

**From:** Pascarelli, Robert  
**Sent:** Tuesday, March 09, 2010 9:36 AM  
**To:** phlashley@firstenergycorp.com; Patricia.Furio@cengllc.com; Edmund.Tyler@cengllc.com; jpechac@entergy.com; RWalpol@entergy.com; jlynch4@entergy.com; fmcginn@entergy.com; wlobo@entergy.com; Thomas.HardingJr@cengllc.com; mhcrowthers@pplweb.com; jmeyer5@entergy.com; jdevinc@entergy.com; Jeffrie.Keenan@pseg.com; margaret.earle@dom.com; michael\_okeefe@nexteraenergy.com; Randy.hart@duke-energy.com; bdmckinn@southernco.com; Ken.ashe@duke-energy.com; Kent.alter@duke-energy.com; bthompson@scana.com; fcmashburn@tva.gov; DavidBryan.Miller@pgnmail.com; Ken.Frehafer@fpl.com; Eric.Katzman@fpl.com; Bob.Tomonto@FPL.com; mkscarpello@aep.com; Tony.Browning@nexteraenergy.com; hassouna@dteenergy.com; Gabor.Salamon@xenuclear.com; Richard.Loeffler@xenuclear.com; gschwar@entergy.com; JAMES.COSTEDIO@nexteraenergy.com; Dale.Vincent@xenuclear.com; douglas.walker@exeloncorp.com; phlashley@firstenergycorp.com; rclark@entergy.com; telwood@ameren.com; mchumphreys@energy-northwest.com; dwvande@nppd.com; fburfor@entergy.com; Timothy.hope@luminant.com; TRB1@pge.com; bhansher@oppd.com; Russell.Stroud@aps.com; BBURMEI@entergy.com; DLORFIN@entergy.com; Linda.Conklin@sce.com; awharrison@stpegs.com; mmason@entergy.com; dihoope@wcnoc.com; kecasey@tva.gov  
**Cc:** Erlanger, Craig; Howe, Allen; Singal, Balwant; Wengert, Thomas  
**Subject:** draft generic questions on NEI-08-09  
**Attachments:** Generic cyber questions 0309.doc

On January 28, 2010, I forwarded you a set of draft generic questions on Appendix A of NEI 08-09 that had been shared with the Executive Task Force of the Nuclear Security Working Group (NSWG) and NEI. Both groups have committed to representing operating power reactor licensees by working with the NRC to resolve these generic questions. The NRC has discussed these questions with the NSWG and NEI and we received a written response to the first set of questions on March 5th. The purpose of this transmittal is to provide all operating reactor licensees with an information copy of the second set of draft generic questions which were provided to both groups on February 26, 2010. In order to minimize confusion due to large number of questions and subsequent modifications, a single file containing all 76 questions is attached. Questions 1 through 30 were attached to my January 28th e-mail.

It should be noted that the draft generic questions that were attached to my January 28, 2010 e-mail were designated Official Use Only - Security Related Information because the NEI-08-09, Revision 3 template that was utilized for your license amendment requests was withheld from public disclosure under 10 CFR 2.390. On February 4, 2010, NEI submitted NEI-08-09, Revision 5. This revision removed the withhold from public disclosure under 10 CFR 2.390 marking but did not change the content of the document or affect the draft generic questions. Since NEI-08-09, Revision 5 does not contain security-related information and is publically available (ML100610106) the complete list of draft generic questions will be made available on the public side of ADAMS.

Within the next few weeks, the NRC will be evaluating these responses and factoring that information into our acceptance review evaluation for the cyber security plans that were submitted as license amendment requests. The attached generic questions are being provided for information only and **no response from licensees is required at this time**. If these cyber security plans are accepted for review, these draft generic questions will be issued to all licensees as Requests for Additional Information (RAI's) and will require a formal licensee response.

Attachments:

1. Draft generic questions on NEI 08-09

Robert Pascarelli, Chief  
Plant Licensing Branch III-1  
Division of Operating Reactor Licensing  
Office of Nuclear Reactor Regulation

---

### E-mail Properties

Mail Envelope Properties (F9A211EDBB9D36408BEFE2CBD7380E280CC188C1A3)

Subject: draft generic questions on NEI-08-09  
Sent Date: 3/9/2010 9:36:21 AM  
Received Date: 3/9/2010 9:36:00 AM  
From: Pascarelli, Robert

Created By: Robert.Pascarelli@nrc.gov

Recipients:

phlashley@firstenergycorp.com (phlashley@firstenergycorp.com)  
Tracking Status: None  
Patricia.Furio@cengllc.com (Patricia.Furio@cengllc.com)  
Tracking Status: None  
Edmund.Tyler@cengllc.com (Edmund.Tyler@cengllc.com)  
Tracking Status: None  
jpechac@entergy.com (jpechac@entergy.com)  
Tracking Status: None  
RWalpol@entergy.com (RWalpol@entergy.com)  
Tracking Status: None  
jlynch4@entergy.com (jlynch4@entergy.com)  
Tracking Status: None  
fmcginn@entergy.com (fmcginn@entergy.com)

Tracking Status: None  
wlobo@entergy.com (wlobo@entergy.com)  
Tracking Status: None  
Thomas.HardingJr@cengllc.com (Thomas.HardingJr@cengllc.com)  
Tracking Status: None  
mhcrowthers@pplweb.com (mhcrowthers@pplweb.com)  
Tracking Status: None  
jmeyer5@entergy.com (jmeyer5@entergy.com)  
Tracking Status: None  
jdevinc@entergy.com (jdevinc@entergy.com)  
Tracking Status: None  
Jeffrie.Keenan@pseg.com (Jeffrie.Keenan@pseg.com)  
Tracking Status: None  
margaret.earle@dom.com (margaret.earle@dom.com)  
Tracking Status: None  
michael\_okeefe@nexteraenergy.com (michael\_okeefe@nexteraenergy.com)  
Tracking Status: None  
Randy.hart@duke-energy.com (Randy.hart@duke-energy.com)  
Tracking Status: None  
bdmckinn@southernco.com (bdmckinn@southernco.com)  
Tracking Status: None  
Ken.ashe@duke-energy.com (Ken.ashe@duke-energy.com)  
Tracking Status: None  
Kent.alter@duke-energy.com (Kent.alter@duke-energy.com)  
Tracking Status: None  
bthompson@scana.com (bthompson@scana.com)  
Tracking Status: None  
fcmashburn@tva.gov (fcmashburn@tva.gov)  
Tracking Status: None  
DavidBryan.Miller@pgnmail.com (DavidBryan.Miller@pgnmail.com)  
Tracking Status: None  
Ken.Frehafer@fpl.com (Ken.Frehafer@fpl.com)  
Tracking Status: None  
Eric.Katzman@fpl.com (Eric.Katzman@fpl.com)  
Tracking Status: None  
Bob.Tomonto@FPL.com (Bob.Tomonto@FPL.com)  
Tracking Status: None  
mkscarpello@aep.com (mkscarpello@aep.com)  
Tracking Status: None  
Tony.Browning@nexteraenergy.com (Tony.Browning@nexteraenergy.com)  
Tracking Status: None  
hassouna@dteenergy.com (hassouna@dteenergy.com)  
Tracking Status: None  
Gabor.Salamon@xenuclear.com (Gabor.Salamon@xenuclear.com)  
Tracking Status: None  
Richard.Loeffler@xenuclear.com (Richard.Loeffler@xenuclear.com)

Tracking Status: None  
gschwar@entergy.com (gschwar@entergy.com)  
Tracking Status: None  
JAMES.COSTEDIO@nexteraenergy.com (JAMES.COSTEDIO@nexteraenergy.com)  
Tracking Status: None  
Dale.Vincent@xenuclear.com (Dale.Vincent@xenuclear.com)  
Tracking Status: None  
douglas.walker@exeloncorp.com (douglas.walker@exeloncorp.com)  
Tracking Status: None  
phlashley@firstenergycorp.com (phlashley@firstenergycorp.com)  
Tracking Status: None  
rclark@entergy.com (rclark@entergy.com)  
Tracking Status: None  
telwood@ameren.com (telwood@ameren.com)  
Tracking Status: None  
mchumphreys@energy-northwest.com (mchumphreys@energy-northwest.com)  
Tracking Status: None  
dwvande@nppd.com (dwvande@nppd.com)  
Tracking Status: None  
fburfor@entergy.com (fburfor@entergy.com)  
Tracking Status: None  
Timothy.hope@luminant.com (Timothy.hope@luminant.com)  
Tracking Status: None  
TRB1@pge.com (TRB1@pge.com)  
Tracking Status: None  
bhansher@oppd.com (bhansher@oppd.com)  
Tracking Status: None  
Russell.Stroud@aps.com (Russell.Stroud@aps.com)  
Tracking Status: None  
BBURMEI@entergy.com (BBURMEI@entergy.com)  
Tracking Status: None  
DLORFIN@entergy.com (DLORFIN@entergy.com)  
Tracking Status: None  
Linda.Conklin@sce.com (Linda.Conklin@sce.com)  
Tracking Status: None  
awharrison@stpegs.com (awharrison@stpegs.com)  
Tracking Status: None  
mmason@entergy.com (mmason@entergy.com)  
Tracking Status: None  
dihoope@wcnoc.com (dihoope@wcnoc.com)  
Tracking Status: None  
kecasey@tva.gov (kecasey@tva.gov)  
Tracking Status: None  
Craig.Erlanger@nrc.gov (Erlanger, Craig)  
Tracking Status: None  
Allen.Howe@nrc.gov (Howe, Allen)

Tracking Status: None  
Balwant.Singal@nrc.gov (Singal, Balwant)  
Tracking Status: None  
Thomas.Wengert@nrc.gov (Wengert, Thomas)  
Tracking Status: None

Post Office:  
HQCLSTR02.nrc.gov

Files	Size	Date & Time
MESSAGE	267016	3/9/2010
Generic cyber questions 0309.doc		219882

Options  
Expiration Date:  
Priority: olImportanceNormal  
ReplyRequested: False  
Return Notification: False

Sensitivity: olNormal  
Recipients received: ZZZ

## APPENDIX A GENERIC QUESTIONS

1. 10 CFR 73.54 requires the licensee to submit cyber security plans to the NRC. The [Site/Licensee] Cyber Security Plan (CSP) refers to NEI 08-09, Revision 3, Cyber Security Plan for Nuclear Reactors. Various versions of NEI 08-09, Revision 3, were submitted to NRC. What is the date of NEI 08-09, Revision 3, referenced in the CSP? (Note that several licensee CSP submittals incorporate NEI 08-09, Revision 3, and Appendices D & E by reference only).
  
