WILLIAM R. GROSS
Director, Incident Preparedness
Facility Security Officer

1201 F Street NW, Suite 1100
Washington, DC 20004
P: 202.739.8123
wrg@nei.org
nei.org

NUCLEAR ENERGY INSTITUTE

April 8, 2020

Ms. Shana Helton
Director, Division of Physical and Cyber Security Policy
Nuclear Security and Incident Response
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Endorsement of NEI White Paper, "Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Emergency Preparedness Functions," Dated March 2020

Project Number: 689

Dear Ms. Helton:

By letter dated July 27, 2012[1] the Nuclear Regulatory Commission (NRC) found NEI 10-04, "Identifying Systems and Assets Subject to the Cyber Security Rule," Revision 2, dated July 2012 acceptable for use by licensees to identify critical digital systems and critical digital assets. By letter dated September 7, 2017[2], the NRC found NEI 13-10, "Cyber Security Control Assessments," Revision 6, dated August 2017, acceptable for use by licensees to address the security controls provided in their cyber security plans. Lessons learned through the implementation of cyber security programs indicate that improvements are necessary to enhance clarity, support efficient and consistent implementation and to support NRC oversight activities.

Accordingly, the Nuclear Energy Institute (NEI),[3] on behalf of its members, is submitting the revised white paper proposing changes to NEI 10-04 and NEI 13-10 for NRC review and endorsement. The attached white paper addresses the NRC and stakeholder comments provided at the NEI Cyber Security Implementation Workshop on March 3rd though March 5th, 2020. The changes in this white paper improve the screening of 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. These changes are intended to improve the effectiveness and efficiency of licensee cyber security programs while maintaining adequate protection against the radiological sabotage cyber attack. The attached document provides a technical basis for the

[1] ADAMS Accession No. ML12194A532

[2] ADAMS Accession No. ML17240A002

[3] The Nuclear Energy Institute (NEI) is the organization responsible for establishing unified industry policy on matters affecting the nuclear energy industry, including the regulatory aspects of generic operational and technical issues. NEI's members include all entities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect/engineering firms, fuel cycle facilities, nuclear materials licensees, and other organizations and entities involved in the nuclear energy industry.

changes and provides a markup of the relevant changes made to NEI 10-04 and NEI 13-10. The markup does not include all minor editorial and conforming changes. All changes will be incorporated into future revisions of NEI 10-04 and NEI 13-10.

NEI requests that the NRC review and endorse the NEI White Paper, "Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Emergency Preparedness Functions," dated March 2020, by May 8, 2020. While each licensee must review changes to their Commission approved Cyber Security Plan in accordance with the requirements of 10 CFR 50.54(p), NEI requests that the NRC's review confirm that the changes proposed in this white paper do not decrease the effectiveness of the cyber security plan provided in NEI 08-09. If any revisions to this document are desired, please include suggested wording and the technical data to support the proposed change(s).

If you have any questions or require additional information, please contact Richard Mogavero, at (202) 739-8174 or rm@nei.org, or me.

Sincerely,

William R. Gross

Attachments:
1) Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Emergency Preparedness Functions

c: Mr. James D. Beardsley, NSIR/CSD
NRC Document Control Desk

1 INTRODUCTION

1.1 PURPOSE

This white paper describes proposed changes to previously approved 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 (DBT). The proposed 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 DBT as described in § 73.1, "Purpose and scope." Lessons learned from implementation of the cyber security plans and programs required by § 73.54, identified areas that warrant an assessment and revision of the guidance in NEI 10-04, Revision 2, and NEI 13-10, Revision 6. The proposed changes 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 licensees to protect digital computer and communication systems and networks associated with: (i) Safety-related and important-to-safety functions; (ii) Security functions; (iii) Emergency preparedness functions, including offsite communications; and (iv) Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions from 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, "Emergency Planning and Preparedness for Production and Utilization Facilities," and the planning standards in 10 CFR 50.47, "Emergency Plans," Section(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 perform an analysis of 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 demonstrated that licensees have identified (scoped) DAs as CDAs even though compromise via a cyber attack of these DAs could not adversely impact the EP function. The

