1 INTRODUCTION

1.1 PURPOSE

This white paper describes proposed changes to NEI guidance for identifying and protecting Emergency Preparedness (EP) Critical Digital Assets (CDAs). The changes are intended to improve the efficiency of licensee cyber security programs while maintaining program effectiveness to protect against cyber attacks, up to and including the design basis threat. The described changes affect, and will be incorporated into a future revision to:

- NEI 10-04, "Identifying Systems and Assets Subject to the Cyber Security Rule," Revision 2, dated July 2012, and
- NEI 13-10, "Cyber Security Control Assessments," Revision 6, dated August 2017.

1.2 BACKGROUND

Title 10 of the Code of Federal Regulations (CFR), Part 73, "Physical Protection of Plants and Materials," § 73.54, "Protection of Digital Computer and Communication Systems and Networks," requires power reactor licensees 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 § 73.1, "Purpose and scope." Through implementation of the cyber security plans and programs required by § 73.54, the industry has identified several lessons learned that warrant an assessment and revision of the guidance in NEI 10-04, Revision 2, and NEI 13-10, Revision 6. This white paper describes proposed changes to NEI 10-04, Revision 2 and NEI 13-10, Revision 6, that would support more efficient performance of cyber security program activities and oversight, and promote consistent implementation of the requirements of 10 CFR 73.54.

2 DISCUSSION

10 CFR 73.54(a)(1)(iii) requires that EP functions, including offsite communications, be protected against cyber attacks, up to and including the design basis threat as described in 10 CFR 73.1. An EP function is a capability or resource necessary to prepare for, and respond to, a radiological emergency, as required by Section IV of Appendix E to 10 CFR Part 50 and the planning standards in 10 CFR 50.47(b). A licensee's emergency plan describes the site-specific EP functions required to meet regulatory requirements. With respect to cyber security, 10 CFR 73.54 requires a licensee to screen Digital Assets (DAs) associated with EP functions – and NEI 10-04, Revision 2, defines the scope of EP DAs as, "digital computer, and communication systems and networks associated with measures needed for the protection of the public in the event of a radiological emergency."

Industry experience has shown that licensees have identified (scoped) a DA as a CDA even though the compromised DA could not prevent performance of an EP function. In these cases, it was not recognized that the EP function could still be accomplished through other means if the DA was degraded or lost to a cyber attack. A DA associated with an EP function should be

identified as a CDA only if there is no independent alternate method that can be credited to perform the EP function upon the loss of the asset. For purposes of this paper, a "method" is defined as:

> A means that could be employed to perform an emergency response function as described in the site emergency plan or an implementing procedure described in the emergency plan. [Site emergency plans and implementing procedures typically describe primary and one or more alternate METHODS for performing a given function. Provided that at least one METHOD is available, then the ability to perform the associated function has not been lost.][1]

Based on the above information, NEI 10-04 is revised to clearly state the screening criteria described above. In addition, NEI 13-10 is revised to move the EP-related CDA assessment criteria to the identification process discussed in NEI 10-04. If a licensee does not have the capability to prevent an adverse impact to an EP function (i.e., no independent alternate method), then application of the security baseline controls discussed in NEI 13-10 would be necessary.

DAs that are associated with EP functions but that are also associated with other safety-related, important-to-safety, or security functions described in 10 CFR 73.54(a)(1) must also be screened to determine if a cyber attack would adversely impact the other functions for which that DA is associated.

3 COMPLIANCE WITH REGULATORY REQUIREMENTS

10 CFR 73.54(a)(1)(iii) and (iv) require that licensees protect against cyber attacks those digital computer and communication systems and networks associated with emergency preparedness functions, including offsite communications; and support systems and equipment which, if compromised, would adversely impact emergency preparedness functions.

10 CFR 73.54(b)(1) requires that licensees analyze digital computer and communication systems and networks and identify those assets that must be protected against cyber attacks to satisfy 10 CFR 73.54(a).

10 CFR 73.54(b)(2) requires that the licensee establish, implement, and maintain a cyber security program for the protection of the assets identified in 10 CFR 73.54(b)(1).

