent as it could be.

ACTION: Ensure that inline definitions are consistent with those stated in the glossary. This will occur during text editing.

d. The definition of "hardened" is identified within the glossary to be:

**hardened** - Devices configured to be resistant to cyber attack. System hardening results in a minimalistic exposure to cyber threat by reducing the exposure or existence of vulnerabilities through system configuration.

This definition provided generically describes the state of a hardened device. Section 3.2.2.2 provides a listing of items that should be addressed when hardening a system. The use of the term "hardening" is not inconsistently defined throughout the document.

ACTION: In Section 3.2.2.2 System Hardening, replace list a-f with the modified list of a-g detailed above.

**hardened**--Devices configured to be resistant to cyber attack. System hardening results in a minimalistic exposure to cyber threat by reducing the exposure or existence of vulnerabilities through system configuration. This may be accomplished by:

a. removal of unnecessary default accounts or test accounts, file shares, operating system services and ports
b. installation of access controls on file systems, file shares, registries, executables (binaries) where possible to limit inappropriate access or misuse of the system
c. controlling access to the peripheral resources (e.g, external drives, ports (Serial/Parallel, USB, SCSI, Firewire)
d. implementing role-based access controls where appropriate, and reducing privileges to the lowest level possible to reasonably perform a users job function
e. monitoring and logging of logical access to critical digital systems and critical digital assets
f. patching of known vulnerabilities
g. providing physical security measures to prevent access to hardware

11. Identify clear acceptance criteria:
    a. "...but not limited to"

(AGREE IN PART)

Some of the phrases "...but not limited to" are required because of the nature of the technology.

b. Bulleted items are either all inclusive, or ...?

(AGREE) - Working to clarify the differences in a standard format.

12. Cyber security plan and other cyber security documents are not safeguards unless they already meet the safeguards requirements in 10CFR73.21, 73.22, and 10CFR2.390.

(DO NOT AGREE)

ACTION REQUIRED: NONE

13. *Physical and logical boundaries do not have a one-to-one correspondence. For example, PLCs in Protected Area are designated as being cyber security Level 4 assets.*

(DO NOT AGREE)

This assertion is incorrect. This concept was taken directly from NEI 04-04. A one-to-one relationship is identified within NEI 04-04 Appendix B, Page B-6, *Figure B-3: Physical Security Model* that maps the logical aspects of the security

model to the physical areas that exist at each nuclear site. The staff is aware of the fact that when applying theoretical models to real world scenarios, situations will exist where strict adherence to the model is not possible. For this reason, the staff has identified in Section 3.2.1, Overall Site Defensive Strategy, Paragraph 3, Page 13, that exceptions to the model can be made as long as they are fully documented, analyzed, and adequate security controls are used to maintain the high assurance criteria specified in 10 CFR 73.54(a). New plant designs should have fewer exceptions as compared to legacy plants since their designs should take into account the use of a defensive model.

ACTION REQUIRED: NONE

14. Emergency Preparedness
    a. Provide a clear delineation of EP systems to be protected under 10CFR73.54 and those that are not required to be covered under 73.54.
        i. WebEOC and DiaLogics (Emergency Paging systems) and other business related emergency preparedness initiatives
    b. How do emergency response systems affect the ability to prevent radiological sabotage and the theft of nuclear material?
    c. Clarify requirements for communication systems.

ACTION REQUIRED: NONE

These are questions that the Licensee needs to clarify. For part a, this is part of the Licensee's responsibility. Part b the answer is by a graded approach and for part c we need more clarification of what communication systems the Licensee is talking about.

# Stakeholder Comments on Key Guidance in DG-5022

*Presented by the NEI to the NRC as an email after the Jan. 14, 2009 Stakeholder meeting.*

(All NRC comments are in **BLUE** and can be used when addressing NEI.)

Date: 1/15/2009

Good Morning Karl,

On behalf of the Cyber Security Standing Committee, I wish to express my appreciation for the NRC hosted meeting on January 14. We are encouraged with the progress and direction made in the development of the DG to date. The following comments are being provided for the DG-5022 structure agreed on in the meeting and the rewritten technical guidance in progress by the NRC writing team.

1. Physical Security Boundaries and Cyber Security Logical Boundaries do not have a one-to-one correspondence.

(AGREE)

2. Replace phrases using the term “Acceptable” with the phrase like “A method that can be used...”

(AGREE IN PART)

3. Remove the word “dedicated” from the Security Monitoring Network.

(AGREE IN PART)

4. Replace discussion associated with “Adversary” and “Threat” with reference to DBT in RG 5.69. Remove DHS Threat discussion or align with the DBT in arg 5.69.

(AGREE IN PART)

5. Ensure guidance in DG-5022 aligns with the intent of the Commissioners as expressed in SECY 2008-0099 such as the following:

   a. Organizational structure (pages 29 and 121)*

(DO NOT AGREE) The Rule 10 CFR 73.54(g) can not be changed.

b. Define Cyber Attack in such a way to ensure that criminal prosecution is not executed for inadvertent actions (pages 16 and 145)

(AGREE IN PART) The NRC will review the language in DG-5022.

6. Place all definitions in a Glossary.

(AGREE)

*As discussed, escalate the discussion about the alignment of the cyber security organization into the physical security organization. We suggest this may be accomplished by stating the performance objectives you would like to achieve as opposed to specifying a particular organization structure. For example, a performance objective might be stated like... " the Cyber Security technical specialist has appropriate separation of duties to ensure critical digital assets are adequately protected."