screening methodology in the NEI guidance did not include criteria where other methods can be credited to accomplish the EP function. A DA associated with or used to perform an EP function should be identified as a CDA only if there is no alternate method that is adequately independent and diverse that can be credited to perform the EP function upon the loss or compromise of the DA. The identification of a compromise may include software checks, procedural, or administrative methods credited in the Emergency Plan, licensee's implementing procedures, or NRC approved guidance to alert the operator that the EP DA is not performing it's intended function.

For the purposes of screening and identifying EP DAs for protection, methods that are adequately, independent, and diverse credited for fulfilling EP functions shall:

- not be susceptible to the same cyber attack,
- be described in the site emergency plan and/or implementing procedure(s) (Site emergency plans and implementing procedures typically describe primary and one or more alternate methods for performing an EP function. These alternate methods are typically used throughout site emergency plan as consistent terminology (e.g. compensatory measures, backup method, etc.)).

Note:
Two methods would be considered adequately independent and diverse if they do not rely on equipment that if compromised by the same cyber attack 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.).

Provided that a cyber compromise of the DA can be detected and at least one credited method that is adequately independent and diverse is available, then the ability to perform the associated function has not been lost.

The criteria in this document is used to screen and identify EP assets only. These criteria will not be used to screen and identify equipment that performs safety related, important-to-safety, or security functions. Adverse impact is to be interpreted as the loss of an EP function since NRC regulations that govern EP requirements provide flexibility to accomplish the EP function with alternate methods.

EP DAs that either perform or support a safety-related, important-to-safety, or security function(s) described in 10 CFR 73.54(a)(1) or provide a digital pathway to a CDA must also be screened to determine if a cyber attack would adversely impact the function or other CDAs.

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 the licensee to 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 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.[1] The cyber security 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 against cyber attacks, up to and including the DBT as described in § 73.1. The revised approach meets the intent of 10 CFR 73.54(b)(1). The analysis of EP digital computer and communication systems and networks will identify those assets that must be protected against cyber attacks to satisfy 10 CFR 73.54 (a).

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 when the 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 or the analysis (see table 1) determines the DA is a CDA. Licensees may credit the alternate methods as long as the alternate method(s) is/are 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 required specified time limits.

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

NEI 10-04 provides guidance for analyzing DAs to identify CDAs. The analysis will determine if an EP function can be performed using an alternate method in the event the DA is lost or compromised. As noted in the guidance, an acceptable alternate method must be independent and diverse of the primary method and would not be affected by the same cyber-attack. The 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.

For those EP CDAs that require protection, licensees may follow the guidance in the approved NEI 13-10 guidance to determine the security controls that need to be implemented. Licensees may take credit for security controls periodicity verification at the periodicity established by the EP requirements.

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 including EP requirements.
- decrease the effectiveness of the Physical Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, and/or Cyber Security Plan.
- decrease the overall capability of Cyber Security program to adequately protect against cyber attacks, up to and including the DBT as described in § 73.1.

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 **(see table and the flowchart)** for determining whether they are to be protected as CDAs. In doing so, the licensee must ensure the EP function can be performed and there is no

adverse impact to the function. If a compromise or loss of the DA has no adverse impact to the licensee being able to perform the EP function then, the DA may not be required to be identified as a CDA.