With the incorporation of the proposed changes described in this document, a cyber security plan and program would ensure that:

a) Digital assets associated with emergency preparedness functions, and their respective support systems and equipment described in 10 CFR 73.54(a)(1)(iii) and (iv) are analyzed as required by 10 CFR 73.54(b)(1).
b) Where the analysis determines that a cyber attack would adversely impact emergency

[1] This definition was taken from NEI 13-01, "Reportable Action Levels for Loss of Emergency Preparedness Capabilities," Revision 0, dated July, 2014.

preparedness functions, those digital assets would be protected against cyber attacks as required by 10 CFR 73.54(b)(2).

Implementation by a licensee of the changes discussed in this white paper will not decrease the effectiveness of a cyber security plan or compliance with the requirements of 10 CFR 73.54,[2] and the resulting cyber security program will still protect digital computer and communication systems and networks against cyber attacks, up to and including the design basis threat as described in § 73.1. The program will remain capable of protecting digital computer and communication systems and networks associated with EP functions, including offsite communications; and support systems and equipment which, if compromised, would adversely impact EP functions. The updated approach simply makes clear that the identification of a potential impact to an EP-related DA from a cyber attack does not automatically mean the EP function is lost and the DA is a CDA; rather, the classification of DA as a CDA would hinge on whether there is an acceptable alternate method to perform the EP function.

Following implementation of the changes, DAs associated with, or supporting, EP functions will be assessed to determine if they are CDAs. (Previous screenings of DAs associated with EP functions may be credited.) The revised guidance will identify an EP-related DA as a CDA only if an analysis determines there is no acceptable alternate method that can be credited to perform the affected EP function upon a loss or compromise of the DA. To be credited, the alternate method must be described in the emergency plan or a procedure described in the emergency plan. The analysis will consider all applicable function requirements described in the emergency plan, including performance within specified time limits.

NEI 10-04 provides guidance for analyzing DAs to identify CDAs. An analysis will determine if an EP function can be performed using an alternate method in the event that the DA for a primary method is lost or compromised. As noted in the guidance, an acceptable alternate method must be independent of the primary method, i.e., both methods would not be affected by the same cyber attack. The analysis guidance also addresses assignment of testing and functional verification actions, and the training of individuals to perform these tasks. Analyses of DAs will be documented and maintained as a station record, and available for inspection.

In summary, it is expected that a licensee's evaluation of necessary changes to their security plans could conclude:

- The change does not affect compliance with any regulatory requirement.
- The change does not decrease the effectiveness of the Physical Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, and/or Cyber Security Plan.
- The change does not decrease the overall capability of Cyber Security program to adequately protect against cyber attacks, up to and including the design basis threat as described in § 73.1.

[2] This conclusion notwithstanding, depending upon site-specific security plan contents, a licensee may need to confirm this assessment through performance of a change evaluation in accordance with 10 CFR 50.54(p).

4 CHANGES TO NEI 10-04

NEI 10-04, "Identifying Systems and Assets Subject to the Cyber Security Rule," Revision 2, provides guidance for determining whether a system and associated digital assets are subject to the requirements of 10 CFR 73.54. Protection as a CDA is required for those assets which would adversely impact Safety, Security and Emergency Preparedness (SSEP) functions if compromised by a cyber attack. This includes digital assets required for the performance of EP functions necessary to meet the requirements in 10 CFR 50.47(b), 10 CFR 50 Appendix E, and site-specific emergency plans.

The following sections of NEI 10-04, Revision 2, will be revised to better align a licensee's cyber security program scope with the requirements in 10 CFR 73.54 for the protection of EP functions.

[Proposed changes in redline/strikeout]

- Section 2.3, "Emergency Preparedness Systems, Including Offsite Communications," is revised to include language that clarifies the scoping criteria is referring to protection of the EP function as stated in 10 CFR 73.54. The following is added as the first paragraph of Section 2.3.

  Digital assets associated with the EP functions described below require analysis for determining whether they are to be protected as CDAs. In doing so, it is the function which must be protected from adverse impact. If a compromise of the DA has no adverse impact to the licensee being able to perform the EP function, the DA is not required to be identified as a CDA

- Section 2.3 is revised to include language to specify that those EP functions which are maintained through alternate methods do not require protection as a CDA. The following is added after the first paragraph in Section 2.3.