2. 10 CFR 73.54(d)(2) requires the licensee to evaluate and manage cyber risks. The [Site/Licensee] Cyber Security Plan (CSP) Section 3.1.2, "Cyber Security Assessment Team," (CSAT) states that one of the roles and responsibilities of the CSAT is "Evaluating assumptions and conclusions about known cyber security threats; potential vulnerabilities to, and consequences from an attack; the effectiveness of existing cyber security controls, defensive strategies, and attack mitigation methods; cyber security awareness and training of those working with, or responsible for CDAs [critical digital assets] and cyber security controls throughout their system life cycles." Explain how [Site/Licensee] uses the process described above will to stay current on cyber security threats. Please provide a list the sources of cyber security threat information used by [Site/Licensee].
  
3. 10 CFR 73.54(b)(1) requires the licensee to Analyze digital computer and communication systems and networks and identify those assets that must be protected against cyber attacks. Section 3.1.3, "Identification of Critical Assets", of the [Site/Licensee] Cyber Security Plan provides a list of documentation that will be developed for each critical system (CS) examined. Explain how security functional requirements or specifications will be documented with respect to each CS and their associated critical digital assets (CDAs).
  
4. 10 CFR 73.54(b)(2) requires the licensee to establish, implement, and maintain a cyber security program for the protection of the digital assets. Section 3.1.5, "Tabletop Reviews and Validation Testing," of the [Site/Licensee] Cyber Security Plan states "Performing, where practical, a physical inspection of the connections and configuration of CDAs [critical digital asset], including tracing digital communication connections into and out of the CDA to termination points along digital communication pathways." Explain how physical inspections of connections and configurations of CDAs will trace communication connections into and out of the CDA to each termination point along digital and analog communication pathways.
  
5. 10 CFR 73.54(c)(1) requires the cyber security program to implement security controls to protect the assets identified by paragraph (b)(1) from cyber attacks. Section 3.1.6, "Mitigation of Vulnerabilities and Application of Cyber Security Controls," of the [Site/Licensee] Cyber Security Plan states "Implementing alternative controls/countermeasures that eliminate threat/attack vector(s) associated with one or more of the cyber security controls enumerated in (1) above by:

- Performing and documenting the analyses of the CDA [critical digital asset] and alternative countermeasures to confirm that the countermeasures provide the same or greater cyber security protection as the corresponding cyber security control.”

Please describe the process, methods and considerations of the above analyses (e.g., use of “attack vector” analyses).

6. 10 CFR 73.54(c)(1) requires the licensees to implement security controls to protect the assets within the scope of the Rule from cyber attacks. Section 4.2, “Cyber Security Controls,” of the [Site/Licensee] Cyber Security Plan (CSP) states “Alternate controls are implemented in situations where a CDA [critical digital asset] cannot support, or the organization determines it is not advisable to implement, a particular cyber security control because that control could adversely impact SSEP [safety, security, and emergency preparedness] functions. Justification for how the selected controls provide an acceptable cyber security capability or level of protection for the CDA is documented. Evaluation and justification is performed and documented.” Explain the process and provide the criteria for selecting alternate controls to mitigate the lack of the security control for the CDA in accordance with the process described in Section 3.1.6 and clarify that the justification process is applied to all of the alternate security controls that provide equivalent protection in lieu of the security controls from Appendices D and E that cannot be implemented.

7. 10 CFR 73.54(c)(2) requires the licensee to apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks. Section 4.3, “Defense-in-Depth Protective Strategies,” of the [Site/Licensee] Cyber Security Plan (CSP) discusses restricting communications from lower defensive levels to higher defensive levels however does not elaborate how these communications will be restricted. Explain how communications from lower defensive levels to higher defensive levels will be restricted.

8. 10 CFR 73.54(c)(2) requires the licensee to apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks. Section 4.3, “Defense-in-Depth Protective Strategies,” of the [Site/Licensee] Cyber Security Plan discusses protective strategies. Explain how the defensive architecture, in addition to the security controls, manages communications between defensive levels and how the defensive architecture maintains the capability to detect, prevent, delay, mitigate, and recover from cyber attacks.

9. 10 CFR 73.54(b)(2) requires the licensee to establish, implement, and maintain a cyber security program for the protection of the assets within the scope of the Rule. 10 CFR 73.54(d)(2) requires the licensee to evaluate and manage cyber risks. Section 4.4, “Ongoing Monitoring and Assessment,” of the [Site/Licensee] Cyber Security Plan (CSP) describes the ongoing monitoring program. Explain how and with what periodicity the [Site/Licensee] will verify that rogue assets have not been connected to the infrastructure.

10. 10 CFR 73.54(d)(3) requires the licensee to ensure that modifications to assets within the scope of the Rule are evaluated before implementation. 10 CFR 73.54(f) requires the licensee to develop and maintain written policies and implementing procedures to implement the cyber security plan. 10 CFR 73.54(g) requires the licensee to review the cyber security program as a component of the physical security program in accordance with the requirements of 10 CFR 73.55(m), including the periodicity requirements. Section 4.4.1, "Configuration Management and Change Control," of the [Site/Licensee] Cyber Security Plan (CSP) states "A configuration and cyber security life cycle management approach is implemented to update and maintain cyber security controls for CDAs [critical digital assets] in order to ensure that the cyber security program objectives remain satisfied." Explain the life cycle management approach.

11. Appendix B to Part 50--Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants, (Criterion) III, "Design Control," states:

Measures shall be established to assure that applicable regulatory requirements and the design basis, as defined in § 50.2 and as specified in the license application, for those structures, systems, and components to which this appendix applies are correctly translated into specifications, drawings, procedures, and instructions. These measures shall include provisions to assure that appropriate quality standards are specified and included in design documents and that deviations from such standards are controlled. Measures shall also be established for the selection and review for suitability of application of materials, parts, equipment, and processes that are essential to the safety-related functions of the structures, systems and components.

Measures shall be established for the identification and control of design interfaces and for coordination among participating design organizations. These measures shall include the establishment of procedures among participating design organizations for the review, approval, release, distribution, and revision of documents involving design interfaces.

The design control measures shall provide for verifying or checking the adequacy of design, such as by the performance of design reviews, by the use of alternate or simplified calculational methods, or by the performance of a suitable testing program. The verifying or checking process shall be performed by individuals or groups other than those who performed the original design, but who may be from the same organization. Where a test program is used to verify the adequacy of a specific design feature in lieu of other verifying or checking processes, it shall include suitable qualifications testing of a prototype unit under the most adverse design conditions. Design control measures shall be applied to items such as the following: reactor physics, stress, thermal, hydraulic, and accident analyses; compatibility of materials; accessibility for in-service inspection, maintenance, and repair; and delineation of acceptance criteria for inspections and tests. Design changes, including field changes, shall be subject to design control measures commensurate with those applied to the original design and be approved by the organization that performed the original design unless the applicant designates another responsible organization.

10 CFR 73.54(d)(3) requires the licensee to ensure that modifications to assets within the scope of the Rule are evaluated before implementation. 10 CFR 73.54(f) requires the licensee to develop and maintain written policies and implementing procedures to implement the cyber security plan. 10 CFR 73.54(g) requires the licensee to review the cyber security program as a component of the physical security program in accordance with the requirements of 10 CFR 73.55(m), including the periodicity requirements. Section 4.4.1, "Configuration Management and Change Control," of the [Site/Licensee] Cyber Security Plan states that "CDA [critical digital asset] cyber security and configuration management documentation is updated or created for safety and security systems when such documentation was either unavailable or non-existent (e.g., due to the age of the digital asset, lack of support from the vendor/contractor)." Explain how CDA cyber security and configuration management documentation is updated or created for emergency preparedness and support systems when such documentation was either unavailable or non-existent. Explain which safety-related systems lack current configuration management documentation or have no configuration management documentation.

12. 10 CFR 73.54(d)(3) requires the licensee to ensure that modifications to assets within the scope of the Rule are evaluated before implementation. Section 4.4.2, "Cyber Security Impact Analysis of Changes and Environment," of the [Site/Licensee] Cyber Security Plan states "These impact analyses are performed as part of the change approval process to assess the impacts of the changes on the cyber security posture of CDAs and systems that can affect SSEP [safety, security, and emergency preparedness] functions." Explain whether issues identified during these impact analyses are entered into the corrective action program.