- Section 2.3 is revised to include language to specify that the screening methodology in the NEI guidance will include criteria where other methods can be credited to perform those EP functions. DAs whose compromise via cyber means and do not adversely impact the EP function 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 per 10 CFR 73.54(c). The cybersecurity rule requirement of 10 CFR 73.54(b)(1) is to identify those assets that, if compromised, would adversely impact SSEP Functions. The licensee has an established Emergency Plan, independent of the Cyber Security Plan that identifies and describes the licensee's methods for maintaining emergency preparedness and responding to emergencies. These measures are evaluated using the criteria in NEI 10-04, 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, loss, or operational failure). This capability ensures that the licensee can detect a cyber compromise of an EP DA and an alternate method is adequately independent and diverse to fulfill the EP 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.

  EXAMPLE OF ADEQUATE INDEPENDENT AND DIVERSE METHOD

  a. Two methods would be considered adequately independent (diverse) 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.).

- The list beginning on Page 8 of Section 2.3 is revised to include a bullet which clarifies what is an acceptable alternate method(s) that is/are adequately independent and diverse, and it may include both administrative and digital methods. The following is added as a new bullet to the end of the list.

  In the case of scoping EP DAs/CDAs, the "alternate methods" are 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," Rev. 0, defines the term method for accomplishing an EP function as follows:

  > 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.]

For the purposes of evaluating EP DAs, alternate methods credited for fulfilling EP functions shall:

Be described in the site emergency plan and/or an implementing procedure (Site emergency plans and implementing procedures typically describe primary and one or more alternate methods that are adequately independent and diverse for performing a given function. These alternate methods are typically referred to throughout the site emergency plan using consistent terminology (e.g. compensatory measures, backup method, etc.)).

An alternate method that is adequately independent and diverse credited for performing the EP function must be available in sufficient time to detect the compromise of the DA. Detecting the compromise in sufficient time ensures the licensee can implement an alternate method to perform the EP function(s). Licensees may take credit for EP operational checks and the associated performance frequency established in the Emergency Plan (E-Plan) and/or implementing procedures to meet the periodic checks required by cyber security controls. These checks ensure the equipment is capable of performing its intended function and an appropriate response is initiated if the EP DA is compromised.

The methods for fulfilling the functions shall be adequately independent and diverse such that a single cyber attack will not adversely impact the licensee's capability to perform the EP function. Two alternate methods can both be digital if they are adequately independent, diverse, and not susceptible to the same cyber attack (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.).

Administrative methods, including actions performed by licensee personnel, can be considered technically acceptable as an alternate method provided the administrative method does not depend on the EP DA being assessed, are included in the EP plan and/or implementing procedure, or are alternate methods credited to perform the EP function.

- 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 re-classifying EP CDAs to be DAs.
  - Include the guidance for protection of those EP CDAs where alternate methods that are adequately, independent, and diverse do not exist to perform the EP function.
  - 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 focuses on performance of the EP function. The guidance provides a process for determining if a method to detect a cyber compromise and sufficient alternate methods exist to maintain the capability of performing the EP functions in the event of a cyber attack. Section 2.3, "Emergency Preparedness Systems, Including Offsite Communications," provides the guidance and criteria for screening EP systems and associated digital assets that adhere to the 10 CFR 73.54 requirements.

This section describes an acceptable method to consistently identify Critical Digital Assets (CDAs). There are a number of sources from which the meaning of the terms "digital" and "Critical Digital Asset" are defined ; 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 alternate methods that are adequately independent, and diverse 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:

Licensees must ensure EP-only CDAs previously assessed by NEI 13-10 revisions, found acceptable for use by the NRC, include the analysis that demonstrates detection of a cyber compromise and identifies adequate alternate methods to perform required EP functions to be re-classified as DAs. The NEI 13-10 EP only assessments previously performed 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 reclassifying determination. After completing the analyses (see the table and the flowchart), no further evaluation is required for EP-only DA/CDA identification unless there is a subsequent change to the DA or the EP function.