  The licensee is required to perform a documented analysis per 10 CFR 73.54(b)(1) to identify digital assets subject to protection as a CDA per 10 CFR 73.54(c). The cyber security rule requirement of 10 CFR 73.54(b)(1) is to identify those assets that, if compromised, would adversely impact EP Functions. The licensee has an established Emergency Plan, independent of the Cyber Security Plan that requires the licensee to maintain capability for performing Emergency Plan measures. These measures are evaluated using the criteria in Section 4 "Methodology for Identifying and Classifying Plant Systems" to demonstrate the licensee's capability to perform the function regardless of the failure mode (e.g., cyber attack, operational failure). This capability ensures that there are independent alternate methods to fulfill the function. The ability to fulfill the EP function regardless of digital asset compromise is a key decision for determining whether the digital asset is required to be identified as a CDA. Adverse impact is focused on the EP function.

- The list beginning on Page 8 of Section 2.3 is revised to include a bullet which clarifies what is acceptable as independent alternate methods, and that acceptable alternate methods includes both administrative and digital methods. The following is added as a new bullet to the end of the list.

  An attack on a single digital asset does not always eliminate the ability to successfully perform the EP function as required.

  In the case of scoping EP DAs/CDAs, the "alternate methods" are alternate methods for performing the EP functions as required by the licensee's Emergency Plan. NEI 13-01 Reportable Action Levels for Loss of Emergency Preparedness Capabilities defines the term method for accomplishing an EP function:

  > METHOD: A means that could be employed to perform an emergency response function as described in the site emergency plan or an implementing procedure described in the emergency plan. [Site emergency plans and implementing procedures typically describe primary and one or more alternate METHODS for performing a given function. Provided that at least one METHOD is available, then the ability to perform the associated function has not been lost.]

  An alternate method for performing the EP function is required to be available in sufficient time such that the compromise of the DA would not adversely impact the licensee's ability to perform EP functions.

  The methods for fulfilling the functions shall be independent such that a single cyber attack instance will not prevent the licensee's capability to perform the function. Two alternate methods can both be digital if they are independent and not susceptible to the same cyber attack instance.

  Administrative methods, including actions performed by personnel, can be considered as an alternate methods provided the administrative method does not depend on the EP DA being assessed.

- Section 5, "Methodology for Identifying Critical Digital Assets," is revised to:
  - Include a clause that allows the use of previously completed EP only CDA assessments as evidence of alternate methods for scoping out EP CDAs as non-critical.
  - Include the guidance for protection of those EP CDAs where independent alternate methods do not exist.
  - Clarify the criteria for making a digital device a CDA related to the word "performs" – the performance of an EP function is not the sole criteria for identifying a DA as critical.

NEI 10-04 includes clarifications and structured guidance for screening EP systems and digital assets in accordance with the licensee's CSP Section 3.1.3 that focus on the protection of the function. The guidance provides a process for determining if sufficient alternate methods exist to maintain the capability for performing the EP functions in the event of a cyber attack. Section 2.3 "Emergency Preparedness Systems, Including Offsite Communications" and this section provide the guidance and criteria for screening EP systems and associated digital assets that adhere to the 10 CFR 73.54 requirements and align to the purpose of protecting the function.

The section describes an acceptable method to consistently identify Critical Digital Assets (CDA). There are a number of sources from which the meaning of the terms "digital" and "Critical Digital Asset" can be either explicitly or implicitly deduced, including 10 CFR 73.54; NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6; Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," dated January 2010; Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Revision 2; IEEE 7-4.3.2-2003, and "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

…

Notwithstanding the other guidance in this document related to the identification of CDAs (e.g., where independent alternate methods are available to fulfill the function), a digital device should be identified as a Critical Digital Asset (CDA) if it performs:

a) SSEP functions or whose compromise would adversely impact a SSEP function;
…

EP DA/CDA Scoping Criteria:
EP only CDAs assessed by NEI 13-10, Revisions 4, 5 and 6 include the analysis that demonstrates adequate alternate methods to perform required EP functions, and therefore do not need to be protected as CDAs. The NEI 13-10 EP only assessments should be maintained as records in accordance with the licensee CSP section 4.13 "Document Control and Records Retention and Handling" as evidence of the non-critical determination. No further evaluation is required for EP DA/CDA identification unless there is a subsequent change to the DA or the EP function.

The following criteria determines whether the EP DA is critical as required by the licensee CSP Section 3.1.3 "Identification of Critical Digital Assets." The analysis considers whether a compromise of the EP digital asset(s) can prevent the performance of the EP function.