13. 10 CFR 73.54(g) requires the licensee to review the cyber security program as a component of the physical security program in accordance with the requirements of 10 CFR 73.55(m), including the periodicity requirements. 10 CFR 73.54(c)(1) requires the licensee to implement security controls to protect the assets identified by paragraph (b)(1) from cyber attacks. Section 4.4.3, "Ongoing Assessment of Cyber Security Controls," of the [Site/Licensee] Cyber Security Plan states "The assessment process verifies the status of these cyber security controls [at least every 24 months] or in accordance with the specific requirements for utilized cyber security controls as described in Appendices D and E of NEI 08-09, Revision 3, whichever is more frequent. For CDAs [critical digital assets] in the site configuration management program, this validation may be performed through a verification of the integrity of the configuration documentation for CDAs." Explain how the effectiveness of each security control is assessed and how the validation process is conducted.

14. 10 CFR 73.54(b)(2) requires the licensee to establish, implement, and maintain a cyber security program for the protection of the assets within the scope of the Rule. 10 CFR 73.54(d)(2) requires the licensee to evaluate and manage cyber risk. Section 4.4.3.1, "Effectiveness Analysis," of the [Site/Licensee] Cyber Security Plan states "The effectiveness and efficiency of the cyber security program and the cyber security controls in Appendices D and E of NEI 08-09, Revision 3, are monitored to confirm that the cyber security controls are implemented correctly, operating as intended, and

achieving the desired outcome.” Explain what is meant by “achieving the desired outcome.”

15. 10 CFR 73.54(b)(2) requires the licensee to establish, implement, and maintain a cyber security program for the protection of the assets within the scope of the Rule. 10 CFR 73.54(d)(2) requires the licensee to evaluate and manage cyber risk. Section 4.4.3.1, “Effectiveness Analysis,” of the [Site/Licensee] Cyber Security Plan states “These measures:

- a. provide insight for improving performance of the Cyber Security Program
- b. assist in determining the effectiveness of cyber security controls in Appendices D and E of NEI 08-09, Revision 3
- c. assist in ascertaining whether specific cyber security controls are functioning and are helping facilitate corrective action prioritization
- d. require using the Cyber Security Program activities data with the data obtained from automated monitoring and evaluation tools in a manner that can be tied to cyber security control implementation”

Explain whether problems identified during these analyses are entered into the [Site/Licensee] corrective action program.

16. 10 CFR 73.54(g) requires the licensee to review the cyber security program as a component of the physical security program in accordance with the requirements of 10 CFR 73.55(m), including the periodicity requirements. 10 CFR 73.55(m) states:

“Security program reviews. (1) As a minimum the licensee shall review each element of the physical protection program at least every 24 months. Reviews shall be conducted:

(i) Within 12 months following initial implementation of the physical protection program or a change to personnel, procedures, equipment, or facilities that potentially could adversely affect security.

(ii) As necessary based upon site-specific analyses, assessments, or other performance indicators.

(iii) By individuals independent of those personnel responsible for program management and any individual who has direct responsibility for implementing the onsite physical protection program.

(2) Reviews of the security program must include, but not be limited to, an audit of the effectiveness of the physical security program, security plans, implementing procedures, cyber security programs, safety/security interface activities, the testing, maintenance, and calibration program, and response commitments by local, State, and Federal law enforcement authorities.

(3) The results and recommendations of the onsite physical protection program reviews, management's findings regarding program effectiveness, and any actions taken as a result of recommendations from prior program reviews, must

be documented in a report to the licensee's plant manager and to corporate management at least one level higher than that having responsibility for day-to-day plant operation. These reports must be maintained in an auditable form, available for inspection.

(4) Findings from onsite physical protection program reviews must be entered into the site corrective action program.”

10 CFR 73.54(b)(2) requires the licensee to establish, implement, and maintain a cyber security program for the protection of the assets within the scope of the Rule.

10 CFR 73.54(d)(2) requires the licensee to evaluate and manage cyber risk. Section 4.4.3.1, “Effectiveness Analysis,” of the [Site/Licensee] Cyber Security Plan (CSP) states, “The effectiveness of these cyber security controls is verified every 24 months or in accordance with the specific requirements for employed cyber security controls as described in Appendices D and E of NEI 08-09, Revision 3, whichever is more frequent.” Explain how the CSP will ensure compliance with the periodicity requirements of 10 CFR 73.55(m).

17. 10 CFR 73.54(b)(2) requires the licensee to establish, implement, and maintain a cyber security program for the protection of the assets within the scope of the Rule.

10 CFR 73.54(d)(2) requires the licensee to evaluate and manage cyber risk. Section 4.4.3.1, “Effectiveness Analysis,” of the [Site/Licensee] Cyber Security Plan describes the monitoring of cyber security controls. Explain the process for review of maintenance and repair records of critical digital asset (CDA) components to ensure that CDAs are maintained according to recommendations provided by the manufacturers and any deviations are justified and documented.

18. 10 CFR 73.54(b)(2) requires the licensee to establish, implement, and maintain a cyber security program for the protection of the assets within the scope of the Rule.

10 CFR 73.54(d)(2) requires the licensee to evaluate and manage cyber risk. Section 4.4.3.1, “Effectiveness Analysis,” of the [Site/Licensee] Cyber Security Plan (CSP) states “The effectiveness criteria are established and the bases documented for established thresholds. The above insights are shared with cyber security decision makers to improve the cyber security at the facility.” Describe the effectiveness criteria and thresholds including the bases.

19. 10 CFR 73.54(b)(2) requires the licensee to establish, implement, and maintain a cyber security program for the protection of the assets within the scope of the Rule.

10 CFR 73.54(d)(2) requires the licensee to evaluate and manage cyber risk. Section 4.4.3.2, “Vulnerability Scans,” of the [Site/Licensee] Cyber Security Plan (CSP) states “When new vulnerabilities that could affect the cyber security posture of CDAs [critical digital assets] are identified, testing will be performed on an off-line system where possible and where scanning is deemed necessary.” Explain how the off-line test beds or vendor-maintained environments are as realistic as possible.

20. 10 CFR 73.54(e)(2) requires the licensee’s cyber security program to include measures for incident response and recovery for cyber attacks. Section 4.6, “Attack and

Mitigation Incident Response,” of the [Site/Licensee] Cyber Security Plan states, “Measures necessary to deny, deter, or detect cyber attacks are implemented by network protective devices and align with the Defensive Strategy.” Security features integrated into critical digital assets (CDAs) can be used to deny, detect, and deter cyber attacks. Explain how these CDA security features will be used to deny, detect, and deter cyber attacks.

21. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR 73.1. 10 CFR 73.54(e)(2) requires the licensee’s cyber security program to include measures for incident response and recovery from cyber attacks. Section 4.6, “Attack and Mitigation Incident Response,” of the [Site/Licensee] Cyber Security Plan (CSP) states “[Policies, Procedures, Programs] document cyber security controls to deny, deter, and detect adverse threats and conditions to CDAs [Critical Digital Assets] that may be susceptible to remote electronic attacks which exploit system vulnerabilities.” Explain how the [Site/Licensee] will deny, deter, and detect threats and conditions to CDAs that may be susceptible to cyber attacks which are not remote (e.g. on-site).

22. 10 CFR 73.54(e)(2) requires the licensee’s cyber security program to include measures for incident response and recovery for cyber attacks. Section 4.6, “Attack and Mitigation Incident Response,” of the [Site/Licensee] Cyber Security Plan (CSP) states, “Cyber Attacks/Incidents are evaluated, tracked, and managed by the Incident Response and Corrective Action Programs [CAP].” Explain how [Site/Licensee] cyber attacks/incidents will be documented.

23. 10 CFR 73.54(e)(2) requires the licensee’s cyber security program to include measures for incident response and recovery from cyber attacks. Section 4.6, “Attack and Mitigation Incident Response,” of the [Site/Licensee] Cyber Security Plan (CSP) states, “Cyber security attack containment activities are directed by site procedures. These measures include but are not limited to:

- a. Isolate the affected CDA [critical digital asset] with approval by [Shift Superintendent Operations], if possible; and
- b. Verify surrounding networks and support systems are not contaminated.”

Explain how [Site/Licensee] determines what constitutes “cyber security attack containment activities.” Or the criteria used to determine when containment activities are to be instituted.

24. 10 CFR 73.54(e)(2) requires the licensee’s cyber security program to include measures for incident response and recovery from cyber attacks. Section 4.6, “Attack and Mitigation Incident Response,” of the [Site/Licensee] Cyber Security Plan states “Recovery activities include but are not limited to functional recovery test, restoration to operational state, verification of operability, and return to service. Systems, networks, and/or equipment affected by cyber attacks are restored and returned to operation as directed by site procedures. Post incident analysis is conducted in accordance with site

Corrective Action Program [CAP] procedures.” Explain how the [Site/Licensee] will perform security and requirements testing as part of the recovery activities to ensure the security features are operating properly. Explain how post incident corrective measures ensure that restoration activities do not return the asset to its original, exploitable state. Explain how the [Site/Licensee] ensures that vulnerabilities are not built into the restore point(s).

25. 10 CFR 73.54(e)(2) requires the licensee’s cyber security program to include measures for incident response and recovery from cyber attacks. Section 4.7, “Cyber Security Contingency Plan,” of the [Site/Licensee] Cyber Security Plan (CSP) provides information about the [Site/Licensee] cyber security contingency plan. Explain how the licensee cyber security contingency plan includes the following:

- a. a formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among [Site/Licensee] entities, and compliance
- b. formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls

Explain the process for [Site/Licensee] updating the contingency planning policy and procedures and, where necessary, related policies and procedures for other programs.