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

If the licensee has implemented alternate methods that are adequately independent and diverse to fulfill the Emergency Plan requirements, the impact from compromise or loss of the EP-only 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. The asset must be screened for other functions (SSEP) in NEI 10-04.
b. Yes; proceed to #2

2. Is the EP only digital asset interconnected with other non-EP CDAs such that the DA can be leveraged (e.g., via a cyber attack or compromise) to 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)? Note: If the EP DA provides protection that is inherited by a non-EP CDA, the EP DA must be assessed to ensure the attack vector does not exist or has been mitigated through the implementation of cyber security controls.

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 cyber compromise of the DA be detected in time so that the EP function(s) performed by the digital asset can 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.

For those EP CDAs that do not meet the indirect criteria, then the CDA will be a direct CDA and licensees will have to address all the security controls in accordance with their CSPs Section 3.1.6. Licensees may utilize the approved NEI 13-10 guidance for the cyber security controls assessment process.

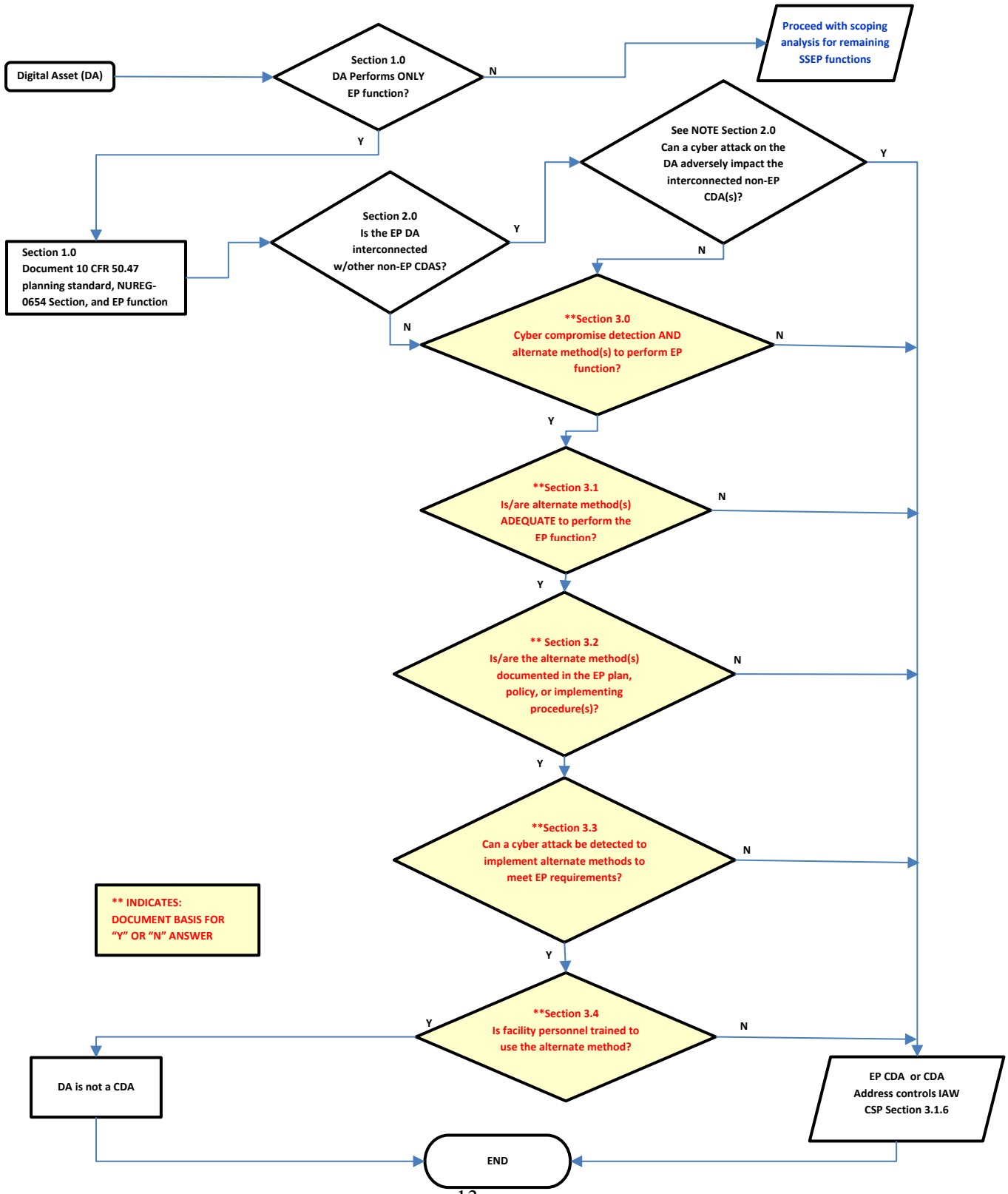
Analysis of the scoping criteria may be documented using the table below.