If the licensee has implemented independent alternate methods to fulfill the Emergency Plan requirements, the impact from compromise of the EP digital asset will not prevent execution of the EP function.

EP Scoping Criteria for Critical Digital Asset Determination:

1. Does the digital asset only perform an EP function as described in the sixteen planning standards (Section 2.3)?
    a. No; is not associated with the EP criterion, or is also relied on for safety, important-to-safety, or security functions
    b. Yes; proceed to #2
2. Is the EP only digital asset interconnected with other non-EP CDAs such that a cyber security attack on the DA would adversely impact the interconnected non-EP CDA (i.e., the attack vector exists and has not been mitigated through the implementation of cyber security controls implemented in accordance with CSP Section 3.1.6)?
    a. No; proceed to #3
    b. Yes; identify DA as CDA
3. If the digital asset is compromised due to a cyber attack, can the EP function(s) performed by the digital asset be fulfilled as required by the associated planning standard(s)?
    a. No; identify DA as CDA
    b. Yes; DA is not a CDA. The EP Scoping Analysis template below may be used to document the basis that supports the non-Critical classification.

Note - A YES answer in step 2.0 or any NO answer in step 3.0 below, may be remediated in lieu of classifying the EP asset as a CDA.

For those EP DAs identified as CDAs, the cyber security baseline controls are required as described in NEI 13-10, Section 5, “Baseline Cyber Security Protection Criteria.”

Analysis of the scoping criteria may be documented using the table below.

EP Scoping Analysis		
1.0	Does DA perform ONLY an EP-related or EP support systems and equipment function?	☐ YES ☐ NO
Note: The following guidance may be used for identification of EP CDAs associated with EP functions that are not otherwise also relied on for safety, important-to-safety, or security functions.		
If YES, document applicable 10 CFR 50.47 Planning Standard(s) below:		
If YES, document applicable NUREG -0654 Section(s) below:		
If YES, document the Emergency Planning function(s) below:		
IF YES, THEN proceed Step 2.0	IF NO, THEN proceed with scoping analysis for remaining SSEP functions	

2.0	Is the EP only digital asset interconnected with other non-EP CDAs such that a cyber security attack on the DA would adversely impact the interconnected non-EP CDA (i.e., the attack vector exists and has not been mitigated through the implementation of cyber security controls implemented in accordance with CSP Section 3.1.6)?	☐ YES ☐ NO
	Note: Connectivity alone does not constitute a DA being identified as a CDA. For this question to be a YES, determine whether the DA could be leveraged to adversely impact another safety, important-to-safety, or security function. If so AND the interconnected CDA is not adequately protected from potential adverse impact, then the DA would be a CDA.	
IF NO, THEN proceed Step 3.0		IF YES, THEN the EP only asset is a CDA and apply baseline security controls of NEI 13-10, Section 5, "Baseline Cyber Security Protection Criteria"
3.0	Are alternate methods available for performing the intended EP function, including offsite communications? Document basis for YES or NO answer:	☐ YES ☐ NO
IF YES, THEN proceed to Step 3.1		IF NO, THEN the EP only asset is a CDA. Apply baseline security controls of NEI 13-10, Section 5, "Baseline Cyber Security Protection Criteria"
3.1	Are one or more of the alternate methods administrative, non-digital, or if digital is it adequately independent? Document basis for YES or NO answer:	☐ YES ☐ NO
Note: 1.) Two methods would be considered adequately independent if they do not rely on equipment that if compromised by cyber attacks would adversely impact both methods of performing the EP function (e.g., a PBX-based phone system vs. satellite phones, data obtained by MET tower vs. data obtained through a weather service, data obtained from SPDS vs. received via fax, etc.). 2.) Administrative methods, including actions performed by personnel, can be considered as an alternate methods provided it does not depend on the DA being assessed.		
IF YES, THEN proceed to Step 3.2		IF NO, THEN the EP only asset is a CDA. Apply baseline security controls of NEI 13-10, Section 5, "Baseline Cyber Security Protection Criteria"
3.2	Is the alternate methods documented? Document basis for YES or NO answer:	☐ YES ☐ NO
Note: The alternate methods must be documented in a plant plan, policy, or implementing procedure.		
IF YES, THEN proceed to Step 3.3		IF NO, THEN the EP only asset is a CDA and apply baseline security controls of NEI 13-10, Section 5, "Baseline Cyber Security Protection Criteria"
3.3	Is the equipment that a compromise of the DA would impact periodically checked to ensure the equipment is capable of performing its intended function and an appropriate response initiated, if needed? Document basis for YES or NO answer.	☐ YES ☐ NO
Note: 1.) Specifically, a cyber attack that would prevent the EP-related equipment from performing its intended function can be detected and responded to prior to an adverse impact on the EP-related function during a radiological emergency.		