26. 10 CFR 73.54(d)(2) requires the licensee to evaluate and manage cyber risks. Section 4.9, “Evaluate and Manage Cyber Risk,” states “Cyber risk is evaluated and managed utilizing site programs and procedures outlined in the Performance Requirements in Section 2.2. Refer to Appendix E of NEI 08-09, Revision 3, which describes how the following cyber security controls are used to evaluate and manage risk.” The security controls referenced in Section 4.9 are not included in Appendices D and E of NEI 08-09, Rev. 3. Explain how [Site/Licensee] will include these security controls within the appropriate appendix.

27. 10 CFR 73.54(d)(1) requires that licensees “[e]nsure that appropriate facility personnel, including contractors, are aware of cyber security requirements and receive the training necessary to perform their assigned duties and responsibilities.” The [Site/Licensee] Cyber Security Plan (CSP) Section 4.11, Roles and Responsibilities, indicates the Cyber Security Incident Response Team (CSIRT) will respond to a credible cyber attack. Explain how the CSIRT will determine which attacks are credible.

28. 10 CFR 73.54(g) requires the licensee to review the cyber security program as a component of the physical security program in accordance with the requirements of 10 CFR 73.55(m), including the periodicity requirements. 10 CFR 73.55(m) states

“Security program reviews. (1) As a minimum the licensee shall review each element of the physical protection program at least every 24 months. Reviews shall be conducted:

(i) Within 12 months following initial implementation of the physical protection program or a change to personnel, procedures, equipment, or facilities that potentially could adversely affect security.

(ii) As necessary based upon site-specific analyses, assessments, or other performance indicators.

(iii) By individuals independent of those personnel responsible for program management and any individual who has direct responsibility for implementing the onsite physical protection program.

(2) Reviews of the security program must include, but not be limited to, an audit of the effectiveness of the physical security program, security plans, implementing procedures, cyber security programs, safety/security interface activities, the testing, maintenance, and calibration program, and response commitments by local, State, and Federal law enforcement authorities.

(3) The results and recommendations of the onsite physical protection program reviews, management's findings regarding program effectiveness, and any actions taken as a result of recommendations from prior program reviews, must be documented in a report to the licensee's plant manager and to corporate management at least one level higher than that having responsibility for day-to-day plant operation. These reports must be maintained in an auditable form, available for inspection.

(4) Findings from onsite physical protection program reviews must be entered into the site corrective action program."

Section 4.12, "Title," of the [Site/Licensee] Cyber Security Plan (CSP) does not provide an explicit commitment to implement each of the required reviews at the frequency specified in 10 CFR 73.55(m). Explain how the review processes required by 10 CFR 73.55(m) including those pertinent to results, recommendations and findings are addressed and committed to within the Cyber Security Program.

29. 10 CFR 73.54(h) requires the licensee to retain all records and supporting technical documentation required to satisfy the requirements of this section as a record until the Commission terminates the license for which the records were developed, and shall maintain superseded portions of these records for at least three (3) years after the record is superseded, unless otherwise specified by the Commission. Section 4.13, "Title," of the [Site/Licensee] Cyber Security Plan (CSP) does not explicitly describe which specific documents [Site/Licensee] intends to use to document access history and use to discover the source of cyber attacks affecting critical digital assets and safety, security and emergency planning functions. Explain how [Site/Licensee] will include this information.

30. 10 CFR 73.54 requires that "Each [Cyber Security Plan] submittal must include a proposed implementation schedule. Implementation of the licensee's cyber security program must be consistent with the approved schedule." The implementation schedule

provided with the [Site/Licensee] Cyber Security Plan (CSP) does not appear to be reasonable considering the following:

- a. The NRC 2002 Interim Compensatory Measures Order (EA-02-026), along with the associated implementing guidance, required that [Site/Licensee] identify all of [Site/Licensee]'s digital systems associated with Safety, Security, and Emergency Preparedness (SSEP) and institute appropriate protective measures.
- b. The NRC 2003 Design Basis Threat (DBT) Order (EA-03-086) added the cyber attack vector to the list of adversary characteristics that [Site/Licensee] must defend against with high assurance.
- c. The DBT Order also required [Site/Licensee] to revise the site-specific security plans (by 2004) to address all of the new adversary characteristics.
- d. [Site/Licensee]'s site-specific security plan includes cyber security program provisions for digital assets associated with SSEP functions.
- e. In 2005 the NRC endorsed the Nuclear Energy Institute's NEI 04-04 "Cyber Security Program for Nuclear Power Plants." It is the understanding of the NRC understanding from discussions with NEI that all power reactor licensees implemented an NEI 04-04 program by 2008. NEI 04-04 described cyber security program provisions for digital assets associated with SSEP functions.
- f. In 2007 the NRC finalized the DBT Rule (10 CFR 73.1) and the associated implementing guidance (Regulatory Guide 5.69) which describe the cyber attack threat. This Rule, in combination with 10 CFR 73.55(b), required power reactor licensees to protect against all DBT adversary characteristics.
- g. In 2008 NEI and several industry licensees responded to the Federal Energy Regulatory Commission's (FERC) proposed Order 706-B by indicating that FERC's cyber requirements were not needed because NEI 04-04 programs were in place at all power reactor sites.
- h. The North American Electric Reliability Corporation (NERC) 706-B Implementation Plan requires compliance with the CIP Reliability Standards by the later of the FERC effective date plus 18 months, or the NERC/NRC Memorandum of Understanding execution date plus 10 months. For requirements that are outage-dependent, the NERC Implementation Plan requires compliance with the Critical Infrastructure Protection Reliability Standards within 6 months after the completion of the first refueling outage that is at least 18 months following the FERC effective date.

Given the above, justify each date in the CSP implementation schedule provided, including interim milestones.

31. 10 CFR 73.54(c)(1) requires the cyber security program to implement security controls to protect critical digital assets from cyber attacks. Sections 4.4.3.1, "Effectiveness analysis," and 4.4.3.2 "Vulnerability Scans," describe effectiveness analysis and vulnerability scans. Will effectiveness analysis and vulnerability scans be performed at the time security controls are first implemented to provide high assurance they are operating as intended and producing the desired outcome, or only as part of periodic monitoring activities described in Sections 4.4.3.1 and 4.4.3.2?

32. 10 CFR 73.54(c)(1) requires the cyber security program to implement security controls to protect critical digital assets from cyber attacks. Section 4.5, "Addition and Modification of Assets" of the Cyber Security Plan (CSP) states that "The preferred approach for assessing new/modified [critical digital assets] CDAs is to use the assessment process described in Section 3.1 of this Plan. Alternately, a process that reviews and addresses Cyber Security Controls listed in Appendices D and E of NEI 08 09, Revision 3, may be used." Please explain what conditions warrant the use of the alternate assessment process as opposed to those outlined in Section 3.1, and provide greater detail as to how the alternative process mentioned in Section 4.5 provides the same level of assurance as the preferred approach.

33. 10 CFR 73.54(c)(1) requires the cyber security program to implement security controls to protect the assets identified by paragraph (b)(1) of 10 CFR 73.54 from cyber attacks. Section 4.5, "Addition and Modification of Assets," of the Cyber Security plan (CSP) states, "[Programs, Procedures, Processes] have been established, implemented, and maintained to control life cycle phase activity cyber security controls for [critical digital assets] CDAs. These [programs, procedures, processes] ensure that modifications to a CDA within the scope of 10 CFR 73.54 are evaluated before implementation to ensure that the cyber security performance objectives of 10 CFR 73.54(a)(1) are maintained and that acquired CDAs have cyber security requirements developed to achieve the site's cyber security program objectives." This statement addresses acquisition of new CDAs or modifications made to existing CDAs. Please clarify whether any assets that do not provide direct, or supporting, roles in the proper functioning of critical systems but are later reprogrammed (moved, reconfigured, or modified in any way) for use as a CDA are evaluated before implementation to ensure the security performance objectives of 10 CFR 73.54 are maintained.

34. 10 CFR 73.54(b)(1) requires the licensee to analyze digital computer and communications systems and networks and identify those assets that must be protected against cyber attacks. Section 2.1 states, "This Plan establishes a means to achieve high assurance that digital computer and communication systems and networks associated with the following functions (hereafter designated as Critical Digital Assets (CDAs)) are adequately protected against cyber attacks up to and including the Design Basis Threat (DBT) as described in § 73.1:

- a. Safety-related and important-to safety functions;
- b. Security functions;
- c. Emergency preparedness functions including offsite communications; and
- d. Support systems and equipment which if compromised, would adversely impact safety, security, or emergency preparedness functions."

However, Section 3.1.3 of the CSP of states that "[Critical systems] CSs are identified by conducting an initial consequence analysis of site systems, equipment, communication systems and networks determine those which, if compromised, exploited or were to fail, could impact the [Safety, security and emergency preparedness] SSEP functions of the nuclear facility without accounting for existing mitigating measures." Please explain whether the analysis conducted in Section 3.1.3 will include support systems and equipment which if compromised, would adversely impact SSEP functions.

35. 10 CFR 73.54(b)(1) requires the licensee to analyze digital computer and communications systems and networks and identify those assets that must be protected against cyber attacks. Section 4.4.3.2 states, "Electronic vulnerability scanning of [critical digital assets] CDAs is performed as required by specific guidance in the cyber security controls in Appendices D and E of NEI 08-09, Revision 3. When new vulnerabilities that could affect the cyber security posture of CDAs are identified, testing will be performed on an off-line system where possible and where scanning is deemed necessary." The criteria for when scanning activities will be "deemed necessary" is not clear. Please explain whether the phrase "deemed necessary" applies only to vulnerability scanning performed as part of testing activities. If not, provide the criteria for when electronic vulnerability scans will, and will not be, deemed necessary.