1.0	Does DA being assessed perform ONLY an EP-related or EP supported 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 DA being assessed interconnected with other non-EP CDAs such that the DA can be leveraged (e.g., via a cyber attack or compromise) to 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)? Note: If the EP DA provides protection that is inherited by a non-EP CDA, the EP DA must be assessed to ensure the attack vector does not exist or has been mitigated through the implementation of cyber security controls.	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 being assessed could be leveraged to adversely impact a safety, important-to-safety, or security function AND if the interconnected CDA is not adequately protected from potential adverse impact. If the answer is NO, 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 requires controls provided in the licensee's CSP in accordance with Section 3.1.6.
3.0	Can a cyber compromise of the DA be detected in time AND are alternate methods available for performing the intended EP function, including offsite communications, in time to fulfill the associated required EP standard(s)? **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 and requires documentation and controls provided in the licensee's CSP in accordance with Section 3.1.6.
3.1	Are one or more of the alternate methods administrative, non-digital, or if digital is it diverse and adequately independent? **Document basis for YES or NO answer:**	YES NO
Note: 1.) Two methods would be considered diverse and 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 method 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 and requires documentation and controls provided in the licensee's CSP in accordance with Section 3.1.6.	
3.2	Is/are the alternate method(s) documented? **Document basis for YES or NO answer:**	YES NO
Note: The alternate method(s) must be documented in a plant EP, policy, or implementing procedure.		

IF YES, THEN proceed to Step 3.3	IF NO, THEN the EP only asset is a CDA and requires documentation and controls provided in the licensee's CSP in accordance with Section 3.1.6.	
3.3	Are there measures to detect a cyber attack on the DA so alternate methods can be implemented as required to meet the EP requirements to ensure the equipment can perform its intended function and an appropriate response is 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 include required EP equipment operational checks and the associated performance frequency established in the E-Plan or EP implementing procedures for the cyber security controls required periodicity checks to ensure the equipment can perform its intended function within the required EP timelines, if applicable, and an appropriate response initiated if the EP DA is compromised.		
IF YES, THEN proceed to Step 3.4	IF NO, THEN the EP only asset is a CDA and requires documentation and controls provided in the licensee's CSP in accordance with Section 3.1.6.	
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 requires documentation and controls provided in the licensee's CSP in accordance with Section 3.1.6.	

Do not use this flowchart without following the guidance in Section 3



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 the criteria to determine EP CDA protection in NEI 13-10 can be better utilized 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-only CDAs are those CDAs associated with licensee's performance of required EP functions and where the screening process has determined a method that is independent and diverse does not exist to perform the EP function(s). Therefore, the compromise of the EP-only digital assets would adversely impact the EP function(s).

  ~~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.~~

  For EP-only 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-only CDAs as described in Section 5, "Baseline Cyber Security Protection Criteria."

  Where the analysis determines the ability to detect and mitigate against adverse impact of the EP function can't be accomplished, then the EP CDA is direct and the required technical security controls for the CDA is addressed as described in Section 6.

- Section 4, "EP Functions Maintained through Alternate Method," 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 Method 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 protections 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.