2.) Measures for detection and response may be technical, procedural, or administrative, and could include periodic functional or availability testing (e.g., existing periodic operability tests performed on plant systems or equipment). The measures in place must be performed at a frequency to ensure the ability to employ the alternate methods in a timeframe sufficient to mitigate the adverse consequences of a cyber attack.		
IF YES, THEN proceed to Step 3.4	IF NO, THEN the EP only asset is a CDA and apply baseline security controls of NEI 13-10, Section 5, "Baseline Cyber Security Protection Criteria"	
3.4	Are appropriate facility personnel trained to use the alternate method? Document basis for YES or NO answer:	☐ YES ☐ NO
IF YES, THEN the EP DA is non-critical (i.e., DA is not a CDA).	IF NO, THEN the EP only asset is a CDA and apply baseline security controls of NEI 13-10, Section 5, "Baseline Cyber Security Protection Criteria."	

5 CHANGES TO NEI 13-10

NEI 13-10, "Cyber Security Control Assessments," provides guidance for implementation of cyber security controls. Operating experience with cyber security program implementation has indicated that the steps for protecting EP CDAs can be performed during the CDA identification assessment, thus streamlining the overall process.

The following sections of NEI 13-10, Revision 6, will be revised to align with changes to NEI 10-04, Revision 2. Again, compliance with 10 CFR 73.54 is not affected.

[Proposed changes in redline/strikeout]

- Section 3.1, "EP CDAs," is revised to describe the conditions at which an EP DA would be identified as a CDA and the required assessment methodology.

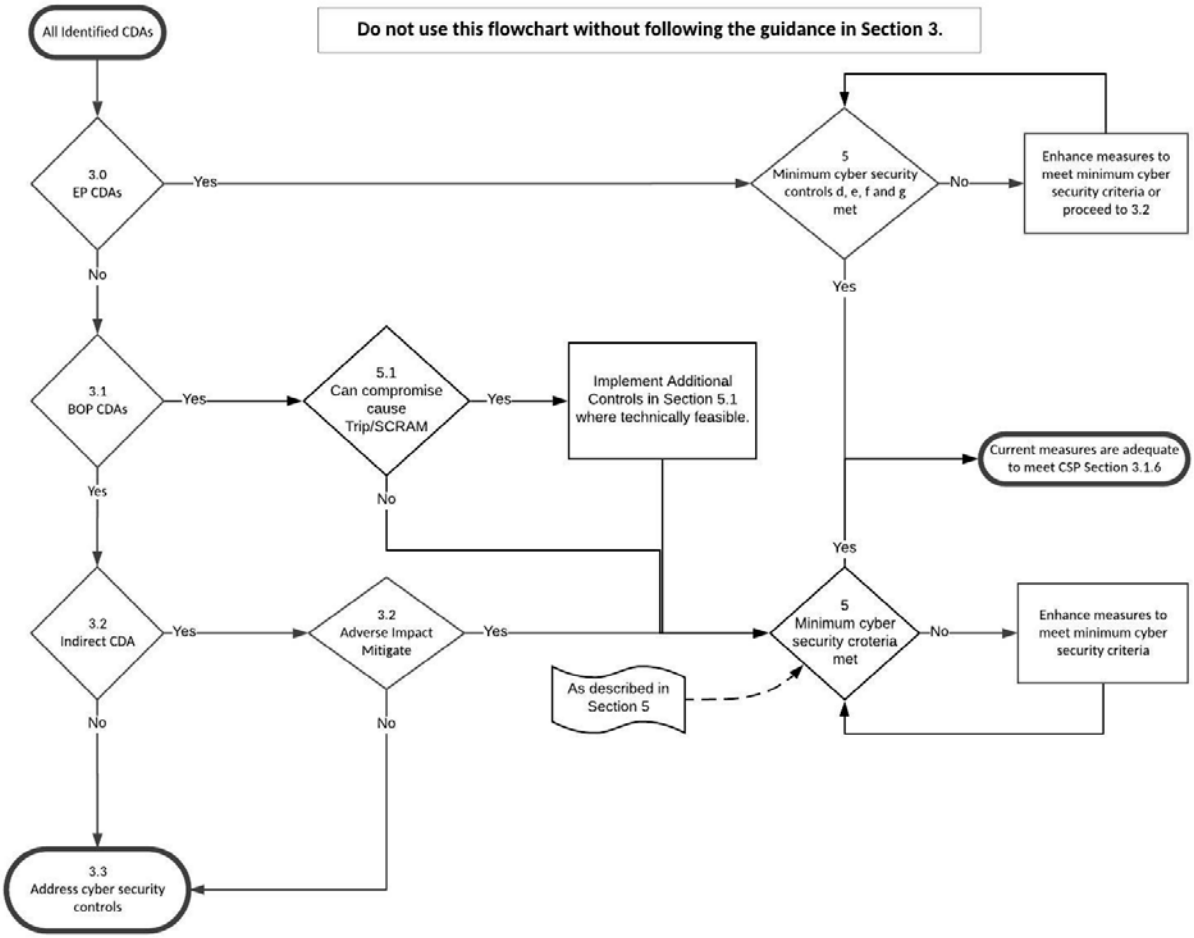
> 3.1 EP CDAS
>
> EP CDAs are those CDAs that support licensee's performance of EP functions where the licensee does not have ~~and that have an~~ independent alternate methods ~~means~~ of performing those functions. ~~EP CDAs must meet the following criteria:~~
>
> ~~1. The CDA only supports an EP function and does not perform or support any other Safety, Important-to-Safety or Security function.~~
> ~~2. An Alternate Means assessment is performed in accordance with Section 4 of this document to demonstrate and document that an independent alternate means of performing the EP function will be available in sufficient time such that the compromise of the CDA would not adversely impact the licensee's ability to perform that EP function .~~
> ~~3. EP CDAs must meet all of the requirements defined in Section 4 of this document.~~