36. 10 CFR 73.54(b)(2) requires the licensee to establish, implement, and maintain a cyber security program for the protection of the critical digital assets. Section 2.2, "Performance Requirements" provides a list of performance based requirements for the CSP. The following clarifications are needed:

10 CFR 73.54(e)(2)(ii) states the cyber security plan must describe how the licensee will mitigate the consequences of cyber attacks. Section 2.2.2 states, "Ensure that the Program maintains the capability to detect, respond to, and recover from cyber attacks up to and including the design basis threat of radiological sabotage as stated in §73.1 at all times. (§ 73.55(b)(2)(i), § 73.54(e)(2)(i), and § 73.54(e)(2)(iv))." Clarify whether performance based requirements will include maintaining the capability to mitigate the consequences of cyber attacks as part of cyber attack response capabilities.

10 CFR 73.54(e)(2)(iii) states the cyber security plan must describe how the licensee will correct exploited vulnerabilities. Section 2.2.2 states, "Ensure that the Program maintains the capability to detect, respond to, and recover from cyber attacks up to and including the design basis threat of radiological sabotage as stated in §73.1 at all times. (§ 73.55(b)(2)(i), § 73.54(e)(2)(i), and § 73.54(e)(2)(iv))." Clarify whether performance based requirements will include maintaining the capability to correct exploited vulnerabilities as part of cyber attack recovery capabilities.

10 CFR 73.54(d)(1) states the licensee shall ensure appropriate facility personnel, including contractors, are aware of cyber security requirements and receive the training necessary to perform their assigned duties and responsibilities. Clarify whether performance based requirements will include training facility personnel, including contractors, to be aware of cyber security requirements training necessary to perform their assigned duties and responsibilities.

10 CFR 73.54(d)(3) states the licensee shall ensure that modifications to critical digital assets are evaluated before implementation to ensure that the cyber security performance objectives identified in paragraph (a)(1) of the Rule are maintained. Clarify whether performance based requirements will include evaluation of modifications to CDAs prior to implementation to achieve high assurance that digital computer and communications systems and networks are adequately protected against cyber attacks, up to and including the DBT.

## SECURITY CONTROL GENERIC QUESTIONS

37. 10 CFR 73.54(d)(2) requires the licensee to evaluate and manage cyber risks. The [SITE/LICENSEE] Cyber Security Plan (CSP) describes in multiple sections that the licensee will perform a “risk assessment.” For example, Appendix D, Section 1.3 states:

“Authorizes personnel access to privileged functions and security-relevant information consistent with the risk assessment established policies and procedures.”

However, the [SITE/LICENSEE] CSP does not describe what this risk assessment is, how it is performed, or how the results are used. This term is used throughout the CSP including:

Appendix D – 1.1  
Appendix D – 1.2  
Appendix D – 1.3  
Appendix D – 1.7,  
Appendix D – 1.10  
Appendix D – 1.17  
Appendix D – 1.18  
Appendix D – 2.2  
Appendix D – 2.5  
Appendix D – 2.6  
Appendix D – 2.8,  
Appendix D – 2.9,  
Appendix D – 3.7  
Appendix D – 3.15  
Appendix D – 4.1  
Appendix D – 4.3  
Appendix D – 5.2  
Appendix E – 1.5,  
Appendix E – 1.6  
Appendix E – 3.4  
Appendix E – 5.5  
Appendix E – 5.10,  
Appendix E – 6  
Appendix E – 7.3,  
Appendix E – 8.2  
Appendix E – 8.3,  
Appendix E – 8.5,  
Appendix E – 9.4  
Appendix E – 10.3  
Appendix E – 10.5  
Appendix E – 10.6  
Appendix E – 10.8  
Appendix E – 11.2  
Appendix E – 11.4,

How is the risk assessment performed and how are the results used?

38. 10 CFR 73.54(d)(2) requires the licensee to evaluate and manage cyber risks. The [SITE/LICENSEE] Cyber Security Plan (CSP) describes in multiple sections actions that occur “periodically.” For example in Appendix E, Section 3.6 of NEI 08-09, Revision 3 the CSP states:

“The correct operation of security functions of CDAs are verified and documented, periodically, upon startup and restart, upon command by a user with appropriate privilege, and when anomalies are discovered, where possible.”

However, the CSP does not provide the time spans for these “periods” nor does it describe how a risk assessment would produce these time spans. The same language is also used in other sections including:

Section 3.1  
Appendix D – 1.1  
Appendix D – 2  
Appendix D – 3.1  
Appendix D – 4.1  
Appendix D – 4.7  
Appendix E – 1.1  
Appendix E – 3.1  
Appendix E – 4.1  
Appendix E – 5.1  
Appendix E – 7.1  
Appendix E – 10.2  
Appendix E – 11.1

Specify the time spans for these “periods” stated. If the periodicity is not consistent with the periodicity described in NEI 03-12, describe the process by which the periodicities are determined.

39. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Appendix D, Section 1.2, “Account Management,” of the [SITE/LICENSEE] Cyber Security Plan (CSP) states:

“[SITE/LICENSEE] reviews critical digital asset accounts consistent with the access control list provided in the design control package, access control program, cyber security procedures and initiates required actions on critical digital asset accounts within a maximum time period as determined by the risk assessment.”

The purpose of reviewing accounts frequently is to eliminate unnecessary accounts, such as temporary, guest, default, and shared accounts. This minimizes the opportunity for an adversary to exploit such accounts. A review period for physical access is in 10 CFR 73.56(j), “Access to Vital Areas.” It requires licensees to update and re-approve vital area access lists at least every 31 days.

Describe how the frequency selection will provide the same level of protection as the frequency currently required by 10 CFR 73.56.

40. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR 73.1. The [SITE/LICENSEE] Cyber Security Plan, Appendix D, Section 1.2, "Account Management," does not provide criteria for ensuring that the principle of "least privilege" is applied to critical digital asset (CDA) accounts. Least privilege minimizes the potential for user abuse or misuse of his/her privileges to adversely impact CDAs or safety, security, or emergency preparedness (SSEP) functions. This strategy requires ensuring that access rights remain limited to only those necessary to perform an individual's current job function. The process control, cyber security, and IT industries support the principle of least privilege by using role-based assignment of user privileges. Clarify whether the [SITE/LICENSEE] uses role-based assignment of user privileges, or describe the process used to minimize the adverse impact to site's SSEP functions through management of user account privileges.

41. 10 CFR 73.54(c)(1) requires the licensee to implement security controls to protect the digital assets within the scope of the rule from cyber attacks. 10 CFR 73.54(c)(2) requires the licensee to apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks. 10 CFR 73.54(c)(3) requires the licensee to mitigate the adverse affects of cyber attacks. 10 CFR 73.54(e)(2) requires the licensee's Cyber Security Plan (CSP) to include description of how the licensee will:

- (i) Maintain the capability for timely detection and response to cyber attacks;
- (ii) Mitigate the consequences of cyber attacks;
- (iii) Correct exploited vulnerabilities; and
- (iv) Restore affected systems, networks, and/or equipment affected by cyber attacks.

10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR 73.1. Additionally, 10 CFR 73.54(c)(1) and 10 CFR 73.54(c)(4) require that the licensees' cyber security programs be designed to implement security controls to protect critical digital assets.

Appendix D, Section 1.4, "Information Flow Enforcement," of the [SITE/LICENSEE] Cyber Security Plan states that it "Maintains documentation that demonstrates the analysis and addressing of permissible and impermissible flow of information between critical digital assets, security boundary devices and boundaries and the required level of authorization to allow information flow as defined in the defensive strategy," and that it "Implements and documents information flow control enforcement using protected processing level as a basis for flow control decisions."

Effective information flow enforcement should be supported by at least the following:

- a. near-real time capabilities that detect, deter, prevent, and respond to unauthorized information flows as they occur;
- b. use of hardware mechanisms to enforce one-way data flow between defensive levels where critical digital assets are located; and
- c. implementation of controls to prevent traffic encryption from being used to block message content checking

Clarify and/or describe the process used by the [SITE/LICENSEE] to support information flow enforcement to detect, deter, prevent, and respond to unauthorized information flows in near-real time, enforce one-way data flow between defensive levels where critical digital assets are located, and prevent traffic encryption from being used to block message content checking.

42. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Additionally, 10 CFR 73.54(c)(1) and 10 CFR 73.54(c)(4) require that the licensees' cyber security programs be designed to implement security controls to protect digital assets from cyber attacks. Appendix D, Section 1.17, "Wireless Access Restrictions," of the [SITE/LICENSEE] Cyber Security Plan states that the cyber security program

"establishes usage restrictions and implementation guidance for wireless technologies," and "documents, justifies, authorizes, monitors, and controls wireless access to critical digital assets and ensures that the wireless access restrictions are consistent with defensive strategies developed through the risk assessment process"

Wireless communications technology is always subject to external interference and interception. Additionally, it is difficult to define the boundary of a device that use wireless communication technology and identify those devices that have a pathway to the device. Describe how and why usage restrictions and implementation guidance for wireless technologies ensure that security effectiveness is not adversely impacted. The explanation should include why and how the usage restrictions and implementation guidance for wireless technologies provide the same level of isolation between defensive levels as hard-wired technologies.

Note that any wireless device that provides a pathway to critical a digital asset (CDA) should itself be considered a CDA. In addition to other devices, equipment or systems connected to such wireless devices could be considered as CDAs. Clarify how protective measures are applied consistently within the same security level. The explanation should describe how the licensee determines what protective measures are applied to a CDA and why the measures are applied.

43. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Additionally, 10 CFR 73.54(c)(1) and (4) require that the licensees' cyber security programs be designed to implement security controls to protect the assets identified by paragraph (b)(1) from cyber attacks. Appendix D, Section 1.17, of [SITE/LICENSEE] Cyber Security Plan (CSP), "Wireless Access Restrictions," does not

address disabling the integral wireless capabilities of critical digital assets (CDAs) that will not be using those capabilities. When the wireless capabilities of CDAs are not disabled, they provide a pathway for cyber attack. If the [SITE/LICENSEE] disables the integral wireless capabilities of CDAs as part of their cyber security program, describe this in the CSP. If not, describe why leaving integral wireless capabilities enabled in CDAs would not provide pathways that an adversary could use to gain access.

44. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Additionally, 10 CFR 73.54(c)(1) and (4) require that the licensee's cyber security programs be designed to implement security controls to protect the assets identified by paragraph (b)(1) from cyber attacks. Appendix D, Section 1.17, "Wireless Access Restrictions," of the [SITE/LICENSEE] Cyber Security Plan, discusses conducting "scans for unauthorized wireless access and disabling access points if unauthorized access points are discovered." Describe the process by which the [SITE/LICENSEE] will determine the frequency of scans for unauthorized wireless devices.

45. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Additionally, 10 CFR 73.54(c)(1) and 10 CFR 73.54(c)(4) require that the licensee's cyber security program be designed to implement security controls to protect digital assets from cyber attacks. Appendix D, Section 1.19, of the [SITE/LICENSEE] Cyber Security Plan (CSP) describes "access control for portable and mobile devices." The last bullet states that the cyber security program:

"Enforces and documents mobile devices are used in one security level and mobile devices are not moved between security levels unless governed by the M&TE [Measuring & Test Equipment] program or equivalent."

Describe how and why the M&TE program ensures that security effectiveness is not adversely impacted by moving mobile devices between security levels. The explanation should include why and how the M&TE program provides the same level of isolation between security levels as the absence of the portable and mobile devices that move between security levels. Note that portable and mobile devices would provide pathways to critical digital assets (CDAs) if they are connected to them. Therefore, those portable and mobile devices should themselves be CDAs. In addition, other devices, equipment or systems connected to portable and mobile devices could be CDAs. Are protective measures applied consistently within the same defensive level? If so clarify this in the [SITE/LICENSEE] CSP. If not, describe how protective measures are applied to these CDAs. How has the MT&E program been augmented to provide high assurance that the mobile devices are secure?

46. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Appendix D, Section 1.22, of the [SITE/LICENSEE] Cyber Security Plan (CSP) describes the "Use of External Systems." It also states that the cyber security program:

"Establishes the terms and conditions to securely manage and restrict external system access from higher levels" and "establishes the terms and conditions to securely manage and restrict external system access to critical digital assets in the higher levels."

For the defensive architecture to protect critical digital assets (CDAs) effectively from cyber attacks, protective measures must be applied consistently within the same defensive level. Two-way communication between higher and lower defensive levels defeats the purposes of establishing defensive levels to isolate a network that includes CDAs from other networks.

Describe why and how the terms and conditions to securely manage and restrict external system access from higher levels would provide the same level of isolation between the higher level and other levels as prohibiting communications between the external systems and the CDAs located in the higher levels. Describe why and how the terms and conditions to securely manage and restrict external system access to CDAs in the higher levels would provide the same level of isolation between the higher level and other levels as prohibiting communications between the external systems and the CDAs located in the higher levels. If the external systems are connected to a CDA or a network to which a CDA is connected, the external systems should themselves be considered CDAs. Additionally, any assets connected to the external systems may be CDAs. Are protective measures applied consistently within the same security level? If so clarify this in the [SITE/LICENSEE] Cyber Security Plan. If not, describe what protective measures are applied to a CDA and why.

47. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR 73.1. The [SITE/LICENSEE] Cyber Security Plan (CSP) does not address how "Publicly Accessible Content Controls" reduce the possibility of sensitive information being made accessible to the public. One of the most commonly used strategies to aid in devising a cyber attack is to seek out sources of publicly accessible information. Effective management of publicly accessible information or content is essential to prevent sensitive information from being unintentionally (or intentionally) disclosed. It is essential to monitor, manage, and restrict the sensitive information that is provided to the public.

Describe in the CSP how the [SITE/LICENSEE] will manage and implement Publicly Accessible Content Controls to reduce the possibility of sensitive information being made accessible to the public.

48. 10 CFR 73.54(c)(1) requires the licensee to implement security controls to protect the digital assets within the scope of the rule from cyber attacks. 10 CFR 73.54(c)(2) requires the licensee to apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks. 10 CFR 73.54(c)(3) requires the licensee to mitigate the adverse affects of cyber attacks. 10 CFR 73.54(e)(2) requires the licensee's Cyber Security Plan (CSP) to include a description of how the licensee will:

- (i) Maintain the capability for timely detection and response to cyber attacks;
- (ii) Mitigate the consequences of cyber attacks;
- (iii) Correct exploited vulnerabilities; and
- (iv) Restore affected systems, networks, and/or equipment affected by cyber attacks.

Appendix D, Section 2.2, "Auditable Events," of the CSP states that the auditable events control "Configures critical digital assets so that auditable events to support after-the-fact investigations of security incidents."

This sentence appears to missing some words. Please clarify how configuring critical digital assets (CDAs) so that auditable events are preserved and adequate to support after-the-fact investigations of security incidents, Also please clarify how the [SITE/LICENSEE]'s cyber security program will ensure the collection, storage, and preservation of auditable events for CDAs.

49. 10 CFR 73.54(c)(1) requires the licensee to implement security controls to protect the digital assets within the scope of the rule from cyber attacks. 10 CFR 73.54(c)(2) requires the licensee to apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks. 10 CFR 73.54(e)(2) requires the licensee's Cyber Security Plan (CSP) to include a description of how the licensee will:

- (i) Maintain the capability for timely detection and response to cyber attacks;
- (ii) Mitigate the consequences of cyber attacks;
- (iii) Correct exploited vulnerabilities; and
- (iv) Restore affected systems, networks, and/or equipment affected by cyber attacks.

Recording privileged functions in the list of events to be audited by the critical digital assets is essential for identifying the mechanisms used, and vulnerabilities exploited, in both attempted and successful cyber attacks. However, Appendix D, Section 2.2, "Auditable Events," of the [SITE/LICENSEE]'s CSP does not include the collection of such information.

Describe the process by which [SITE/LICENSEE]'s cyber security program will enable an audit trail for programmatic execution of privileged functions and how associated audit records will be correlated with the user who initiated the program or script.

50. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks. Additionally, 10 CFR 73.54(c)(1) and 10 CFR 73.54(c)(4) require that the licensee's cyber security program be designed to implement security controls to protect the digital assets identified by paragraph 10 CFR 75.54(b)(1) from cyber attacks. 10 CFR 73.54(e)(2) requires the licensee's Cyber Security Plan (CSP) to include a description of how the licensee will:

- (i) Maintain the capability for timely detection and response to cyber attacks;
- (ii) Mitigate the consequences of cyber attacks;
- (iii) Correct exploited vulnerabilities; and
- (iv) Restore affected systems, networks, and/or equipment affected by cyber attacks.

Appendix D, Section 2.8, "Time Stamps," of the CSP states "This technical cyber security control ensures that critical digital assets use internal system clocks to generate time stamps for audit records as identified by the critical digital asset risk assessment." Since internal system clocks drift, high assurance of synchronized time stamps can not be achieved by their use.

How does [SITE/LICENSEE] ensure that the method(s) selected for such time synchronization do not introduce a vulnerability to cyber attack and common-mode failure? If time synchronization cannot be applied to a CDA, how does [SITE/LICENSEE] implement alternative controls?

51. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks, up to and including the design basis threat. Appendix D, Section 3.1, of the [SITE/LICENSEE] Cyber Security Plan describes "CDA, System and Communications Protection Policy and Procedures" and states that

"This Technical cyber security control ensures development, dissemination, and periodic reviews and updates of..."

Describe the process by which [SITE/LICENSEE] determines the periodicity of and criteria for this review.

52. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR 73.1. Additionally, 10 CFR 73.54(c)(1) and 10 CFR 73.54(c)(4) require that the licensees' cyber security program be designed to implement security controls to protect digital assets from cyber attacks. Appendix D, Section 3.4, of the [SITE/LICENSEE] Cyber Security Plan (CSP) describes "denial of service (DoS) protection" and states that this technical control "Configures Critical Digital Assets (CDA) to protect against or limit the effects of denial of service attacks." This section further states that this technical control "Configures CDAs to manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding-types of denial-of-service attacks."

The NRC staff noted that Appendix D, Section 3.4 of the CSP does not address “saturation type” denial of service (DoS) attacks. DoS attacks generally involve consuming or blocking the use of a necessary resource such as network bandwidth, memory, bulk (disk) storage or central processing unit power. It can also involve overwhelming key system components and applications by “saturating” them with large numbers of concurrent, or rapid sequential, service requests (i.e., the typical way that websites are attacked).

Clarify how the [SITE/LICENSEE]’s cyber security program protects against, or limits the effects of DoS attacks including “saturation” types of DoS attacks.

53. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Appendix D, Section 3.15, “Secure Name/Address Resolution Service (Recursive or Caching)” of the [SITE/LICENSEE] Cyber Security Plan states that the security control:

“Configures the systems that serve name/address resolution service for critical digital assets to perform data origin authentication and data integrity verification on the resolution response they receive from authoritative sources when requested by critical digital assets as identified by the risk assessment.”