Alternate methods are methods (as defined in NEI 13-01, "Reportable Action Levels for Loss of Emergency Preparedness Capabilities," Revision 0, dated July, 2014) for performing EP functions. An alternate method for performing the EP function is required to be available in sufficient time such that the compromise of the DA would not adversely impact the licensee's ability to perform EP functions.

For EP CDAs, licensees may address the technical security controls provided in their CSP using the method provided in Section 3.1.6 of their CSP by ~~documenting that the CDAs meet the EP CDA criteria described above and by~~ implementing the baseline controls for EP CDAs as described in Section 5, "Baseline Cyber Security Protection Criteria."

- Section 4, "EP Functions Maintained through Alternate Means," is deleted in its entirety as the applicable guidance has been moved to NEI 10-04. The word DELETED will be inserted to replace the deleted text

- Appendix A, "Figures" - The "Consequence Assessment" flowchart (Figure 1) is updated regarding the EP only blocks:



- Appendix A – The "Alternative Means Assessment for EP" flowchart (Figure 2) is deleted as this is no longer an applicable section of NEI 13-10. The word DELETED will be inserted to replace the deleted flowchart.

- Various conforming changes are necessary in Appendices B and C of NEI 13-10. These are described herein, and will be incorporated into a future revision to NEI 13-10.

  - In Appendix B, pages B-3 through B-4, the questions related to EP only consequence assessment are updated: Question 1.1 is revised to eliminate collection of redundant documentation, and questions 1.2, 1,3, 1.4, 1.5 are deleted. This assessment is not performed per NEI 13-10, but rather in NEI 10-04. EP only baseline cyber security controls will remain. The word DELETED will be inserted to replace the deleted text.

  - In Appendix C, Pages C-3 through C-7; Pages C-23 through C-28: EP only assessment examples are deleted as this assessment type is no longer applicable.

  - In Appendix C, Pages C-13 through C-21: Includes an EP only assessment example where one of the conditions for alternate methods is not met, however, a corrective action

is put into place for remediation so that the CDA can be assessed as EP only. This example is deleted as the remediation would be performed as part of the NEI 10-04 determination. This assessment type is no longer applicable to NEI 13-10. The word DELETED will be inserted to replace the deleted text.