Implementation of the control ensures that name/address resolution messages that are received must be authenticated and verified irrespective of whether they are specifically requested or not. If requested and unrequested messages are not both authenticated and verified, an adversary can exploit name/address mapping so that message traffic will go to unauthorized destinations. This type of attack is called “DNS [domain name system] cache poisoning.” Clarify how the [SITE/LICENSEE]’s cyber security program will include authentication and verification of both types of messages, or describe the process by which [SITE/LICENSEE] will protect against DNS cache poisoning.

54. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Appendix D, Section 3.21, “Abstraction Techniques,” of [SITE/LICENSEE]’s Cyber Security Plan describes the use of abstraction techniques to deploy a diverse set of operating systems and applications. Describe the process by which [SITE/LICENSEE] employs abstraction techniques (e.g., virtualization) to create effective diversity, particularly if the underlying critical digital asset hardware platform and base hypervisor software are actually homogeneous?

55. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks. A basic cyber security control is to design systems to fail in a known and desirable state to minimize the adverse impact the system failure has on other functions (i.e., preventing a loss of confidentiality, integrity, or availability). This design principle is particularly important for critical digital assets (CDAs) which by definition are associated with site safety, security, and emergency preparedness (SSEP) functions. The

[SITE/LICENSEE] Cyber Security Plan does not address this control. Describe how the licensee's cyber security program addresses CDA failures and compromises to (1) minimize the adverse impact to the site's SSEP functions and (2) prevent a loss of CDA confidentiality, integrity, or availability.

56. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Appendix D, Section 4.1, "Identification and Authentication Policies and Procedures" of the [SITE/LICENSEE] Cyber Security Plan (CSP) states that the authentication policy and procedures will "uniquely identify users," and will permit "verifying the identity of users." The CSP does not address the ability to uniquely identify processes acting on behalf of a user, in addition to the user himself/herself.

Clarify that Appendix D, Section 4.1, of the CSP provides controls for auditing and identifying processes running on behalf of a user, or describe how the cyber security program addresses and provides for the user identification and activity auditing of processes running on behalf of a user.

57. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Appendix D, Section 4.6, "Identifier Management," of the [SITE/LICENSEE] Cyber Security Plan states that user identifiers will be disabled after a "defined time period of inactivity." Explain the process by which the maximum defined period of inactivity is determined, and, if appropriate, the actual time period established.

58. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Additionally, 10 CFR 73.54(c)(1) and 10 CFR 73.54(c)(4) require that the licensee's cyber security program be designed to implement security controls to protect digital assets. Appendix D, Section 5.1, "Removal of Unnecessary Services and Programs," of the [SITE/LICENSEE] Cyber Security Plan (CSP) addresses a range of "hardening" steps that will be applied to critical digital assets (CDAs). The NRC staff notes that the CSP does not address the elimination or disabling of device drivers for unused peripherals and unused removable media support. Clarify if the removal of unnecessary services and programs includes the elimination or disabling of device drivers for unused peripherals and unused removable media support. If not, describe how device drivers for unused peripherals and unused removable media support are addressed in the CSP to prevent an adversary from exploiting them.

59. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks. 10 CFR 73.54(c)(2) require that the licensees' cyber security program must be designed apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks. Finally, 10 CFR 73.54(e)(2) requires that the cyber security plan (CSP) must include measures for incident response and recovery from cyber attacks. Appendix D, Section 5.2, of the [SITE/LICENSEE] CSP states:

“Configure host intrusion detection system [HIDS] to include attributes such as: static file names, dynamic file name patterns, system and user accounts, execution of unauthorized code, host utilization, and process permissions to configure the HIDS to meet the security requirements as identified by the risk determination.”

Please state whether HIDS are configured to detect cyber attacks up to and including the DBT.

60. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Additionally, 10 CFR 73.54(c)(1) and 10 CFR 73.54(c)(4) require that the licensee’s cyber security program must be designed to implement security controls to protect the digital from cyber attacks and to ensure that the functions of protected digital assets are not adversely impacted due to cyber attacks. Appendix E, Section 1.6, “Media Sanitation and Disposal,” of the [SITE/LICENSEE] cyber security plan discusses that methods are periodically tested to verify proper functioning. Please describe how the period for testing is determined.

61. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks. Additionally, 10 CFR 73.54(c)(1) and 10 CFR 73.54(c)(4) require that the licensee’s cyber security program be designed to implement security controls to protect the digital assets from cyber attacks and to ensure that the functions of protected digital assets are not adversely impacted due to cyber attacks. Appendix E, Section 3.2, “Flaw Remediation” of the [SITE/LICENSEE] cyber security plan (CSP) discusses “flaw remediation.” The [SITE/LICENSEE]’s CSP indicates that software updates to correct flaws following the configuration management process. The [SITE/LICENSEE] CSP is not clear whether the configuration management process will include testing to verify that the updates actually correct the targeted flaw/vulnerability. Please describe how the [SITE/LICENSEE]’s CSP will include testing of a critical digital asset to verify that a flaw has been eliminated before the critical digital asset is returned to operation.

62. 10 CFR 73.54(a)(1) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Additionally, 10 CFR 73.54(c)(1) and 10 CFR 73.54(c)(4) require that the licensee’s cyber security program be designed to implement security controls to protect the critical digital assets (CDA) from cyber attacks and to ensure that the functions of digital assets are not adversely impacted due to cyber attacks. Section E.3.3, “Malicious Code Protection,” of the [SITE/LICENSEE] Cyber Security Plan (CSP) states:

“Malicious code protection software products from multiple vendors are documented and employed as part of defense-in-depth, and the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information systems are addressed.”

If the information systems include critical digital assets, please clarify this.

Appendix E, Section 3.4, "Monitoring Tools and Techniques" of the [SITE/LICENSEE] Cyber Security Plan (CSP) discusses monitoring CDA incidents. To ensure that intrusion detection and prevention tools operate properly, they need to be tested periodically. Please confirm [SITE/LICENSEE] tests intrusion detection and prevention systems to ensure they operate properly. Also specify the frequency of the tests and the basis for the frequency.

63. 10 CFR 73.54 (a) requires the licensee provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Appendix E, Section 3.7, "Software and Information Integrity" of the [SITE/LICENSEE] Cyber Security Plan (CSP) states:

"Reassessing and documenting the integrity, operation and functions of software and information by performing regular integrity, operation and functional scans"

Although the CSP states that the scans will be regular, it does not describe what this period is, does not include any method of determining this period, and unlike other sections of the CSP where a period or interval is determined using a "risk assessment" process, there is no such commitment. Please provide the frequency at which regular integrity, operational, and functional scans will occur. Additionally, describe why the defined period for performing these scans will provide high assurance that the integrity of the critical digital assets has been maintained.

64. 10 CFR 73.54(a) requires the licensee provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Appendix E, Section 3.8, "Information Input Restrictions" of the [SITE/LICENSEE] Cyber Security Plan (CSP) states:

"Checking information for accuracy, completeness, validity, and authenticity as close to the point of origin as possible. Rules for checking the valid syntax of critical digital asset inputs (e.g., character set, length, numerical range, acceptable values) are documented and in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are pre-screened to prevent the content from being interpreted as commands. The extent to which the critical digital asset is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements."

Although the licensee has committed to perform this checking, the CSP states that it will only be done to the *"extent to which the CDA is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements."* However, the CSP does not describe what the policy is, nor what the operational requirements are, how they will be determined or how they will relate to the security requirements of this plan, this control, and the rule.

Describe what organizational policies and operational requirements will be considered in this process and how they will result in a suitably secure level of input checking to ensure critical digital asset cyber security.

65. 10 CFR 73.54(a) requires the licensee provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Appendix E, Section 8.1, "Contingency Plan," of the [SITE/LICENSEE]'s Cyber Security Plan (CSP) states:

"This security control consists of:

- a. Implementing a cyber security contingency plan to maintain the safety, security and emergency preparedness functions by developing and disseminating roles, responsibilities, assigned individuals with contact information, and activities associated with restoring CDAs after a disruption or failure.
- b. Coordinating contingency plan development with organizations responsible for related plans (e.g., Emergency Plan, Physical Security Plan) and requirements (e.g., Technical Specifications)."

Please describe how the CSP addresses deploying critical digital assets (CDA) such that, in the event of a loss of processing within a CDA or a loss of communication with operational facilities, CDA will execute predetermined actions.

66. 10 CFR 73.54(c)(1) requires the licensee to implement security controls to protect critical digital assets from cyber attacks. Appendix E, Section 9.2, "Awareness Training," of the [SITE/LICENSEE] Cyber Security Plan states:

"Loss off signal from control devices"

The word "off" in this phrase appears to be a typographical error. If this is a typographical error, correct it. If this is not an error, clarify the meaning of this paragraph.

67. 10 CFR 73.54(d)(1) requires the licensee to ensure that appropriate facility personnel, including contractors, are aware of cyber security requirements and receive the training necessary to perform their assigned duties and responsibilities. Appendix E, Section 9.3, "Technical Training," of the [SITE/LICENSEE] Cyber Security Plan (CSP) states:

"This security control further consists of establishing, implementing and documenting requirements to:

- a. Provide cyber security-related technical training to individuals:
- b. Before authorizing access to CDAs or performing assigned duties, and
- c. When required by policy or procedure changes and plant modifications, and
- d. At a licensee-defined interval, to mitigate risk and to ensure personnel maintain competency."

Although the CSP contains a commitment to provide technical training, it does not specify the interval for this training. If the [SITE/LICENSEE]'s training interval is greater than annual, describe this in the CSP. If not, describe the method used to determine the training interval and how it provides high assurance that technical skills and

competencies for personnel performing, verifying, and managing activities within the scope of the cyber security program are maintained.

68. 10 CFR 73.54(e)(1) requires that the licensee to describe how the requirements of the rule will be implemented and must account for the site-specific conditions that affect implementation. Appendix E, Section 10.3, of the [SITE/LICENSEE] Cyber Security Plan (CSP) describes "Baseline Configuration." A baseline configuration establishes a full detailed accounting of the settings configuration and components of a device. A comprehensive baseline configuration documentation set should include the following:

- a. a current list of all components (for example, hardware and software),
- b. interface characteristics,
- c. security requirements and the nature of the information communicated,
- d. configuration of peripherals,
- e. version releases of current software
- f. switch settings of machine components

Documentation management for baseline configurations includes:

- a. a log of configuration changes made,
- b. the name of the person who implemented the change,
- c. the date of the change,
- d. the purpose of the change,
- e. any observations made during the course of the change.

Such information is a necessary part of a cyber security program. Additionally, because some support systems and security systems within the scope of the 10 CFR 73.54 may not be covered by the [SITE/LICENSEE]'s current configuration management program, the CSP needs to include the items above. Please clarify that critical digital assets within the scope of the CSP are captured, documented and maintained within the configuration management program,

69. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. Appendix E, Section 11.2, "Supply Chain Protection," of the [SITE/LICENSEE] Cyber Security Plan (CSP) states:

"This security control protects against supply chain threats by employing an organization-defined list of measures to protect against supply chain threats to maintain the integrity of the critical digital assets that are purchased.

Although the CSP states that the licensee protects against supply chain threats, it does not clarify what measures the [SITE/LICENSEE] will use to protect against these threats. Please describe how the [SITE/LICENSEE] will protect the integrity of the supply chain.

70. 10 CFR 73.54 (a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against

cyber attacks. Appendix E, Section 12, "Evaluate and Manage Cyber Risk" of the [SITE/LICENSEE] Cyber Security Plan (CSP) states:

"Scan for vulnerabilities in the [critical digital assets] CDAs at a maximum regular interval and randomly as defined by the risk determination and as necessary when new vulnerabilities affecting the CDAs are identified and reported"

Regular vulnerability scans are critical to preventing cyber attacks. Although the CSP states that the vulnerability scans will occur at regular intervals and randomly as defined by the risk determination, the CSP does not define this risk determination process or how the results will be used.

Describe how the risk assessment process will lead to establishing time periods for scanning for vulnerabilities that will provide high assurance that the CDAs remain protected from new cyber security threats.

If the [SITE/LICENSEE]'s CSP includes the ability to compare the results of vulnerability scans conducted over time, clarify this in the cyber security plan. If not, describe how the licensee's CSP will manage the security controls, flaw remediation activities, and vulnerability management processes to protect critical digital assets from new vulnerabilities and the ever changing capabilities of cyber attackers.

If the [SITE/LICENSEE]'s CSP includes a vulnerability scanning process that supports a comprehensive range of attack modalities and CDA platforms, clarify this in the cyber security plan. If not, describe how the employed vulnerability scans will provide high assurance that CDAs are protected up to the DBT. Also please explain how vulnerability scans are conducted and how the cyber security program uses the results of vulnerability scans.

71. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are protected against cyber attacks. Appendix E, Section 3.5 "Security Alerts and Advisories" of the [SITE/LICENSEE] Cyber Security Plan states:

"...Based on plant and business operational requirements, independently evaluating and determining the need, severity, methods and time frames for implementing security directives consistent with the cyber security controls for the critical digital asset..."

However, the plant and business operational requirements may not be consistent with the security requirements. Please explain how cyber security considerations are factored into the determination of the need, severity, methods and time frames for implementing security directives.

72. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks. 10 CFR 73.54(c)(1) and (4) require that the licensee's cyber security program be designed to implement security controls to protect digital assets from cyber attacks and to ensure that the functions of protected assets are not adversely impacted

due to cyber attacks. Additionally, 10 CFR 73.54(c)(2) requires licenses to ensure the capability to respond to cyber attacks, and 10 CFR 73.54(e)(2) states that the plan must include measures for incident response and recovery from cyber attack.

A critical element of an incident response is the development, implementation, and maintenance of an incident response plan and all its associated components. Although the [SITE/LICENSEE]'s Cyber Security Plan (CSP) describes some aspects of incident response and attack mitigation, and also includes a specific commitment to develop a contingency plan, the CSP does not commit the [SITE/LICENSEE] to develop a cyber incident and attack response plan. Please describe whether the licensee will develop a cyber incident and attack response plan to comply with the requirements of the rule. If not, why not?

73. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks. Additionally, 10 CFR 73.54(c)(1) and (4) require that the licensee's cyber security program be designed to implement security controls to protect digital assets cyber attacks and to ensure that the functions of protected assets are not adversely impacted due to cyber attacks. The [SITE/LICENSEE] Cyber Security Plan (CSP), Appendix E, Section 10.6, "Access Restrictions for Change," states:

"Employs automated mechanisms to enforce access restrictions and to support subsequent audits of enforcement actions."

The intent of automated mechanisms is to (1) detect and prevent unauthorized changes, (2) enforce access restrictions, and (3) to support subsequent audits of enforcement actions. However, the CSP does not appear to contain a commitment to detect and prevent unauthorized changes. For example, cyber attacks might result in a change to the configuration of a critical digital asset without the change going through the configuration management or authentication processes (a virus for example); using automated mechanisms.

If the use of the "automated mechanisms" in the sentence above includes using automated mechanisms to detect unauthorized changes to critical digital assets, clarify this in the CSP. If not, describe how such unauthorized changes to critical digital assets would be detected by automated mechanisms.

74. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are adequately protected against cyber attacks. 10 CFR 73.54(c)(1) and (4) require that the licensee's cyber security program be designed to implement security controls to protect the assets identified by paragraph (b)(1) from cyber attacks and to ensure that the functions of protected assets identified by paragraph (b)(1) are not adversely impacted due to cyber attacks. Additionally, 10 CFR 73.54(c)(2) requires the licensee to maintain the capability to recover from cyber attacks.

Appendix E, Section 8.2, "Contingency Plan Testing," of the [SITE/LICENSEE] Cyber Security Plan (CSP) appears to omit post attack forensic analysis for determining methods of attacks and determining the extent of compromise of critical digital assets

and Safety, Security and Emergency Preparedness (SSEP) functions for the purpose ensuring that the same attack vector will not succeed in the future. What post-attack actions would [SITE/LICENSEE] take to analyze the methods used by the attacker to determine the extent of compromise of critical digital assets and SSEP functions to prevent the same attack vector from succeeding in the future?

75. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR 73.1. 10 CFR 73.54(c)(1) and (4) require that the licensee's cyber security program be designed to implement security controls to protect the assets identified by paragraph (b)(1) from cyber attacks and to ensure that the functions of protected assets identified by paragraph (b)(1) are not adversely impacted due to cyber attacks. Additionally, 10 CFR 73.54(c)(2) requires the licensee to maintain the capability to recover from cyber attacks.

The preamble to Appendixes D and E of the [SITE/LICENSEE] Cyber Security Plan (CSP) states:

"When implementing alternate compensating controls for a security control, the compensating control is considered applied when there is high assurance that the [critical digital asset] CDA is adequately protected from risks associated with the control that is not applied."

This statement appears to contradict the process described in CSP Appendix A, Section 3.1.6, "Mitigation of Vulnerabilities and Application of Cyber Security Controls," which states:

"For CDAs, the information in Sections 3.1.3 - 3.1.5 is utilized to analyze and document one or more of the following:

1. Implementing the cyber security controls in Appendixes D and E of NEI 08-09, Revision 3.
2. Implementing alternative controls/countermeasures that eliminate threat/attack vector(s) associated with one or more of the cyber security controls enumerated in (1) above by:
  - a. Documenting the basis for employing alternative countermeasures;
  - b. Performing and documenting the analyses of the CDA and alternative countermeasures to confirm that the countermeasures provide the same or greater cyber security protection as the corresponding cyber security control; and
  - c. Implementing alternative countermeasures that provide at least the same degree of cyber security protection as the corresponding cyber security control. Not implementing one or more of the cyber security controls by performing an analyses of the specific cyber security controls for the CDA that will not be implemented to provide a documented justification demonstrating the attack vector does not exist (i.e., not applicable) and therefore those specific cyber security controls are not necessary."

The process described in CSP Appendix A Section 3.1.6 states that the alternate compensating controls will provide equivalent protection to the control that is not implemented. Please clarify which method the licensee will use (i.e., the process described in the preamble to Appendix D and E, or the process stated in Section 3.1.6). Also, please explain how the licensee will ensure that these alternate/compensating controls provide an equal level of protection as the control that was not applied.

76. 10 CFR 73.54(a) requires the licensee to provide high assurance that digital computer, communication systems, and networks are protected against cyber attacks. Additionally, 10 CFR 73.54(c)(1) and (4) require that the licensees' cyber security program be designed to implement security controls to protect the assets identified by paragraph (b)(1) from cyber attacks and to ensure that the functions of protected assets identified by paragraph (b)(1) are not adversely impacted due to cyber attacks. Appendix E, Section 11.3, "Trustworthiness," of the [SITE/LICENSEE] Cyber Security Plan (CSP) states:

"This security control requires that the information system meets defined levels of trustworthiness and requires that software developers employ software quality and validation methods to minimize flawed or malformed software."

Please clarify if the phrase "information system" is a typographical error and the term "critical digital asset" was intended. If "information system" was intended, please explain what is meant by this term and how it relates to the CSP.